РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.1

Листов 80

2022

АННОТАЦИЯ

Настоящий документ является руководством администратора Операционной системы (ОС) Аврора релиз 4.0.2 update 2.

Настоящий документ содержит описание доступных администратору функциональных возможностей мобильного устройства (МУ), функционирующего под управлением ОС Аврора[1].

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

ПРИМЕЧАНИЯ:

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

2. 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.

[1]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

ПРИМЕЧАНИЕ. Перед началом работы с МУ администратору необходимо выполнить первоначальную настройку, 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 шифрованному домашнему каталогу пользователя (Рисунок 1);
– разблокировки МУ (Рисунок 2).

ПРИМЕЧАНИЕ. Шифрование раздела с домашними директориями пользователей (подраздел 4.9) происходит в следующих случаях:

– при первом включении МУ
– после сброса МУ до заводского состояния (подраздел 2.2).

Рисунок 1

Рисунок 2

1.2. Установка времени и даты

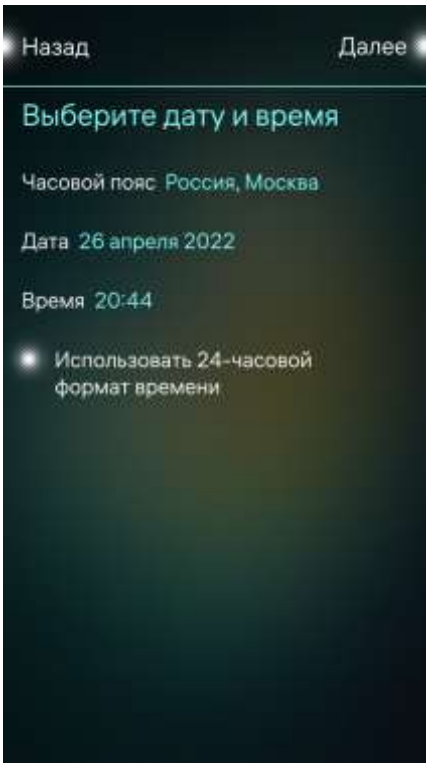

Рисунок 3

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.

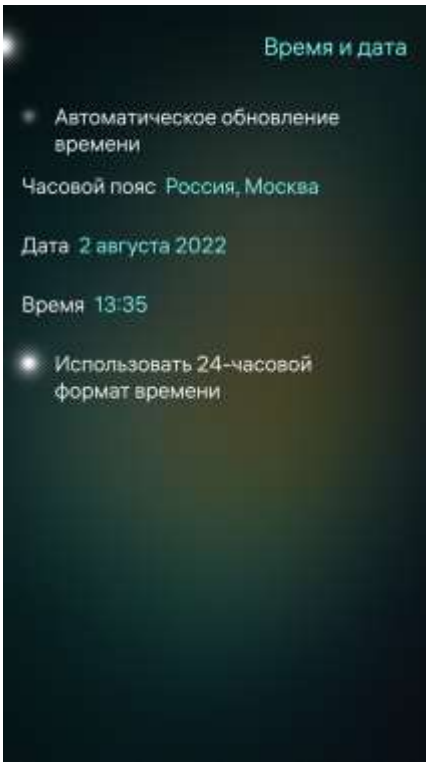

Рисунок 4

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.

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

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

– 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;

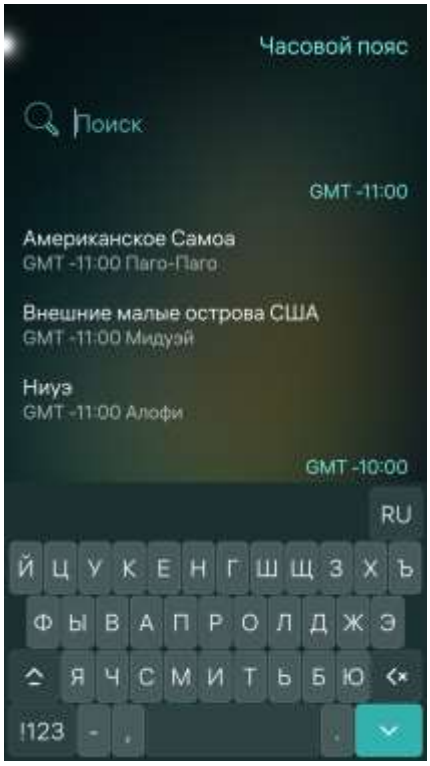

Рисунок 5

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 1.6);

– осуществлять настройку МУ (подраздел 1.7).

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

– не допускать установку любого программного обеспечения (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 (ИС);

– 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.

Роль – совокупность прав доступа, на основе которых определяется возможность выполнения того или иного действия в ОС Аврора.

ПРИМЕЧАНИЕ. В зависимости от выбранной роли возможности МУ, функционирующего под управлением ОС Аврора, могут отличаться.

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 такой ролью, будут применимы ко всем учетным записям МУ;

– до 6 учетных записей с ролью пользователя, создание которых выполняется администратором в системных настройках 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);

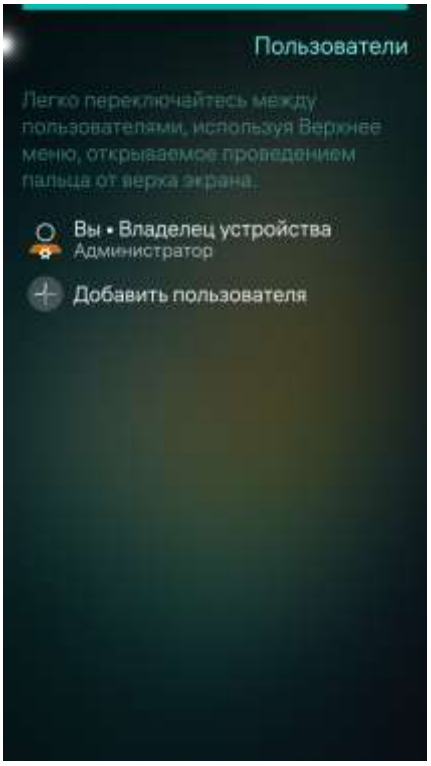

Рисунок 9

ПРИМЕЧАНИЯ:

1. Минимальные и максимальные значения для задания квоты зависят от конструктивных особенностей МУ;

2. Подробная информация о квотировании постоянной памяти приведена в подразделе 1.5.

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

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

Рисунок 10

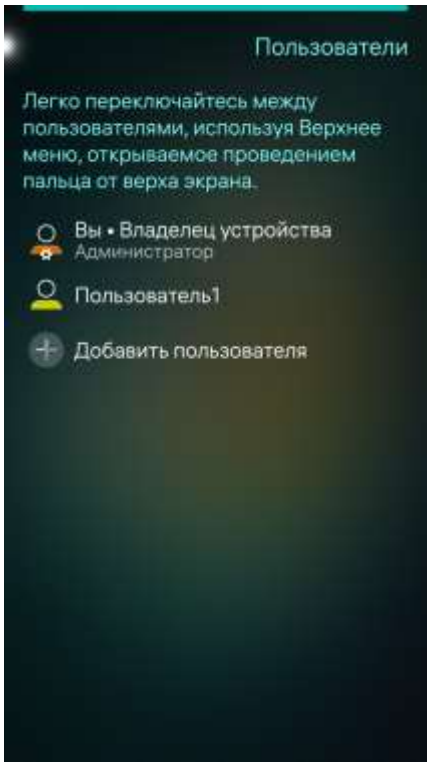

Рисунок 11

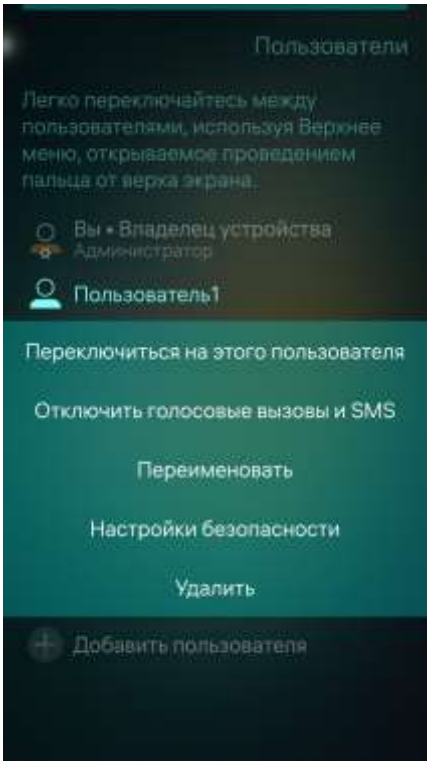

Рисунок 12

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 пользователя (п. 1.4.4);

– настройки безопасности (подраздел 1.6):

– удаление учетной записи пользователя (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 от 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 от верхнего края Экрана блокировки к нижнему;

– коснуться имени учетной записи пользователя;

– в раскрывающемся списке выбрать «Владелец устройства» (Рисунок 14);

– дождаться, когда ОС Аврора 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

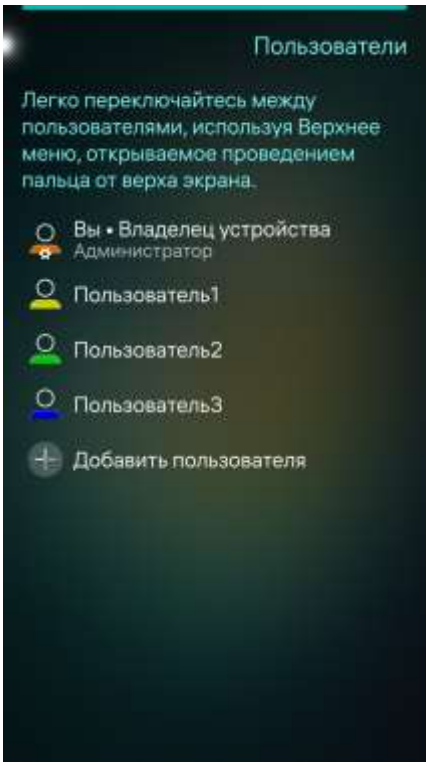

Рисунок 15

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.

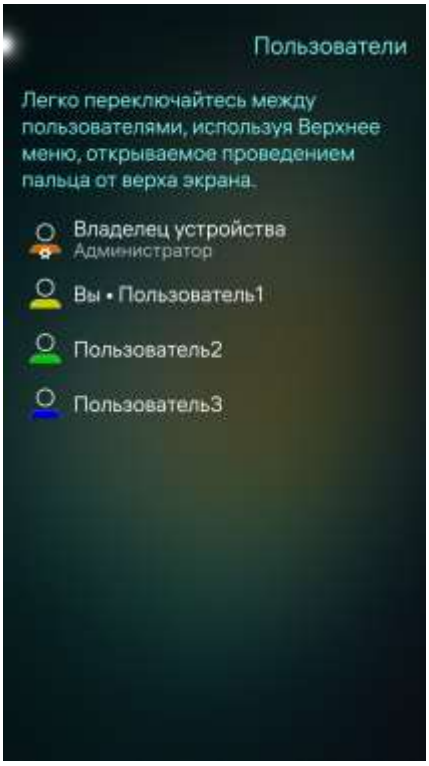

Рисунок 16

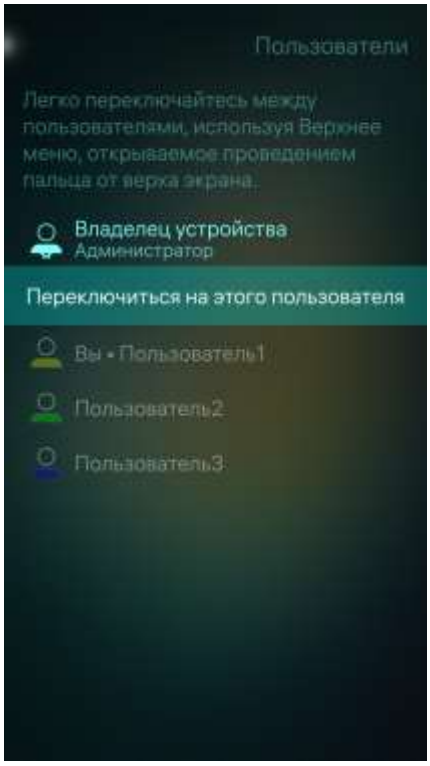

Рисунок 17

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, а также сообщений, выводимых на экран МУ при отключении голосовых вызовов и SMS, приведено в документе «Руководство пользователя».

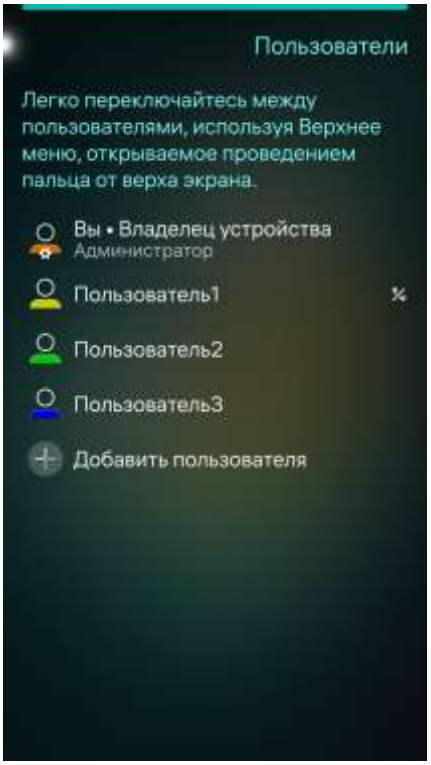

Рисунок 18

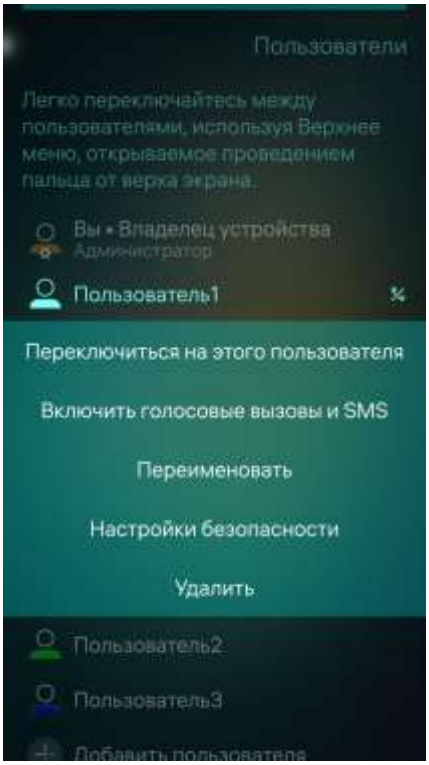

Рисунок 19

1.4.4. Переименование учетной записи

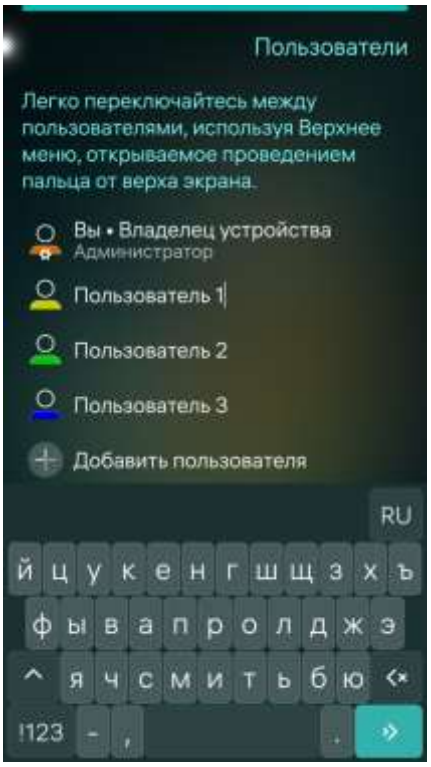

Рисунок 20

Для переименования учетной записи пользователя необходимо выполнить следующие действия:

– коснуться строки с именем учетной записи, которую необходимо переименовать;

– в контекстном меню коснуться пункта «Переименовать» (см. Рисунок 12);

– ввести новое имя учетной записи пользователя (Рисунок 20);

– коснуться значка » для подтверждения действия.

В результате учетная запись пользователя будет переименована.

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 (Рисунок *21*);

– для удаления подтвердить действие вводом текущего кода безопасности.

В результате будет удалена учетная запись и данные пользователя.

1.5. Квотирование постоянной памяти

Квотирование представляет собой разделение ограниченного дискового пространства между учетными записями пользователей МУ и обеспечивает достижение следующих целей:

– создание максимального количества учетных записей пользователей на МУ;

– наличие у учетной записи пользователя дискового пространства (квоты), выделенного специально для нее;

– ограничение квоты, доступной для учетной записи пользователя.

В ОС Аврора предусмотрена возможность при создании учетной записи пользователя выделить для него квоту. Данный пользователь не сможет претендовать на больший объем постоянной памяти, при этом выделенное ему пространство будет недоступно для других пользователей даже в случае, если оно свободно.

Для того, чтобы задать новой учетной записи пользователя квоту на использование дискового пространства, необходимо на странице создания данного пользователя установить количество выделяемых ему ГБ, перемещая соответствующий слайдер вправо для увеличения квоты либо влево для уменьшения (см. Рисунок 10).

ВНИМАНИЕ! Изменение квоты на использование дискового пространства невозможно после создания пользователя.

ОС Аврора автоматически вычисляет допустимые пределы квотирования таким образом, чтобы можно было создать максимальное количество учетных записей: учетная запись с ролью администратора и до 6 учетных записей с ролью пользователя. Нижняя граница квоты устанавливается в 2 ГБ и менее, если общий объем памяти на МУ менее 14 ГБ. Верхняя граница выбирается с расчетом, чтобы для каждой учетной записи пользователя, которую возможно создать на МУ, оставалось хотя бы по минимальному объему памяти.

Подробнее алгоритм вычисления границ *MinQuote* и *MaxQuote* можно представить следующими выражениями:

– *AllSpace* – объем всего раздела;

– *Nusr* – количество созданных на МУ учетных записей, включая администратора;

– *Qi* – квоты созданных на МУ учетных записей;

– *UsrAvSpace* = ***AllSpace – 2 GB;*** // 2ГБ выделяется для учетной записи администратора;

– *MinQuote* = ***min (UsrAvSpace/6 , 2 GB);*** // выделяется минимальная квота 2 ГБ (при наличии небольшого объема пространства выделяется весь доступный объем, разделенный на 6 учетных записей пользователей);

– *MaxQuote* = ***UsrAvSpace - sum (Qi) - MinQuote x (6 - Nusr);*** // максимальная квота, которую можно выделить создаваемому на МУ пользователю – все доступное пространство за вычетом суммы уже выделенных квот, а также количества пользователей, которые могут быть созданы в будущем (т.к. текущий пользователь вычитается сразу, квота на будущее для него не резервируется).

1.6. Настройки безопасности

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

1.6.1. 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.

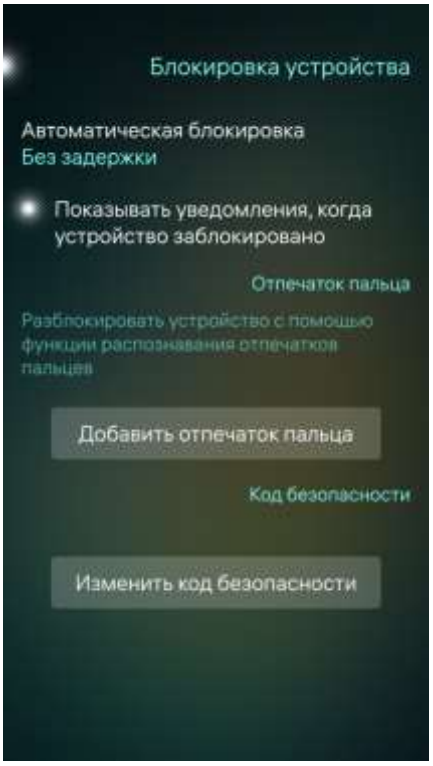

Рисунок 22

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 версии ОС Аврора[2] (Рисунок 23, Рисунок 24).

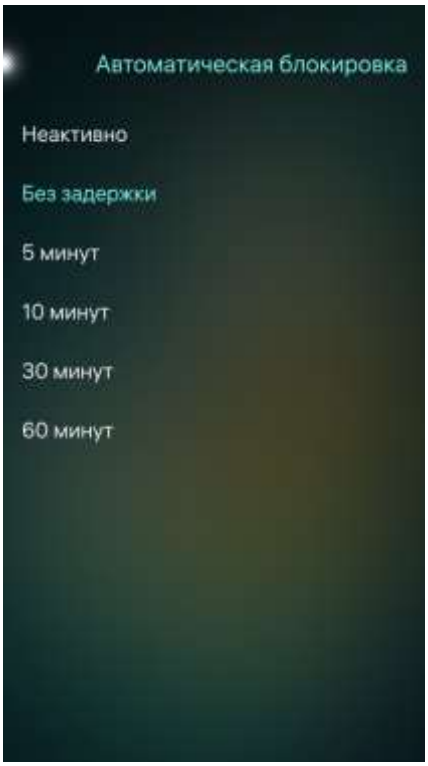

Рисунок 23

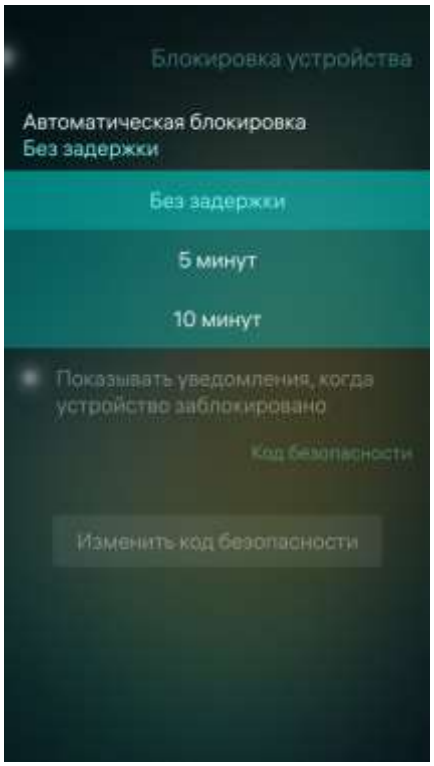

Рисунок 24

[2] Описание возможных версий ОС Аврора приведено в таблице (Таблица 6).

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, а также от версии ОС Аврора. Подробная информация о настройке блокировки с помощью функции распознавания отпечатка пальца приведена в документе «Руководство пользователя».

1.6.2. Настройка парольной политики

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

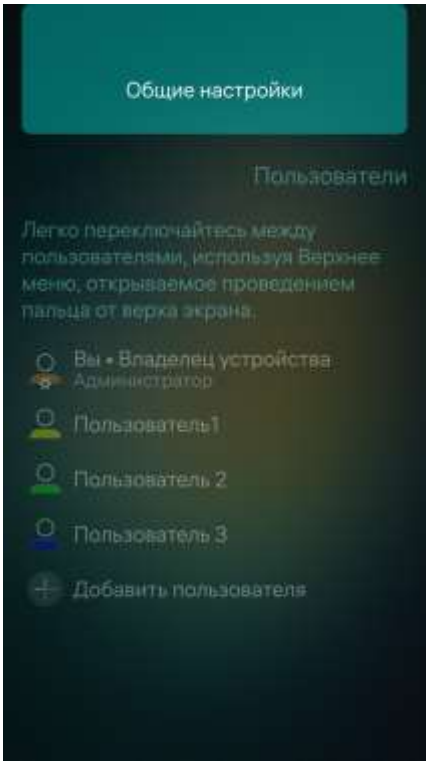

Рисунок 26

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).

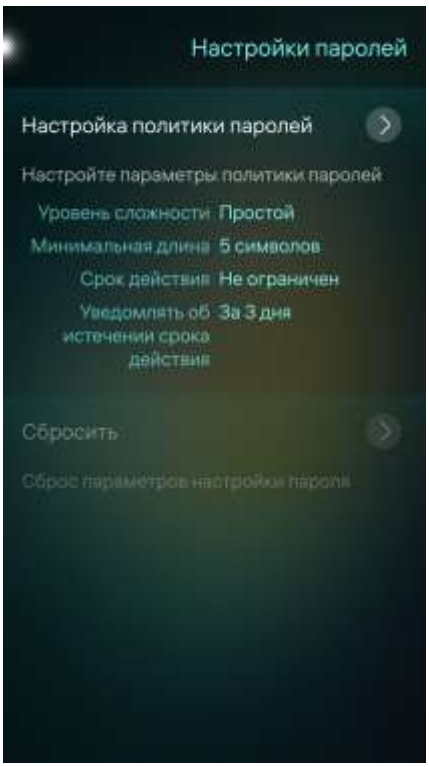

Рисунок 27

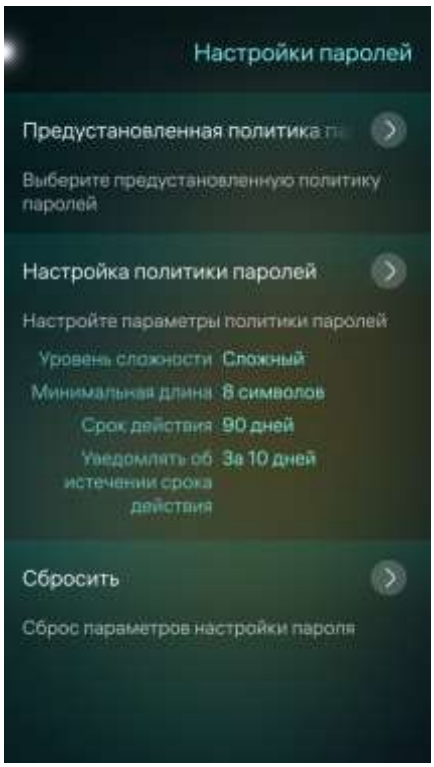

Рисунок 28

ВНИМАНИЕ! Наличие функции выбора предустановленной политики паролей зависит от версии ОС Аврора.

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.

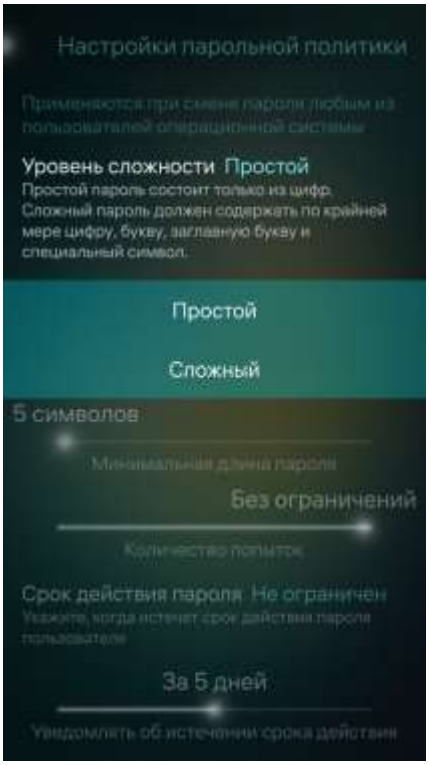

Рисунок 31

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 версии ОС Аврора.

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 ИС, 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):

– 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

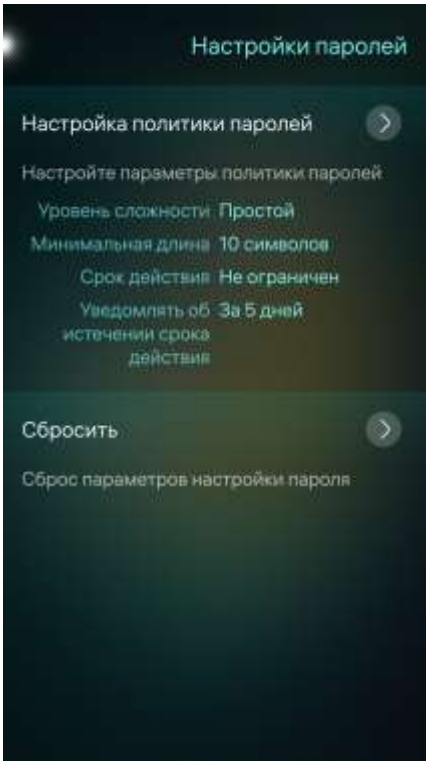

Рисунок 35

Для сброса парольной политики необходимо выполнить следующие действия (Рисунок 35):

– на странице «Настройка паролей» коснуться поля «Сбросить»;

– подтвердить действие вводом текущего кода безопасности.

1.6.3. Настройка безопасности учетной записи 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. 1.6.3.1);
- включить и настроить двухфакторную аутентификацию (2ФА) (п. 1.6.3.2);
- задать одноразовый пароль (п. 1.6.3.3).

1.6.3.1. 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.

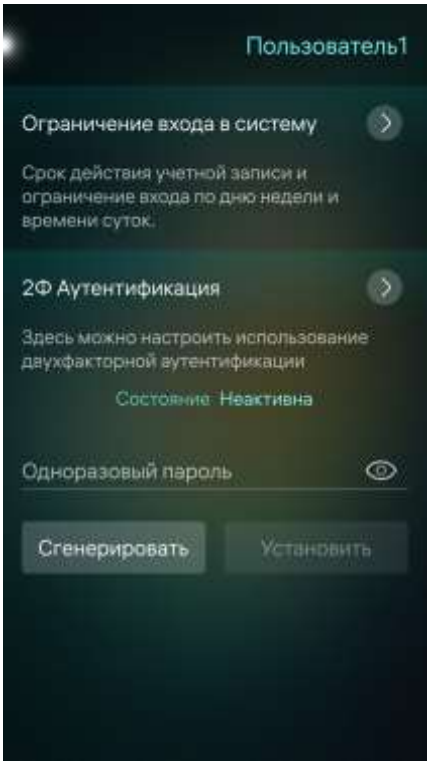

Рисунок 36

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 текущего кода безопасности.

Для выбора 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 текущего 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 текущего кода безопасности.

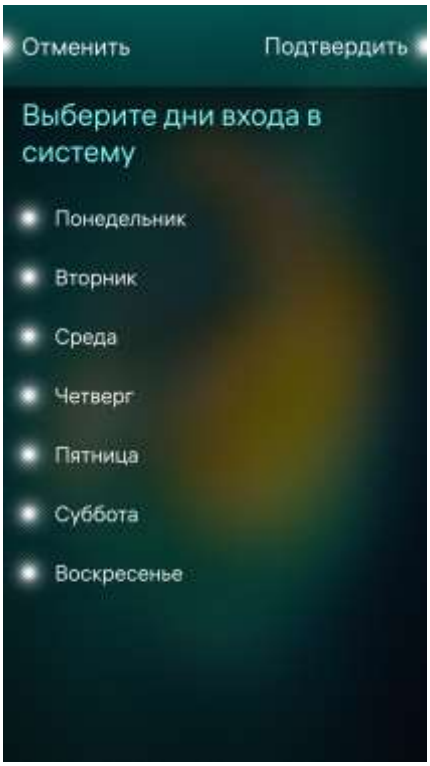

Рисунок 38

Рисунок 39

1.6.3.2. Настройка 2ФА

2ФА – процесс подтверждения подлинности пользователя с помощью применения 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 следует 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 электронно-вычислительной машине (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, 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);

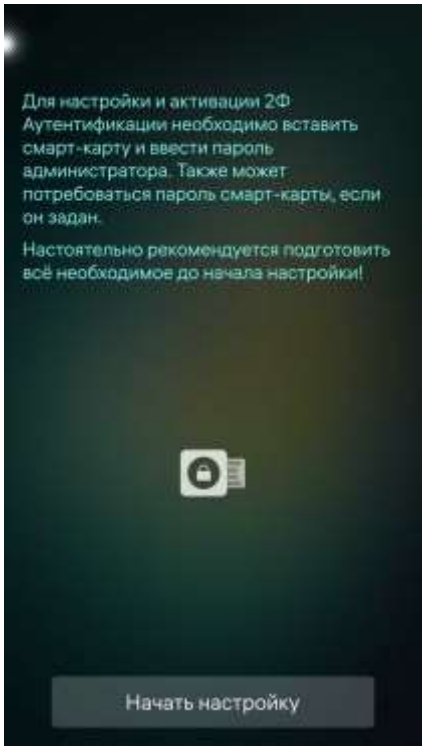

Рисунок 40

Рисунок 41

– на отобразившейся странице «Инициализация смарт-карты» коснуться кнопки «Ввести пароль» для ввода пароля от токена (смарт-карты) либо коснуться кнопки «Попробуйте другую смарт-карту» для подключения другого токена (Рисунок 42)

– в поле ввода ввести пароль от токена(смарт-карты) и коснуться значка » (Рисунок 43);

Рисунок 42

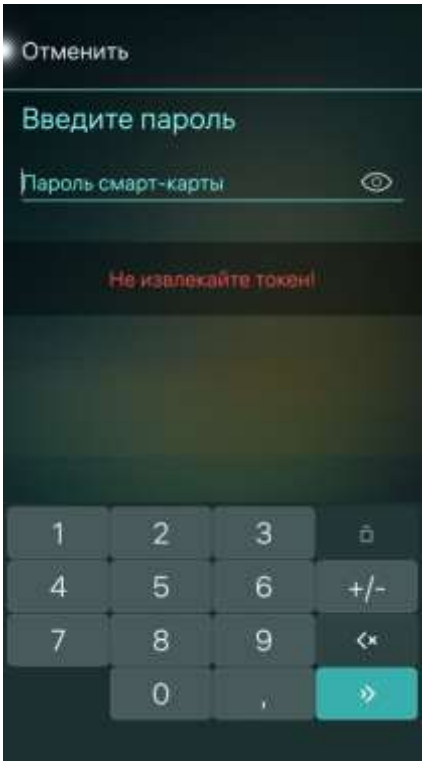

Рисунок 43

– после успешной инициализации токена (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).

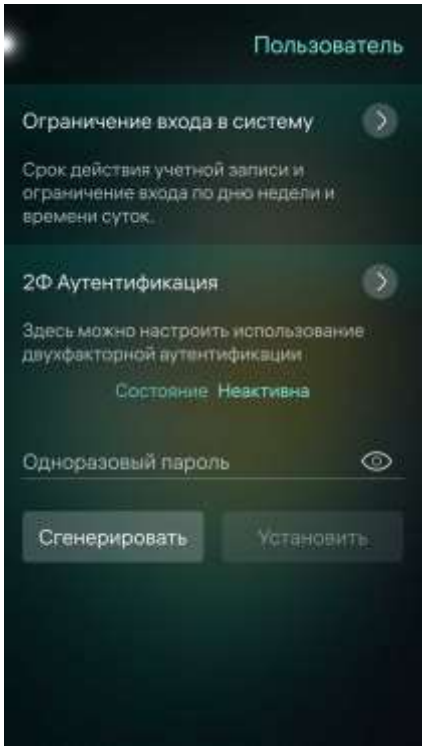

Рисунок 46

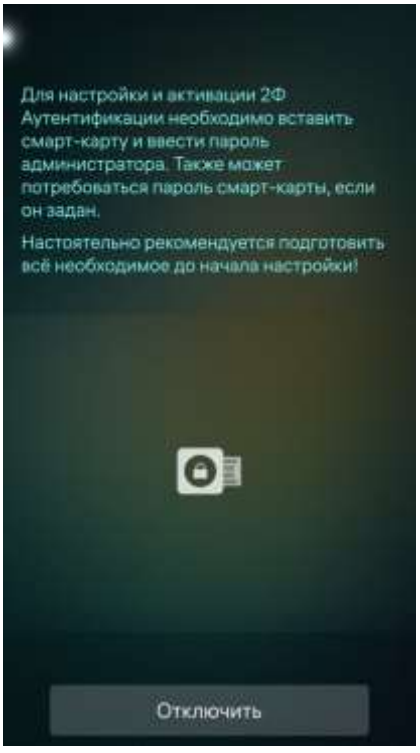

Рисунок 47

1.6.3.3. Задание одноразового пароля для учетной записи пользователя

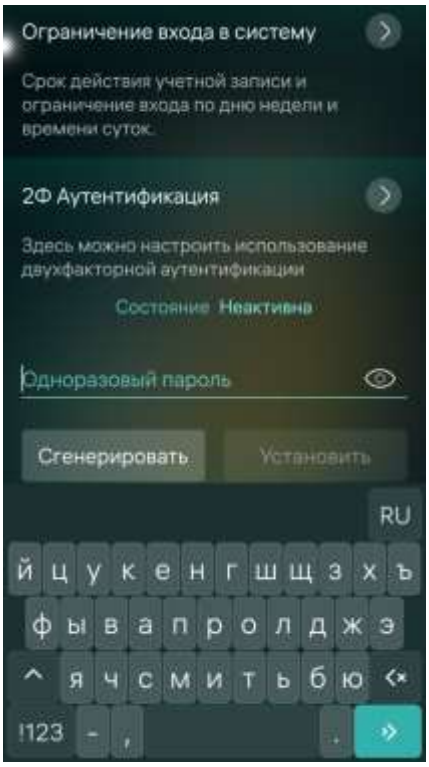

Рисунок 48

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 текущего кода безопасности.

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

1.7. Настройка МУ

Администратору МУ доступны следующие возможности:

– настройка USB-подключения (п. 1.7.1);

– настройка PIN-кода для SIM-карты (п. 1.7.2);

– настройка МП (1.7.3).

1.7.1. 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).

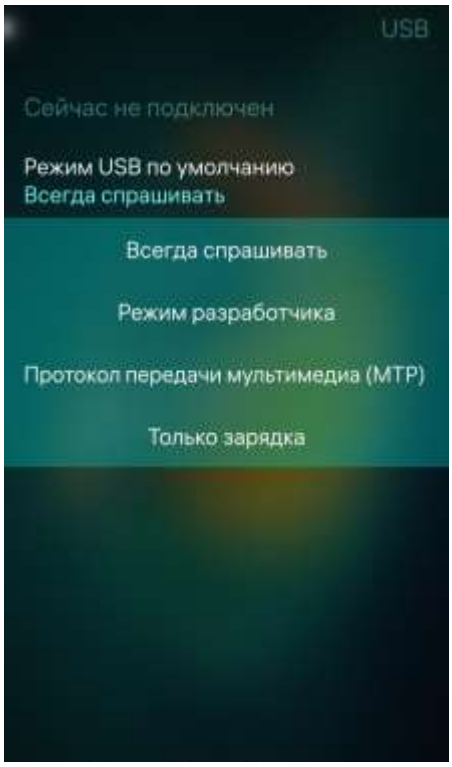

Рисунок 49

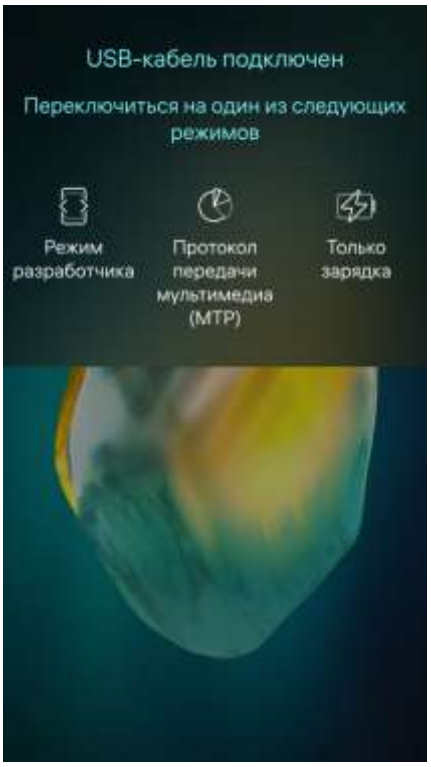

Рисунок 50

1.7.2. 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.

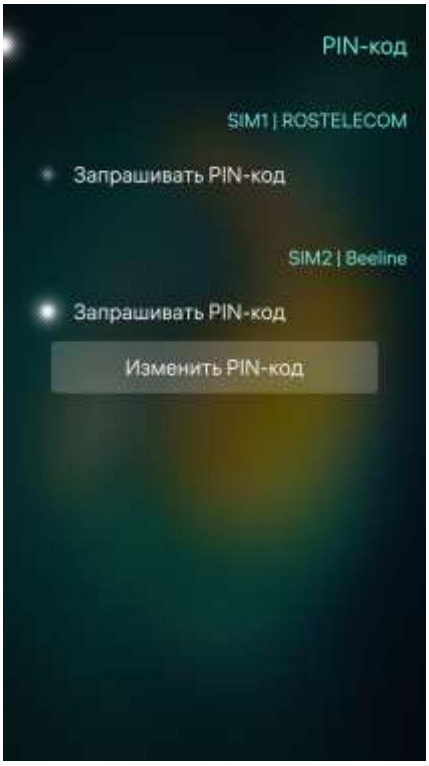

Рисунок 51

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 потребуется 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 (см. 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

1.7.3. 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

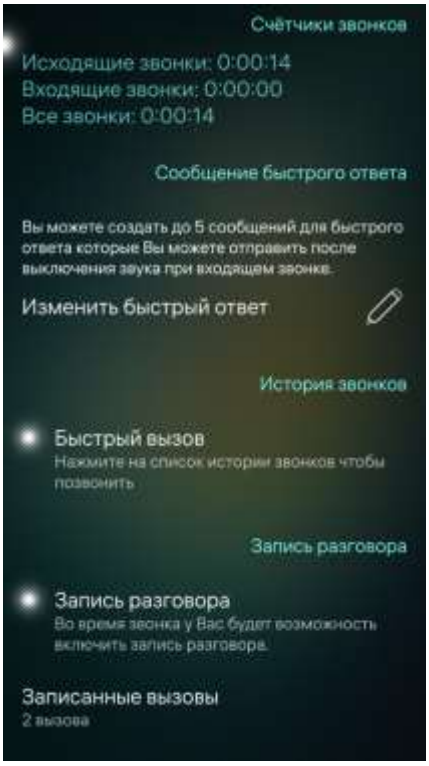

Рисунок 55

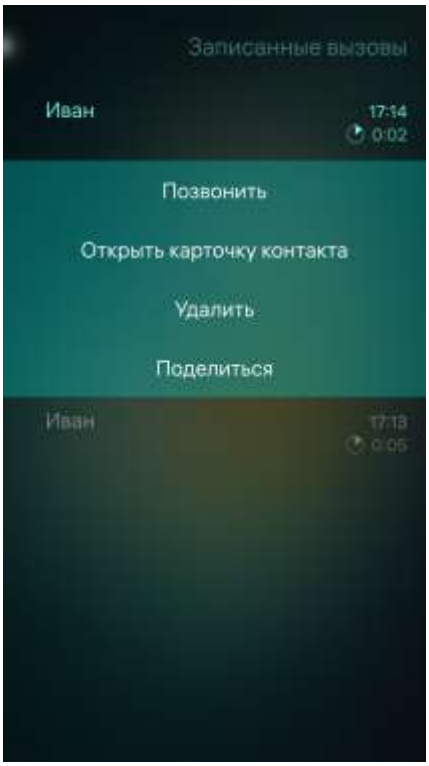

Рисунок 56

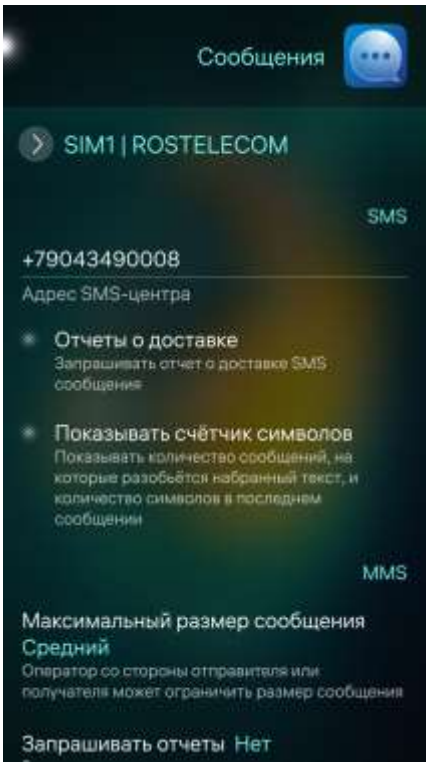

Рисунок 57

2. ВЫПОЛНЕНИЕ ПРОГРАММЫ

2.1. Настройка обновлений ОС Аврора

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

ПРИМЕЧАНИЕ. Для получения информации по обновлению ОС Аврора с использованием ППО следует обратиться к соответствующей документации на ППО, размещенной на веб-сайте: https://auroraos.ru/documentation/.

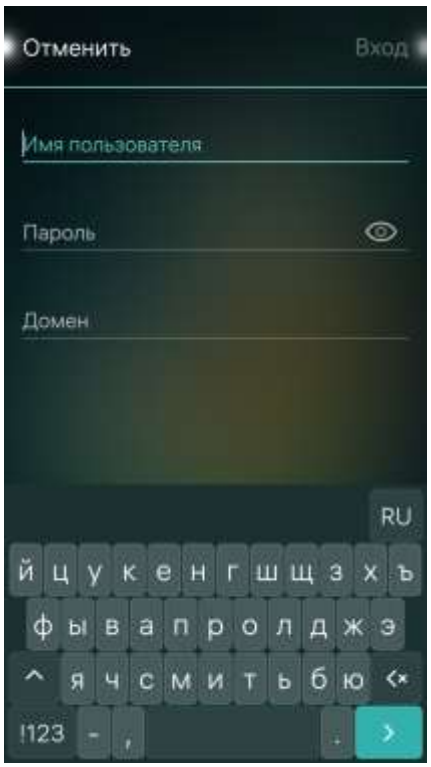

Рисунок 58

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» (Рисунок 59);

ВНИМАНИЕ! Для получения имени пользователя и пароля необходимо обратиться на электронную почту: 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);

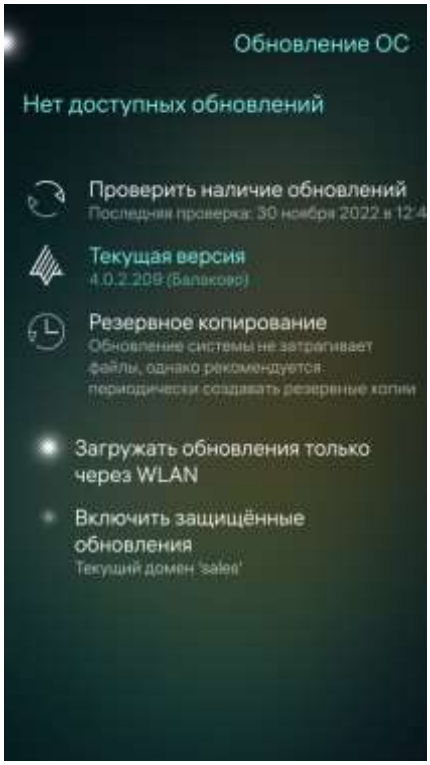

Рисунок 59

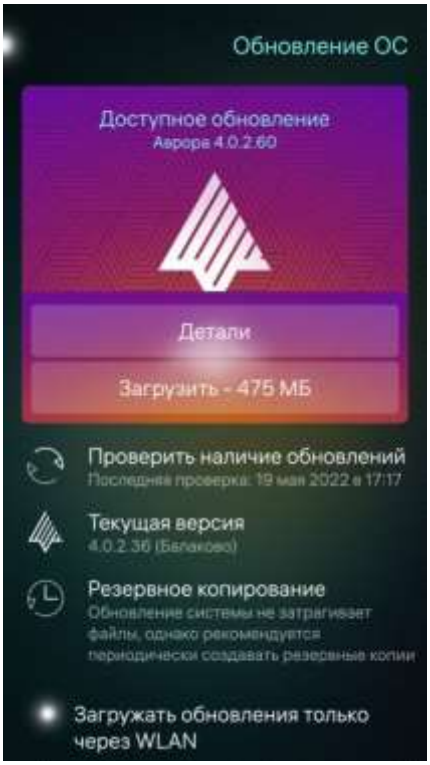

Рисунок 60

– 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).

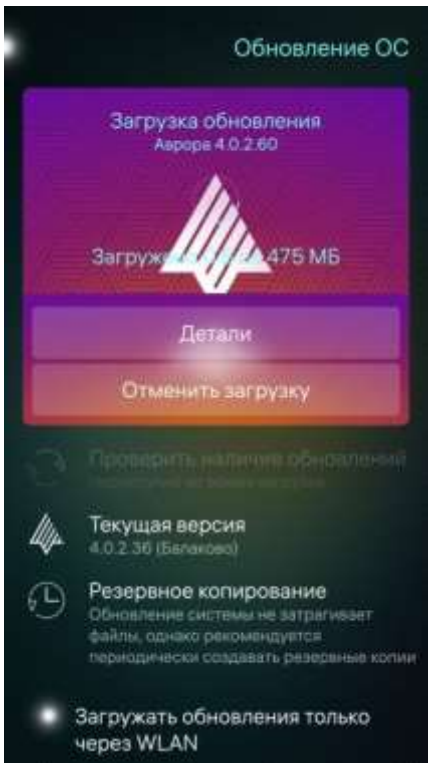

Рисунок 61

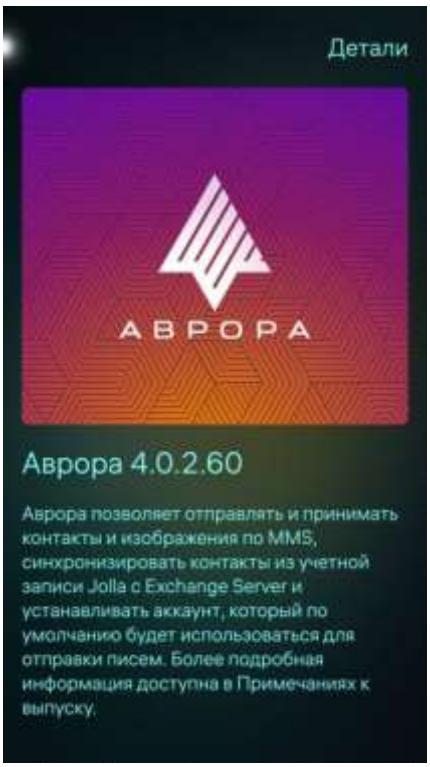

Рисунок 62

– 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.

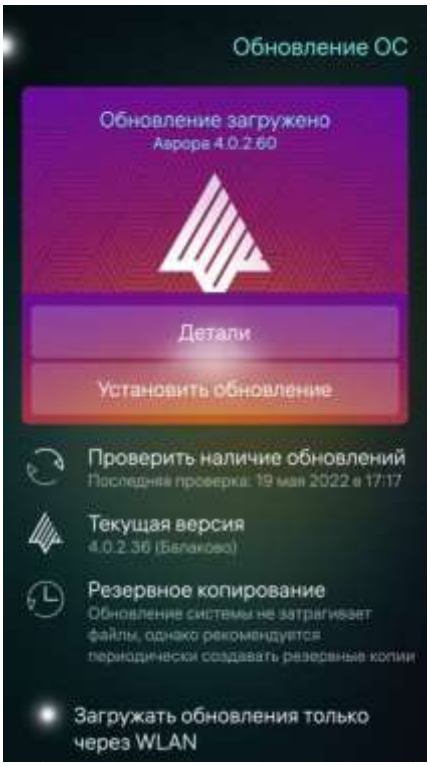

Рисунок 63

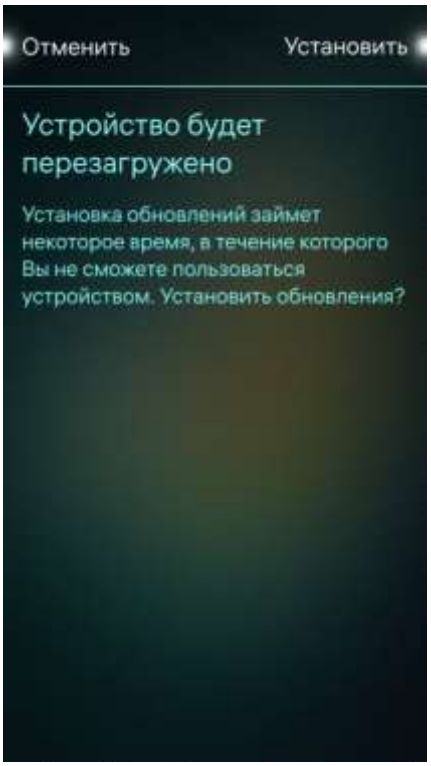

Рисунок 64

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».

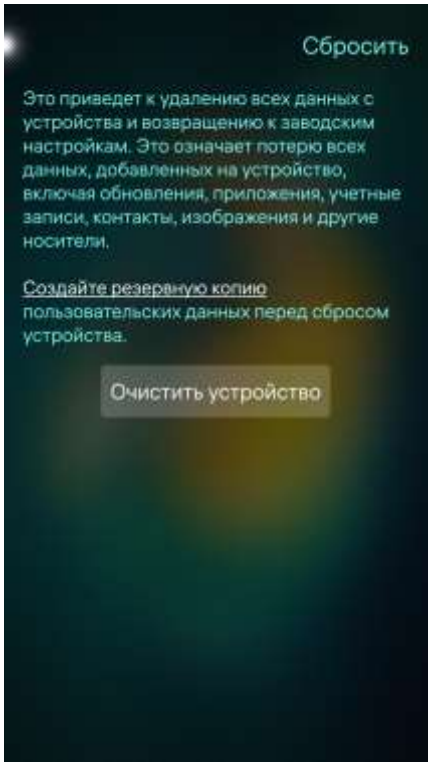

Рисунок 65

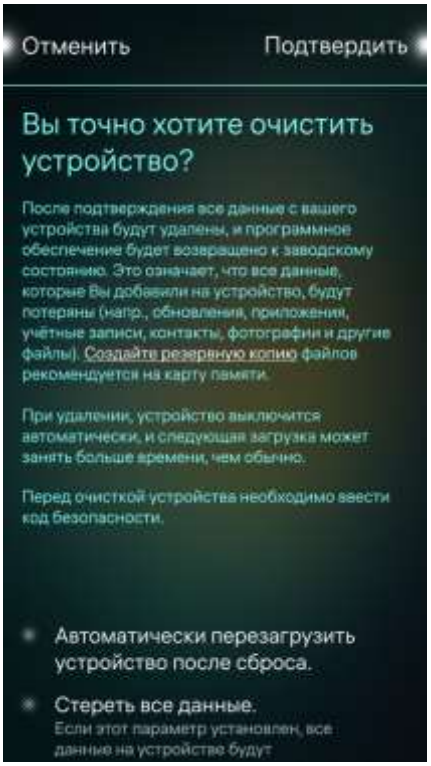

Рисунок 66

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.

Тонкая настройка предназначена для выполнения сервисных операций, недоступных из графического интерфейса (например, настройка прав доступа, исправление конфигурационных файлов и т.д.)

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).

ПРИМЕЧАНИЕ. 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 (см. Рисунок 8).

ПРИМЕЧАНИЕ. МП «Terminal» доступно только администратору.

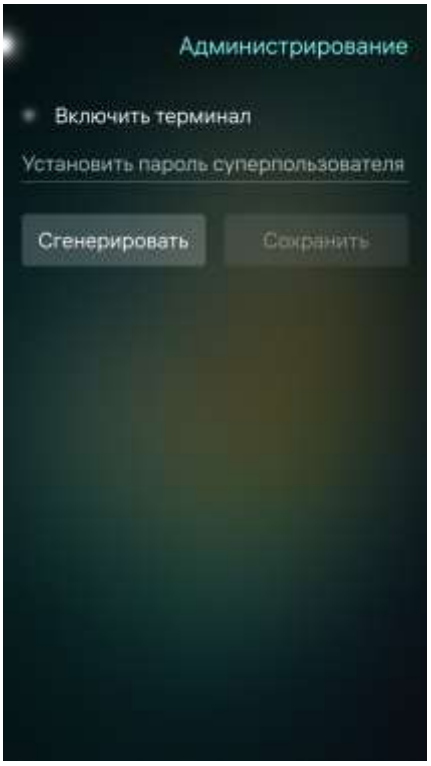

Рисунок 67

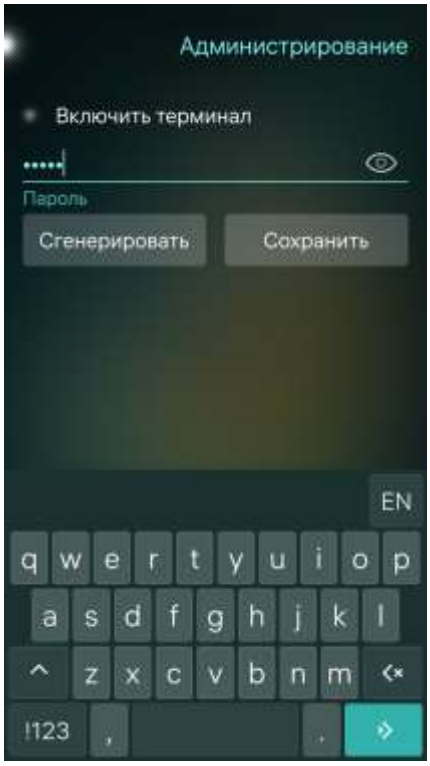

Рисунок 68

2.3.1. Интерфейс МП «Terminal»

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

В интерфейсе МП «Terminal» необходимо коснуться значка  для отображения меню с настройками интерфейса, в котором доступны следующие возможности (Рисунок 69):

- копирование или вставка фрагментов текста;
- поиск URL-ссылок;
- создание нового окна;
- выбор языка интерфейса;
- просмотр информации о МП «Terminal»;
- увеличение и уменьшение размера шрифта;
- выбор ориентации окна;

Рисунок 69

– выбор действия при касании экрана;

– выбора способ отображения клавиатуры;

– установка времени задержки клавиатуры.

ПРИМЕЧАНИЕ. Выполнение данных действий осуществляется посредством касания соответствующих кнопок.

2.3.2. Получение прав суперпользователя

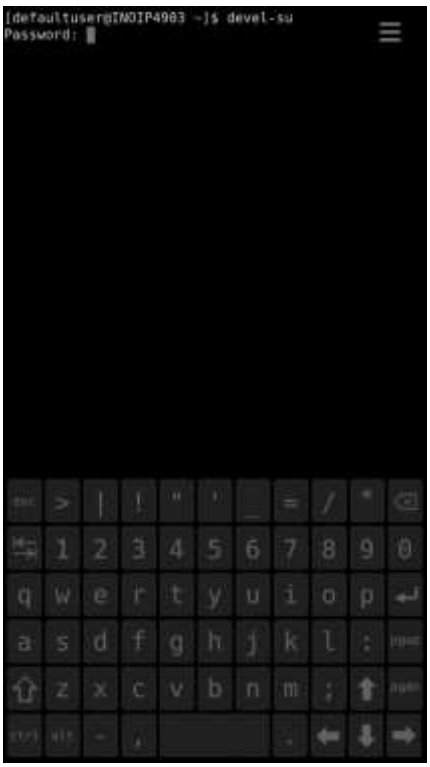

Рисунок 70

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 (Рисунок 70):

– 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 веб-сайте: 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 веб-сайте: https://auroraos.ru/documentation/.

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

При установке сторонних МП администратору необходимо убедится в выполнении следующих условий:

– пакет программ устанавливается штатным образом;
– необходимые исполняемые файлы программы запускаются;
– штатное поведение и выполнение программы сохраняется и после перезагрузки ОС Аврора.

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.

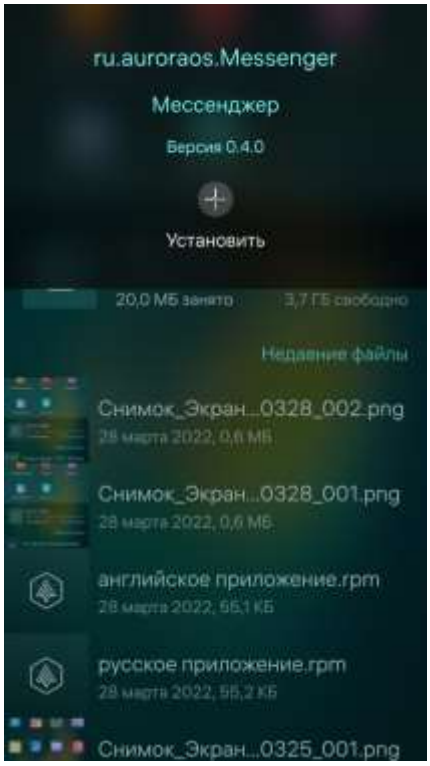

Рисунок 71

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
```

– для подробного ознакомления с возможностями менеджера RPM-пакетов:

```
#rpm -help
```

ПРИМЕЧАНИЕ. Для получения информации о возникающих ошибках и нештатных 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 веб-сайте: https://community.omprussia.ru.

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

– добавить корневой сертификат УЦ в доверенные (пп. 2.4.2.1-2.4.2.2);
– проверить сертификаты (пп. 2.4.2.3);
– подписать МП (пп. 2.4.2.4);
– проверить подпись МП (пп. 2.4.2.5);
– проверить подпись RPM-пакета (пп. 2.4.2.6);
– запустить МП (пп. 2.4.2.7).

2.4.2.1. Общая информация

Для установки стороннего ПО на МУ, функционирующее под управлением ОС Аврора, RPM-пакет должен иметь следующие подписи:

– подпись разработчика, которая является обязательной и позволяет идентифицировать автора пакета, а также используется для подписи пакета и исполняемых файлов внутри него. Без данной подписи невозможно установить МП на МУ, функционирующее под управлением ОС Аврора;

– подпись клиента, которая дополнительно защищает и контролирует установку стороннего ПО на МУ, функционирующем под управлением ОС Аврора. Все МП, которые будут использоваться предприятием-разработчиком, необходимо подписывать данной подписью.

ПРИМЕЧАНИЕ. На МУ, функционирующее под управлением ОС Аврора, можно установить только ПО, прошедшее внутренний контроль и подписанное собственной подписью клиента.

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

Назначение	Алгоритм	Имя файла закрытого ключа по умолчанию	Имя файла запроса на сертификат по умолчанию	Имя файла сертификата по умолчанию
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 веб-сайте: 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 (MTP)», перенести на МУ сертификат УЦ;

– запустить 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 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 следует 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 сертифицированной версии и предназначенном для использования в ИС, 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 текущего 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

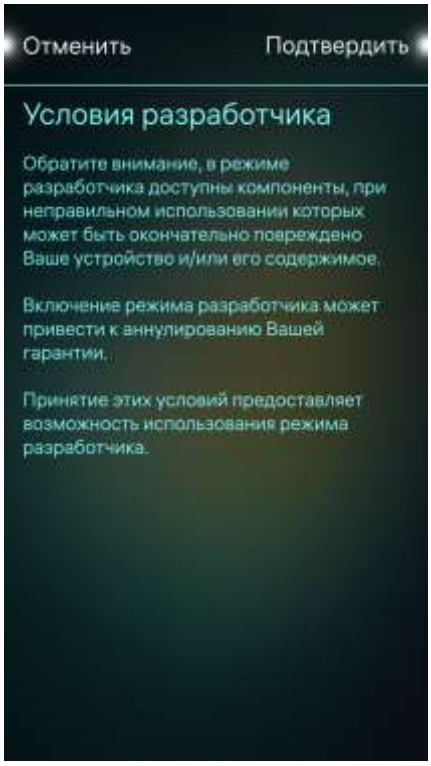

Рисунок 74

3.2. Инструменты разработчика

Для работы с инструментами разработчика необходимо выполнить следующие действия:

– активировать режим разработчика (подраздел 3.1);

– разрешить вход по SSH-паролю, коснувшись переключателя «Удаленное соединение» (Рисунок 75) и подтвердив действие вводом текущего кода безопасности;

– задать либо сгенерировать пароль, коснувшись поля «Сгенерировать», после чего коснуться кнопки «Сохранить» и подтвердить действие вводом текущего 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);

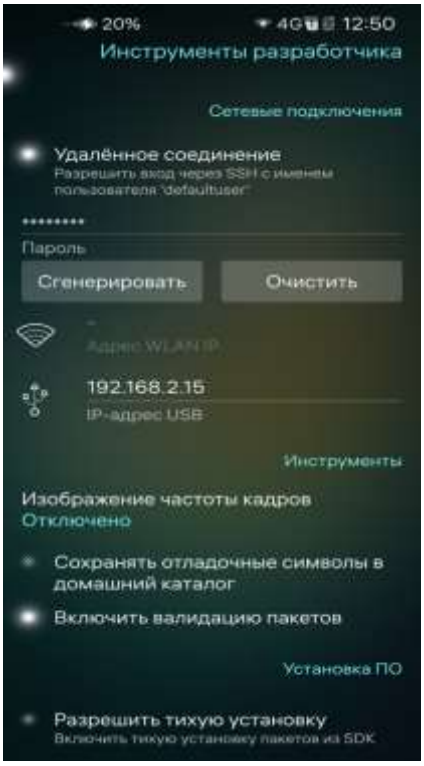

Рисунок 75

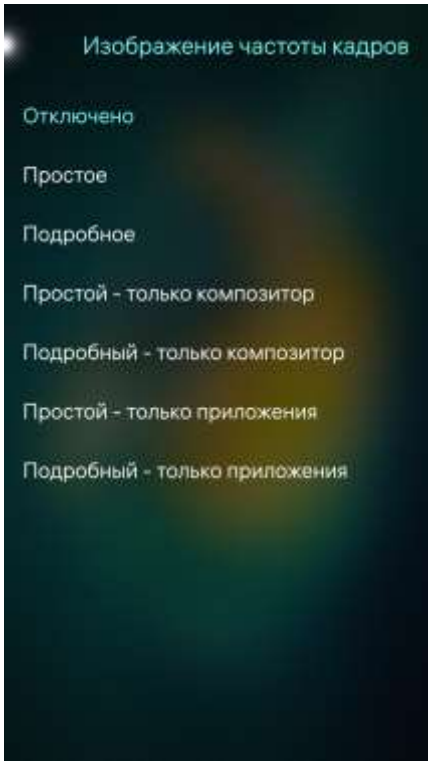

Рисунок 76

– 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 текущего кода безопасности.

4. ОПИСАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ

ОС Аврора представляет собой программное средство общего назначения, предназначенное для эксплуатации в составе государственных информационных (автоматизированных) систем до первого класса защищенности включительно. Может также использоваться для обработки персональных данных в составе ИС систем персональных данных до первого уровня защищенности включительно. Кроме того, ОС Аврора предназначена для запуска различных пользовательских МП и программ для решения разнообразных повседневных и/или служебных задач в интересах ее потребителей.

ОС Аврора реализует следующие функции безопасности:

– идентификация и аутентификация;
– управление доступом (политики безопасности);
– регистрация событий безопасности (аудит);
– ограничение программной среды;
– изоляция процессов;
– защита памяти;
– контроль целостности (КЦ);
– обеспечение надежного функционирования;
– фильтрация сетевого потока.

Каждая функция безопасности настраивается с помощью соответствующих интерфейсов. Описание соответствующих настроек и интерфейсов приводится в следующих разделах:

– управление учетными записями – описывает создание, модификацию и удаление учетной записи пользователя;

– настройка аутентификации – описывает все возможные настройки аутентификационной информации;

– настройка паролей – описывает настройки политики паролей, сроки их действия, устаревания и т. п;

– настройка двухфакторной аутентификации– описывает процесс инициализации и входа учетных записей пользователей ОС Аврора с применением второго фактора для подтверждения подлинности;

– управление разграничением доступа – описывает применение различных ограничений, связанных с установкой политик разграничения доступа к мобильным приложениям (МП) и файлам (папкам), настройкой управления информационными потоками и настройкой разнообразных ограничений функций ОС Аврора;

– управление дискреционным разграничением доступа – описание настройки ограничений, применяемых для файлов, папок и МП;

– управление информационными потоками – описание настроек межсетевого экрана ОС Аврора;

– управление политиками безопасности – описание настроек, связанных с управлением функциями ОС Аврора, такими как возможности использования настроек времени, Bluetooth®, WLAN и т.п.;

– управление ПО – описание менеджера пакетов;

– управление ограничениями программной среды – описание настроек лимитов на вычислительные ресурсы и т.п;

– управление функциями очистки остаточной информации – описание настроек, необходимых при осуществлении операций гарантированного удаления;

– контроль целостности – описание использования механизмов КЦ;

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

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 КЦ;
- 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 шифрованном 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:

– программы `journalctl` и `dmesg`, имеющие интерфейс командной строки;
– конфигурационный файл `/etc/omp/sdjd.conf`;

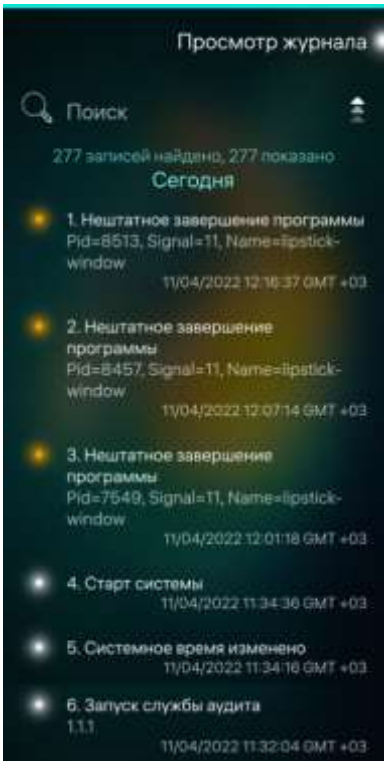

Рисунок 77

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

- запуск выполнения службы аудита;
- старт проверки КЦ;
- 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».

4.1.4. Отчет

Отчет имеет формат tar.bz. Имя отчета имеет следующую маску: reports-YYYYMMDD-HHMMSS.tar.bz.

Подробная информация о создании отчета приведена в документе «Руководство пользователя».

4.1.5. Зашифрованный отчет

Зашифрованный отчет имеет формат tar.bz.cms. Имя зашифрованного отчета имеет следующую маску: reports-YYYYMMDD-HHMMSS.tar.bz.cms. Дополнительно формируется файл с информацией о сертификате, публичный ключ которого был использован для шифрования отчета. Он создается рядом и имеет формат txt: reports-YYYYMMDD-HHMMSS.tar.bz.txt. Время создания у этих файлов в названии идентичное.

Пример файла с информацией:

```
cat reports-20220329-104949.tar.bz2.txt
Subject: OMP Test
Group: developer
Subgroup: regular
Key ID:
7003efe7156bd53a2e88c2cb3c0d43e9786760c53721933dd5052fdaf443dbfb
```

Подробная информация о создании зашифрованного отчета приведена в документе «Руководство пользователя».

4.1.5.1. Расшифровка отчета

Отчет можно расшифровать соответствующим ключом и сертификатом (см. колонку «SKID» в таблице с сертификатами, если ключ боевой, то нужно спрашивать коллег, чтобы его расшифровали) с помощью openssl (должен быть подключен гостовый движок):

```
openssl cms -decrypt -in /home/defaultuser/Documents/reports-
20220228-173753.tar.bz2.cms -recip system-developer-cert.crt  -inkey
system-developer-key.pem -inform DER > reports-20220228-173753.tar.bz2
```

4.1.5.2. Шифрование

Используется блочное шифрование GOST 28147-89.

4.1.5.3. Текущий набор модулей

Текущий набор модулей, используемый в зашифрованном отчете, приведен в таблице (Таблица 2).

Таблица 2

Модуль	Описание
available-packages	Список доступных и установленных пакетов
battery	Информация об аккумуляторе
bluetooth	Информация о Bluetooth®
cellular	Информация SIM-картах
disks	Информация о дисках и занятом/свободном пространстве
dmesg	Лог ядра
emm	Папка /etc/emm
info	Общая информация об устройстве: – контрольные суммы загрузочного раздела; – информация об AIDE; – список функций; – информация о релизе ОС; – информация о HW релизе ОС; – версия ядра
internet	Информация об активном Интернет-соединении
logcat	Системные сообщения
memory	Информация о памяти
mount-points	Текущие точки монтирования
policy	Папка /etc/policy
process-list	Текущие список процессов
push-daemon	Папки /etc/xdg/push-daemon и /var/lib/push-daemon
rpms	Список установленных пакетов
screen	Информация об экране
sdjd	События безопасности

Модуль	Описание
ssu	Информация о репозиториях
systemboot	Информация о системной загрузке
system	Краткая информация о системе: – режим экономии заряда аккумулятора; – подключение к мобильной сети/сети Интернет; – статус подключения; – активность WLAN
systemctl	Список сервисов
system-journal	Системный журнал

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 корпоративной версии ОС Аврора пользователю будет необходимо установить код безопасности для доступа к МУ;

– в сертифицированной версии ОС Аврора 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.

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`, `kexec` 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 атмосфер
3	AppLaunch	Запуск и остановка сервисов `systemd`
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 разговорам
9	Camera	Доступ к камере, съемка фото и видео
10	CommunicationHistory	Доступ к истории вызовов и сообщений
11	Contacts	Просмотр и модификация данных контактов

№	Элемент	Описание
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
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 о МУ
32	LogSecurityEvents	Запись в регистрационный журнал
33	PushNotifications	Чтение push-уведомлений
34	Reports	Генерирование архива с системными отчетами
35	SecureStorage	Хранение шифрованных файлов
36	UserStatus	Извлечение списка пользователей системы

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).

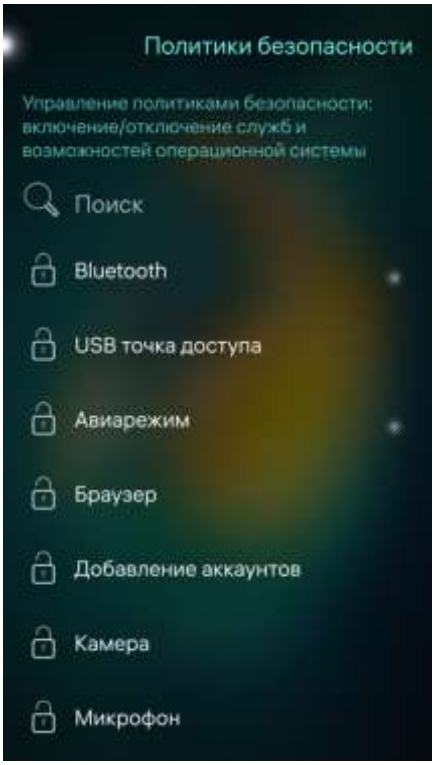

Рисунок 78

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 4).

Таблица 4

№	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

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
4	Настройки WLAN	Использование сети WLAN	WlanToggleEnabled	Разблокирована	GUI
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	Настройка прокси-	NetworkProxyS	Заблокирована	GUI

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
	прокси	сервера	ettingsEnabled		
19	Установка приложений	Установка МП	ApplicationInstallationEnabled	Заблокирована	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. 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 которым 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.

4.5. 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 secdel, который очищает на носителе неиспользуемые блоки ФС непосредственно при их освобождении с помощью перезаписи их маскирующей последовательностью.

4.6. Подписи RPM-пакетов

Каждый RPM- пакет имеет название, состоящее из следующих частей:

– название программы;

– версия программы;

– номер выпущенной версии. Обозначает количество пересборок программы одной и той же версии или дистрибутив, под который собран RPM-пакет (например, mdv (Mandriva Linux) или fc4 (Fedora Core 4));

– архитектура, под которую собран RPM-пакет (armv7hl, i386, ppc и т. д.).

Собранный RPM-пакет обычно имеет следующий формат названия:

```
<название>-<версия>-<релиз>.<архитектура>.rpm
```

Например:

```
nano-0.98-2.i386.rpm
```

RPM-пакет может содержать только исходные коды, при этом информация об архитектуре отсутствует и заменяется на src.

Например:

```
libgnomeuimm2.0-2.0.0-3.src.rpm
```

Библиотеки, как правило, распространяются в двух отдельных пакетах: первый содержит собранный код, второй (обычно к нему добавляют `-devel`) содержит заголовочные файлы, а также файлы, требуемые для разработки.

Необходимо, чтобы версии двух пакетов совпадали, в противном случае библиотеки могут работать некорректно. Пакеты с расширением `noarch.rpm` не зависят от конкретной архитектуры устройства. Обычно они содержат графику, архитектурно-независимые скрипты и тексты, используемые другими программами.

RPM-пакет обеспечивает:

– легкость удаления и обновления программ;

– популярность – т.к. многие программы собираются именно в RPM, отсутствует необходимость сборки программы из исходных кодов;

– «неинтерактивную установку» - процесс установки/обновления/удаления легко автоматизируется;

– проверку целостности пакетов с помощью КС и подписей;

– DeltaRPM - аналог патча, позволяющий обновить установленное ПО с минимальной затратой трафика;

– возможность аккумуляции опыта сборщиков в spec-файле;

– относительную компактность spec-файлов за счет использования макросов.

Специфика работы RPM-пакетов в составе ОС Аврора связана с переработанным механизмом КЦ.

ПРИМЕЧАНИЕ. В составе ОС Аврора допускается установка только подписанных RPM-пакетов. Неподписанные пакеты не могут быть установлены.

Подпись RPM-пакета проверяется в момент его установки и хранится в ОС Аврора после окончания процесса установки в особой БД, называемой OMPCERT. Подписи RPM-пакета формируются с помощью алгоритма по ГОСТ Р 34.10-2012.

– функции хеширования и длиной хеш-кода 256 бит по ГОСТ Р 34.11-2012;

– дату подписания пакета;

– подпись указанных выше полей с применением алгоритма ГОСТ Р 34.10-2012 и функции хеширования ГОСТ Р 34.11-2012, длина выхода 256 бит;

– сертификат субъекта подписи пакета.

Для проверки подписи в процессе установки RPM-пакета имеет значение структура и состав сертификата ключа проверки ЭП. Сертификат должен быть выдан клиенту (субъекту) компанией предприятия-разработчика.

Процесс получения субъектом сертификата состоит из следующих этапов:

– генерация ключевой пары, защищенной паролем. Подробная информация приведена на веб-сайте: https://community.omprussia.ru/;

– создание запроса на сертификат с указанием в обязательном порядке наименования клиента;

– отправка запроса на получение сертификата предприятию-разработчику и получение сертификата с присвоенной меткой группы безопасности;

– подписание RPM-пакета, полученного сертификата и защищенного ключа подписи;

Метка группы безопасности является строкой и может быть произвольной, однако при выдаче сертификата Разработчик ОС Аврора использует определенный набор меток. Обработка подписанного пакета зависит от присвоенной сертификату метки группы безопасности по правилам, изложенным ниже.

В начале эксплуатации ОС Аврора не связана с каким-либо субъектом. При установке первого пакета ключ клиента (client certificate key id) устанавливается в ОС Аврора, при этом в ОС Аврора создается привязка ОС Аврора к клиенту (субъекту).

ПРИМЕЧАНИЕ. На ОС Аврора устанавливается только подписанный клиентом RPM-пакет.

В дальнейшей эксплуатации механизмы для изменения привязки не предусмотрены. В этом случае необходимо предпринять одно из следующих действий:

– переустановить ОС Аврора;

– установить пакет, который удаляет привязку, после чего повторно привязать ОС Аврора к клиенту с помощью пакета, который должен быть подписан клиентом (к клиенту должен быть привязан экземпляр ОС Аврора).

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;

– подпись клиента подписывает область подписи разработчика;

– каждая последующая подпись добавляется в конец и подписывает предыдущую.

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

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

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

При отзыве скомпрометированных ключей происходит отзыв ключа, а не сертификата.

В целях разделения зоны и поддержания глубины интеграции сторонних RPM-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.

В целях упрощения процесса у разработчика сохраняется возможность отключения валидации пакетов, однако при этом основные критические для системы проверки останутся активными.

Группы (метки) безопасности пакетов: после привязки экземпляра ОС Аврора невозможна установка RPM-пакетов, неподписанных клиентом или подписанных другим клиентом, поэтому особое внимание должно уделяться первому подписанному пакету.

RPM-пакет является подписанным клиентом, если сертификат последней подписи пакета имеет метку группы безопасности `client`.

Группы безопасности:

– обязательная подпись разработчика, метка – `developer`;

– опциональная подпись специализированной лаборатории, утверждающая безопасность пакета, метка – `seclab`;

– обязательная подпись клиента, метка – `client`.

Подписи накладываются следующие образом: сначала разработчик подписывает RPM-пакет, который он произвел. Далее (по желанию) пакет с подписью разработчика может быть направлен в лабораторию для дополнительной независимой проверки. В этом случае лаборатория подписывает пакет с подписью разработчика своим ключом. Затем для успешной установки в ОС Аврора пакет в обязательном порядке должен быть подписан клиентом (владельцем ОС Аврора, субъектом).

При этом разработчик подписывает сам RPM-пакет, а каждый последующий субъект подписывает предыдущую подпись (т.е. лаборатория подписывает подпись разработчика, клиент подписывает подпись лаборатории), тем самым организована иерархия подписей, в которой на каждом из этапов проверки можно выявить расхождения.

Корневой сертификат предприятия-разработчика: для установки доверия между сертификатами и системой предлагается иерархическая связь между сертификатами, которые используются для подписи пакетов. Разработчик ОС Аврора генерирует посредством утилиты `tk26sig` сертификат, который считается корневым. Далее Разработчик ОС Аврора, используя данный сертификат, выдает сертификаты своим клиентам на основе их запроса на сертификат (CSR) — это могут быть ключи разработчика, клиента и любые другие. Таким образом, всегда возможно проследить связь между цепочкой сертификатов: если выданный клиентам сертификат не выдан Разработчиком ОС Аврора, такой сертификат считается недействительным, соответственно, все попытки установить RPM-пакеты, подписанные сертификатами, не выданными Разработчиком ОС Аврора, будут неудачными.

Путь до корневого сертификата зашит программно: `/etc/rpm/rootcacert-omp.pem`.

Сертификат разработчика: среди всех сертификатов для группы `developer` наиболее важным является сертификат, выданный Разработчику ОС Аврора для разработки ОС Аврора. Такими сертификатами, как правило, подписываются все продукты Разработчика ОС Аврора и все системные пакеты. Если какой-либо пакет подписан данным сертификатом, он не подвергается процессу валидации (т.к. считается, что эти пакеты всегда являются доверенными). Для отличия сертификатов идентификатор публичного ключа сертификата устанавливается в ФС по пути `/etc/rpm/system-developer-keyid` и при установке каждого пакета происходит сверка публичного ключа сертификата разработчика, которым подписан пакет с ключом, расположенным в ФС.

Внутренняя структура подписей: подписи файла IMA интегрируются в блок подписи разработчика, подпись IMA переносится из заголовка пакета.

Только первая подпись (не весь файл) заверяется второй подписью, что положительно влияет на производительность.

Секции RPM-пакета: общий формат подписанного RPM приведен на рисунке (Рисунок 79).

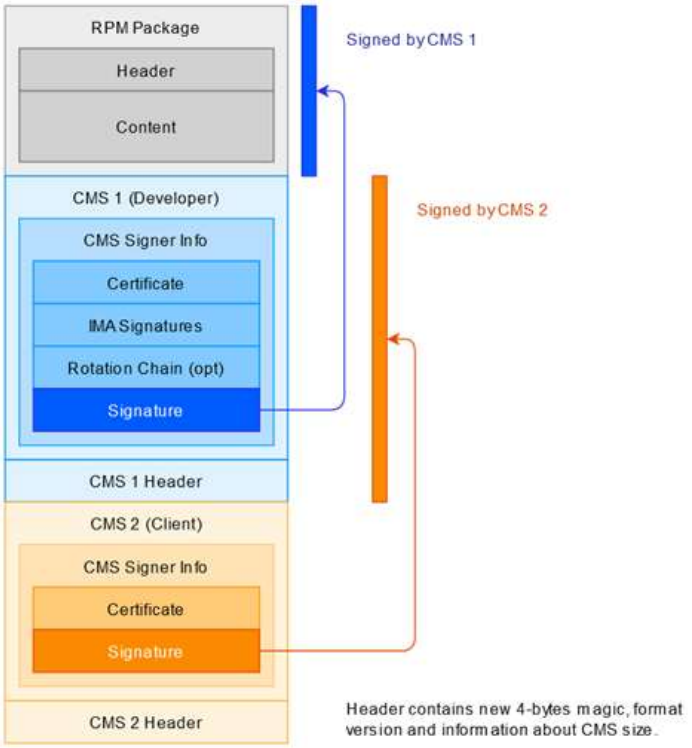

Рисунок 79

Валидация RPM-пакетов: пакеты валидируются (проверяются на корректность) сценарием, находящимся в проекте `rpm-validator`. Процесс валидации проходят не все пакеты, а только те, которые не удовлетворяют условиям по безопасности. Пакеты, подписанные ключом Разработчика ОС Аврора, не проходят процесс валидации. Данное решение было принято для возможности корректного обновления пакетов, входящих в состав ОС Аврора.

При установке через `librpm` RPM-пакет проходит следующие стадии:

– внутренние проверки RPM-пакетов;

– валидация плагином `rpm-plugin-validation`.

Плагин rpm-plugin-validation, вызванный перед установкой пакета, выполняет следующие проверки (по порядку):

– проверка подписей и сертификатов пакета;

– проверка привязки системы к определенному клиенту, и в случае ее отсутствия выполняется попытка привязки к клиенту, подпись которого стоит на RPM-пакете. Отсутствие подписи трактуется как ошибка установки;

– если пакет является обновлением, то проверяется, что сертификат разработчика не изменился (т.е. не сменился ли разработчик). Изменение сертификата разработчика трактуется как ошибка установки;

– если пакет подписан не Разработчиком ОС Аврора, выполняется валидация пакета. Неуспешная валидация трактуется как ошибка установки;

– выполняется вставка сертификата в системный IMA keyring. Неуспешный процесс трактуется как ошибка установки;

– выполняется вставка информации о подписях и сертификатах пакета в базу данных rpmsign-external. Неуспешный процесс трактуется как ошибка установки.

По завершении обработки RPM-пакета каждое действие создает сообщение аудита в `sdjd` (система аудита Разработчика ОС Аврора), а именно успех или неуспех при установке или удалении пакета.

При неуспешной установке RPM-пакета данные из БД OMPCERT удаляются. Такой механизм реализован в связи с тем, что в `librpm` не существует способа отката транзакции после установки.

При установке любого RPM-пакета необходимо учитывать следующее:

– каждый пакет должен иметь как минимум подпись разработчика пакета и т.н. «подписью клиента», если пакет для установки взят из доверенного источника (например, из магазина приложений);

– исполняемые файлы и загружаемые библиотеки, входящие в состав пакета, также должны быть подписаны ключом при сборке пакета в системе сборки.

4.7. 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.

4.8. Контроль целостности

ОС Аврора отслеживает целостность следующих компонентов ОС Аврора:

– устанавливаемых пакетов ПО (любого устанавливаемого в ОС Аврора пакета) формата .rpm;

– загружаемых внешних модулей уровня ядра;

– всех исполняемых файлов при попытке их запуска;

– разделов (начиная с версии 4).

ПРИМЕЧАНИЯ:

1. Для КЦ указанных компонентов ОС Аврора, как правило, не требуется специальных действий со стороны администратора;

2. Каждый устанавливаемый в ОС Аврора пакет ПО должен иметь цифровую подпись. Описание механизма подписи RPM приведено в подразделе 4.6.

В случае необходимости произвести КЦ произвольного файла, ELF-файла или разделов, которые могут объединяться в группы, следует использовать утилиту `integrityd` (начиная с версии 4), доступную в терминальном режиме. В отличие от других инструментов, `integrityd` использует электронную подпись (IMA и secureboot) как источник доверия.

Перед выполнением КЦ требуется обратить внимание на следующее:

– проверка целостности указанных файлов по умолчанию производится каждый раз при загрузке ОС Аврора, а также в 00 часов один раз в сутки;

– время загрузки ОС Аврора увеличивается пропорционально количеству файлов, требуемых для проверки целостности, т.е. чем больше список файлов на проверку, тем дольше по времени длится проверка целостности;

– при проверке целостности выполняются математические операции. Это приводит к повышению использования ресурсов процессора, следовательно, к увеличению расхода заряда МУ.

Получение от сервиса `integrityd` отрицательного статуса проверки целостности системных файлов свидетельствует о нарушении целостности, в результате чего компонент `securityd` блокирует доступ к ОС Аврора. Необходимо передать МУ администратору для переустановки ОС.

ПРИМЕЧАНИЯ:

1. Начиная с релиза 4.0, программный компонент `integrityd` заменяет AIDE и осуществляет подсчет контрольных сумм, который раннее выполнялся компонентами: `securityd` и `libpartitioninfo`.

2. Информация о начале и/или завершении процедуры КЦ, а также о результатах ее выполнения, записывается в системный журнал.

4.9. 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 введения 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.

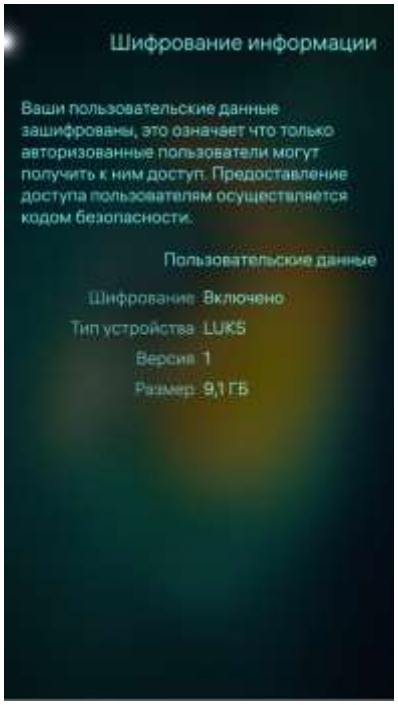

Рисунок 80

Для просмотра информации о шифровании (Рисунок 80) 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 5).

Таблица 5

№	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 предприятия-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: – с использованием ППО «Аврора Центр», развернутой для компании-клиента: внутри периметра организации или у внешнего поставщика (ИТ-интегратора); – 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 на веб-сайте: https://auroraos.ru/documentation); – из графического интерфейса ОС Аврора; – с использованием МП «Terminal»
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. 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) запрещает обновления через интерфейс МУ
6.	МУ заблокировано, требуется код доступа	Необходимо обратиться к администратору МУ либо оператору ППО 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: `telnet 10.12.66.66`; – 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 6).

Таблица 6

Термин/ Сокращение	Расшифровка
Администратор	Пользователь, обладающий правами на выполнение операций, связанных с администрированием системы
Версия ОС Аврора	1. Корпоративная версия - исполнение ОС Аврора, предназначенное для организации доверенных мобильных рабочих мест, на которых не происходит обработка информации, подлежащей защите в соответствии с законодательством РФ; 2. Сертифицированная версия - исполнение ОС Аврора, прошедшее сертификационные испытания в системе сертификации нормативных регуляторов РФ (ФСТЭК России, ФСБ России), имеющее соответствующий комплект программных документов и готовые к серийному производству. Предназначены для организации доверенных мобильных рабочих мест, на которых происходит обработка информации, подлежащей защите в соответствии с законодательством РФ. Могут использоваться в ГИС, на объектах КИИ и в иных регулируемых ИС
2ФА	Двухфакторная аутентификация
ИС	Информационная система
Квота	Объем дискового пространства, выделяемого администратором для записи данных учетных записей пользователей
КЦ	Контроль целостности
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
Пользователь	Лицо, использующее систему для выполнения заложенных в

Термин/ Сокращение	Расшифровка
	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
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 PTP 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
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

Термин/ Сокращение	Расшифровка
RPM-пакет	Файл формата RPM, позволяющий устанавливать, удалять и обновлять приложение на МУ
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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Описание изменения	ФИО	Дата
1.0	Начальная версия	Белянкина Н. Андронова К.	30.11.2022 г.
1.1	Внесены изменения	Белянкина Н. Андронова К.	21.12.2022 г.