РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.3

Листов 69

2022

АННОТАЦИЯ

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

Настоящий документ содержит описание доступных администратору функциональных возможностей мобильного устройства (МУ) с предустановленной ОС Аврора[1].

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

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

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

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

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

При вводе в эксплуатацию МУ с предустановленной ОС Аврора администратор может выполнять следующие основные действия:

– соблюдать ограничения по эксплуатации (подраздел 1.1);
– создавать учетные записи пользователей и управлять ими (подраздел 1.2);
– выполнять настройку безопасности (подраздел 1.3);
– осуществлять дополнительную настройку (подраздел 1.4).

1.1. Ограничения по эксплуатации

Администратору необходимо соблюдать следующие правила и ограничения по эксплуатации МУ с предустановленной ОС Аврора:

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

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

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

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

1.2. Учетные записи ролей

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

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

На МУ 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 администратором, будут применимы ко всем пользователям МУ;

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

- изменение периода спящего режима экрана. Подробное описание настроек спящего режима приведено в документе «Руководство пользователя»;
- изменение допустимого количества попыток ввода кода безопасности (п. 1.3.2);
- изменение времени автоматической блокировки экрана (п. 1.3.1).

По умолчанию при первом включении МУ загружается в режиме администратора

1.2.1. Создание учетной записи пользователя

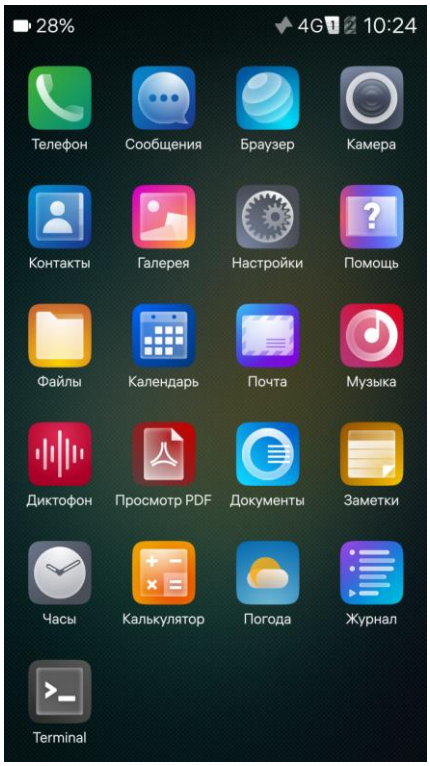

Рисунок 1

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

– открыть меню настроек касанием значка на Экране приложений (Рисунок 1);

– в меню системных настоек коснуться пункта «Пользователи» ;

– на странице «Пользователи» коснуться пункта «Добавить пользователя» (Рисунок 2);

– на отобразившейся странице ввести имя и логин новой учетной записи пользователя (Рисунок 3);

– установить количество выделяемых пользователю ГБ, перемещая соответствующий слайдер вправо для увеличения квоты либо влево для уменьшения (Рисунок 3);

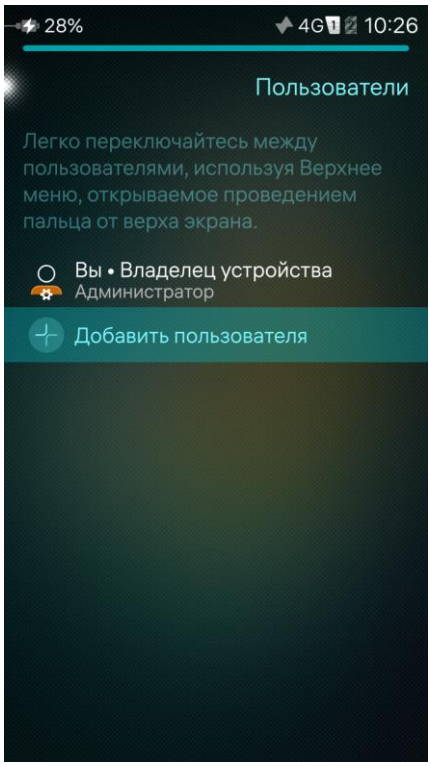

Рисунок 2

Минимальное значение для задания квоты – 2ГБ. Максимальные значения для задания квоты зависят от конструктивных особенностей МУ

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

– в случае необходимости сохранения изменений подтвердить действие вводом кода безопасности, в результате чего на странице «Пользователи» отобразится строка с созданным пользователем (Рисунок 4).

При первом запуске учетной записи пользователя отобразится экран, в котором необходимо задать код безопасности и коснуться значка ✓ (Рисунок 18). Способ задания кода безопасности зависит от варианта исполнения ОС Аврора.

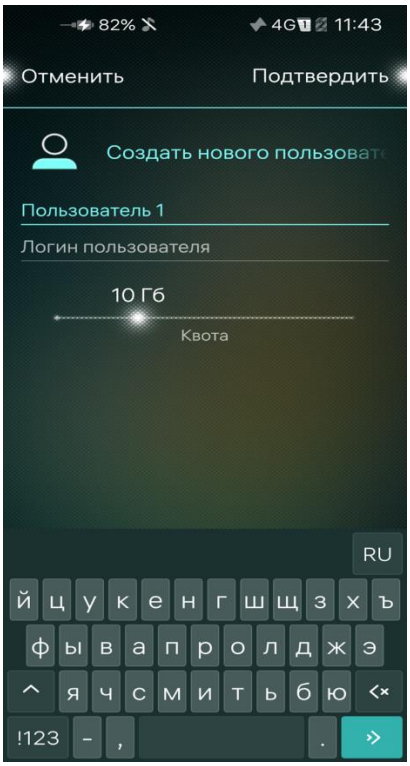

Рисунок 3

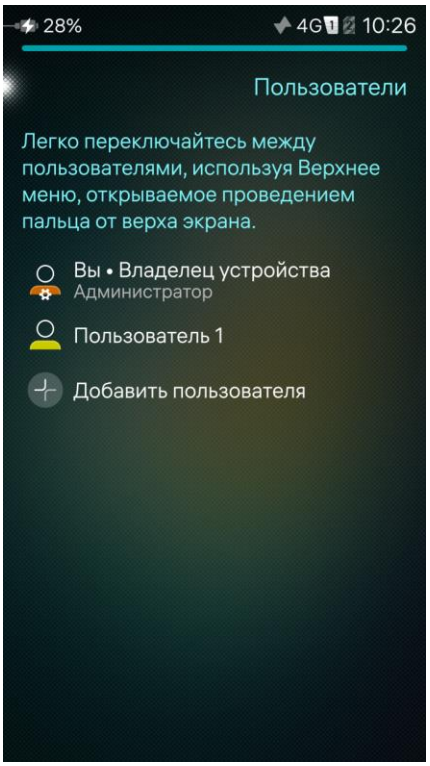

Рисунок 4

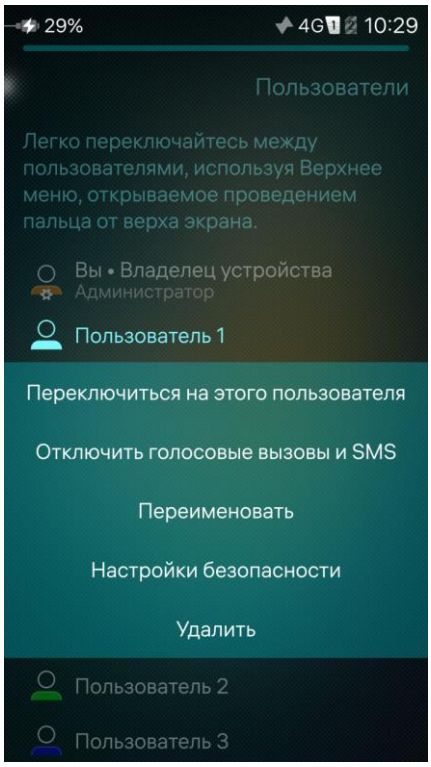

Рисунок 5

При работе с учетными записями пользователей администратору доступны следующие действия (Рисунок 5):

–переключение между учетными записями ролей (п. 1.2.2);

–управление голосовыми вызовами и SMS (п. 1.2.3);

–переименование учетной записи (п. 1.2.4);

–настройки безопасности (подраздел 1.3):

–удаление учетной записи (п. 1.2.5).

1.2.2. Переключение между учетными записями

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

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

– включить экран МУ;

– открыть верхнее меню, проведя с верхнего края Экрана блокировки к нижнему. В левом нижнем углу будет отображаться текущая роль: «Владелец устройства», если МУ загружено в режиме администратора, либо имя пользователя, если МУ загружено в режиме пользователя (Рисунок 6).

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

– включить экран МУ;

– открыть верхнее меню, проведя с верхнего края Экрана блокировки к нижнему;

– коснуться имени учетной записи пользователя;

– в раскрывающемся списке выбрать «Владелец устройства» (Рисунок 7);

– дождаться, когда ОС переключится на учетную запись администратора;

– убедиться, что текущая роль «Владелец устройства»: слева от названия роли «Владелец устройства» должна отображаться пометка «Вы».

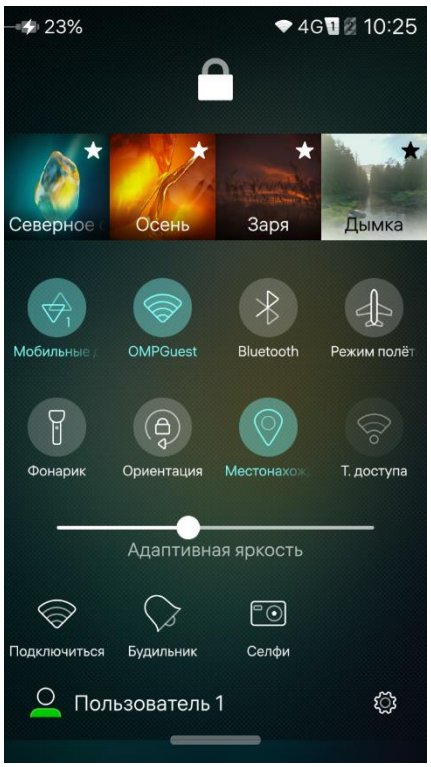

Рисунок 6

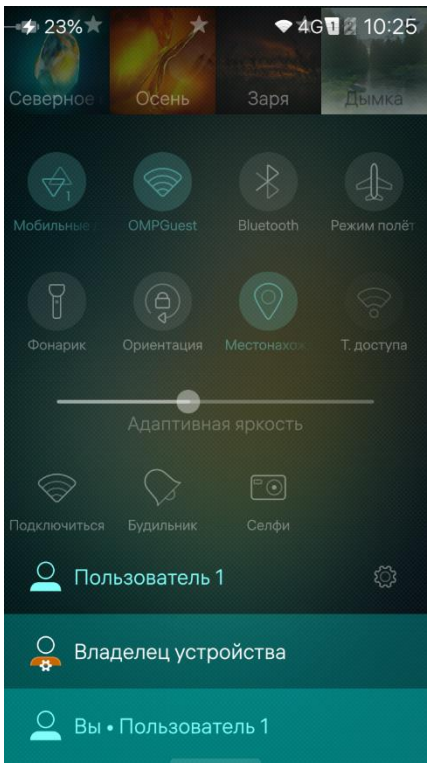

Рисунок 7

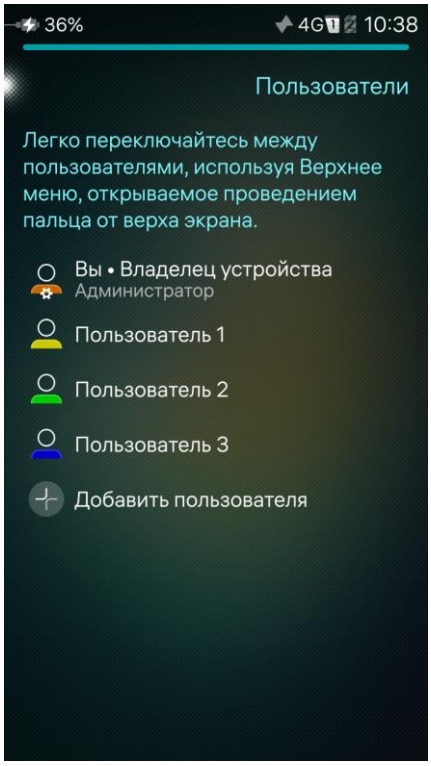

Рисунок 8

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

– коснуться пункта меню «Пользователи» в меню системных настроек, в результате чего отобразится страница «Пользователи» со списком учетных записей пользователей, созданных на МУ (Рисунок 8);

– при работе МУ в режиме администратора в поле «Владелец устройства» отображается пометка «Вы», означающая, что текущий пользователь МУ наделен ролью администратора (Рисунок 8). Для перехода в режим пользователя необходимо выполнить следующие действия:

- коснуться строки с именем одной из учетных записей пользователей созданных на МУ пользователей;

- в контекстном меню коснуться пункта «Переключится на этого пользователя» (см. Рисунок 5);
- 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 9). 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 10);
- процесс переключения займет несколько секунд. По окончании процесса переключения необходимо ввести код безопасности пользователя, на которого происходит переключение.

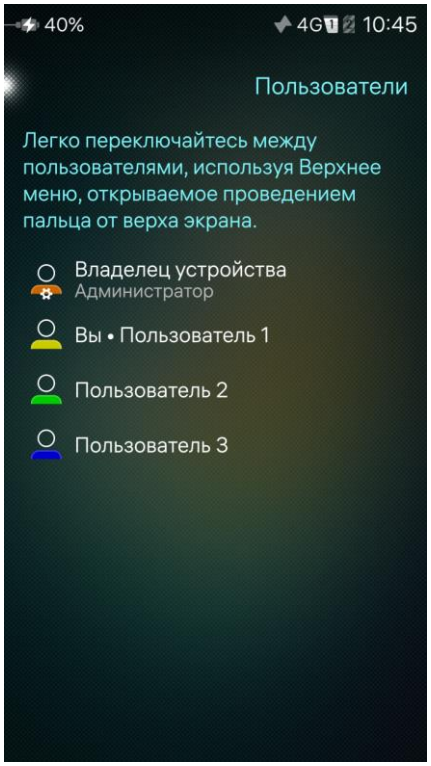

Рисунок 9

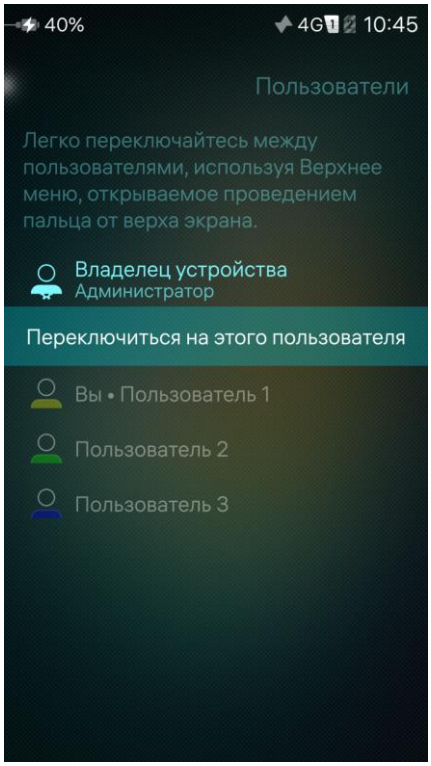

Рисунок 10

1.2.3. Управление голосовыми вызовами и SMS

Для отключения голосовых вызовов и SMS необходимо в контекстном меню коснуться пункта «Отключить голосовые вызовы и SMS» (Рисунок 5).

Далее у выбранного пользователя отобразится предупреждающий значок (Рисунок 11) и его возможности в МП «Телефон» и МП «Сообщения» будут ограничены.

Для включения голосовых вызовов и SMS администратору необходимо в контекстном меню коснуться пункта «Включить голосовые вызовы и SMS» (Рисунок 12), после чего предупреждающий значок перестанет отображаться у выбранного пользователя, и его возможности в МП «Телефон» и МП «Сообщения» будут восстановлены.

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

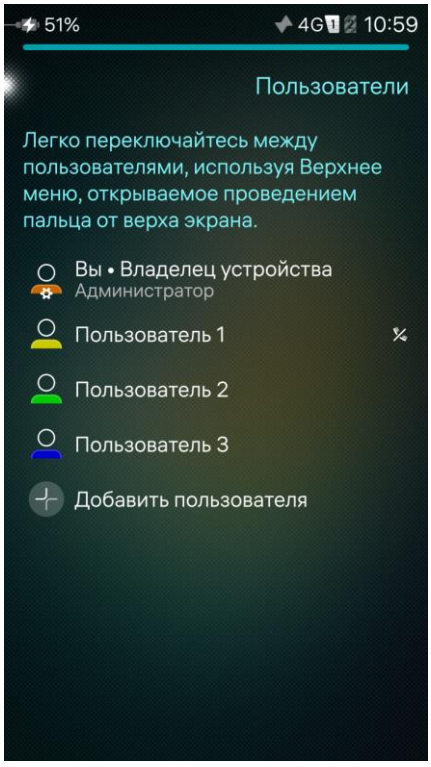

Рисунок 11

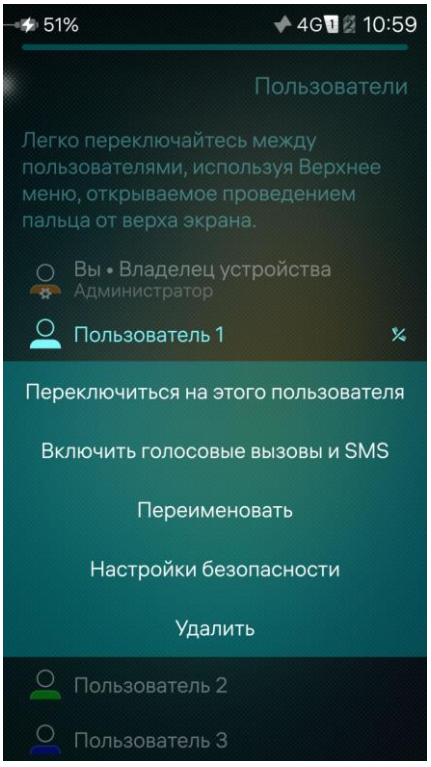

Рисунок 12

1.2.4. Переименование учетной записи

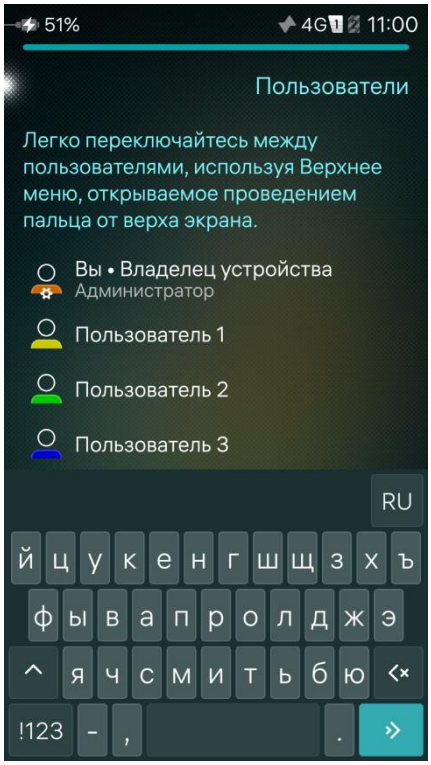

Рисунок 13

Для переименования учетной записи пользователя необходимо выполнить следующие действия:

– коснуться одной из созданных учетных записей пользователей;

– в контекстном меню коснуться пункта «Переименовать» (см. Рисунок 5);

– ввести новое имя учетной записи пользователя (Рисунок 13);

– коснуться значка » для подтверждения действия.

1.2.5. Удаление учетной записи пользователя

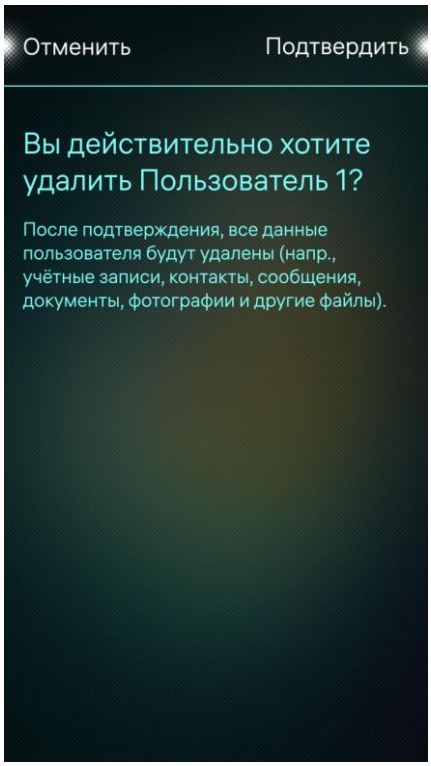

Рисунок 14

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 5);

– на отобразившейся странице коснуться кнопки «Подтвердить» для удаления учетной записи пользователя либо кнопки «Отменить» для отмены операции;

– для удаления подтвердить действие вводом кода безопасности.

1.3. Настройки безопасности

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

1.3.1. Настройка блокировки

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.

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

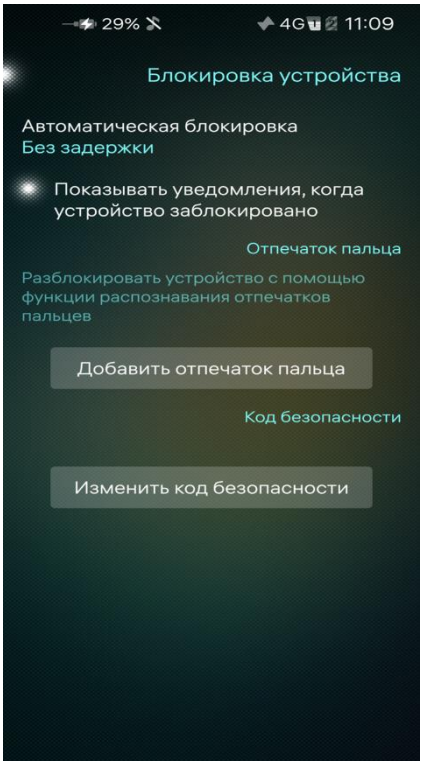

Рисунок 15

Для включения блокировки МУ необходимо выполнить следующие действия:

– коснуться пункта «Блокировка устройства» в меню настроек безопасности, в результате чего отобразится страница с настройками блокировки МУ (Рисунок 15);

– коснуться поля «Автоматическая блокировка» и на открывшейся странице выбрать время до автоматической блокировки МУ (Рисунок 16, Рисунок 17) либо коснуться поля «Неактивно» для отключения автоматической блокировки;

ВНИМАНИЕ! Варианты значений в поле «Автоматическая блокировка» отличается в зависимости от варианта исполнения ОС Аврора[2] (Рисунок 16, Рисунок 17)

[2] Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 4).

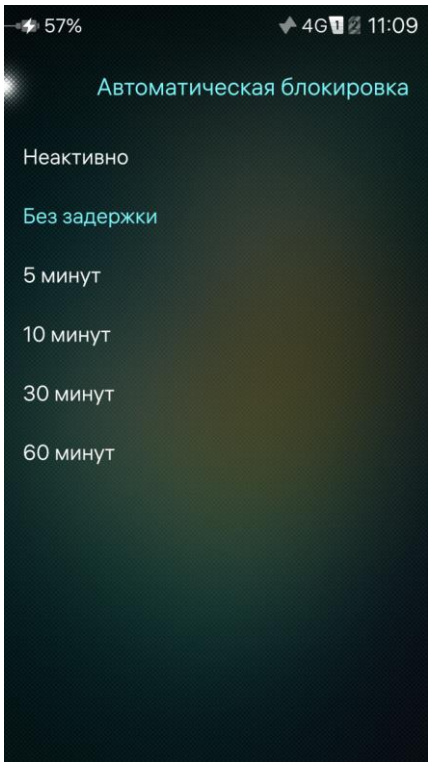

Рисунок 16

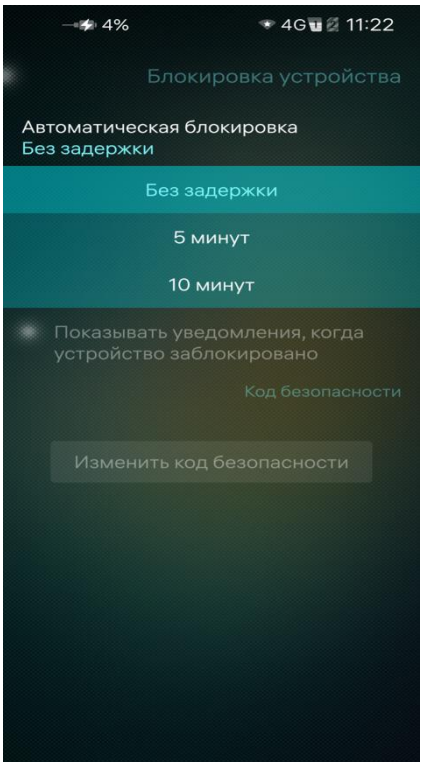

Рисунок 17

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

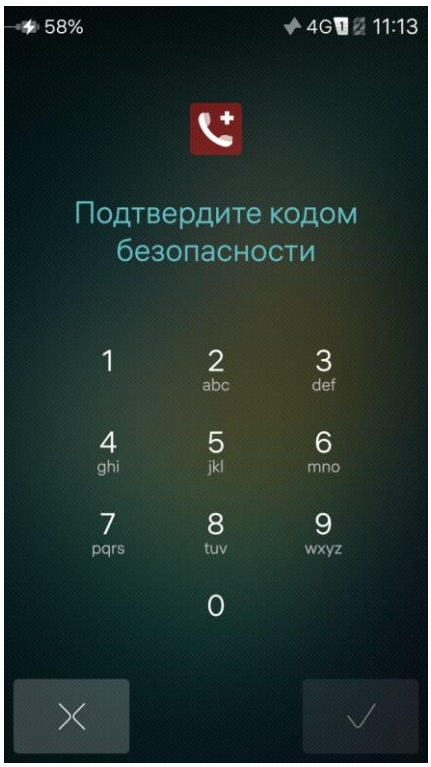

Рисунок 18

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 соответствующей действию кнопки, подтвердить действие вводом текущего кода безопасности, затем дважды ввести новый код.

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

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

1.3.2. Настройки парольной политики

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

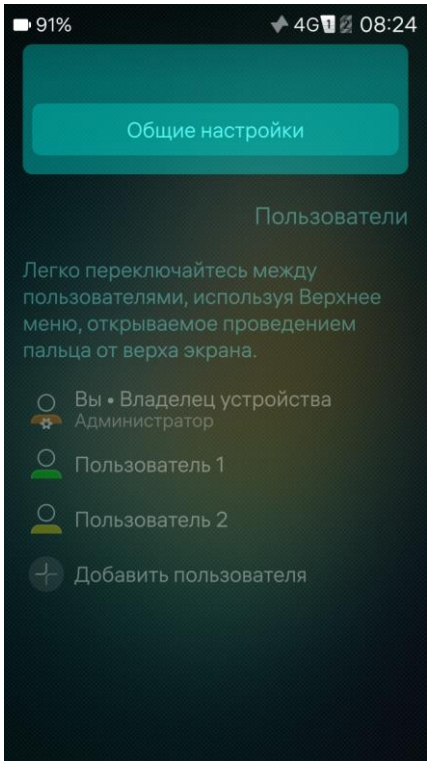

Рисунок 19

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 19), в результате чего отобразится страница «Общие настройки»;

– коснуться пункта «Настройка политики паролей» и на отобразившейся странице коснуться поля «Настройка политики паролей» (Рисунок 20).

ВНИМАНИЕ! Интерфейс страницы «Настройка паролей» может отличаться в зависимости от варианта исполнения ОС Аврора[3] (Рисунок 20, Рисунок 21)

[3] Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 4).

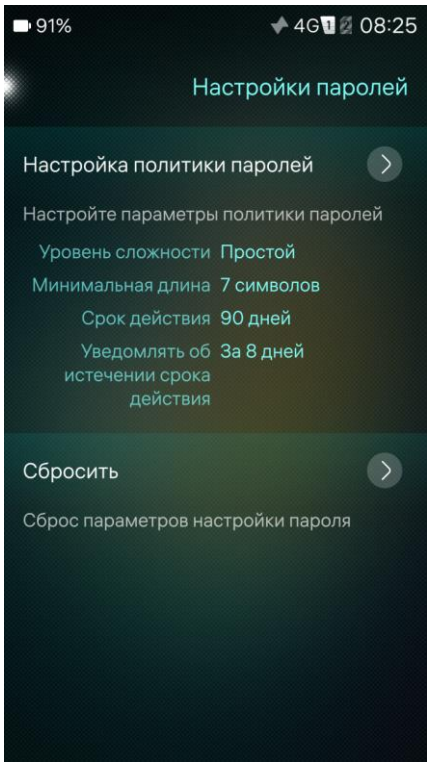

Рисунок 20

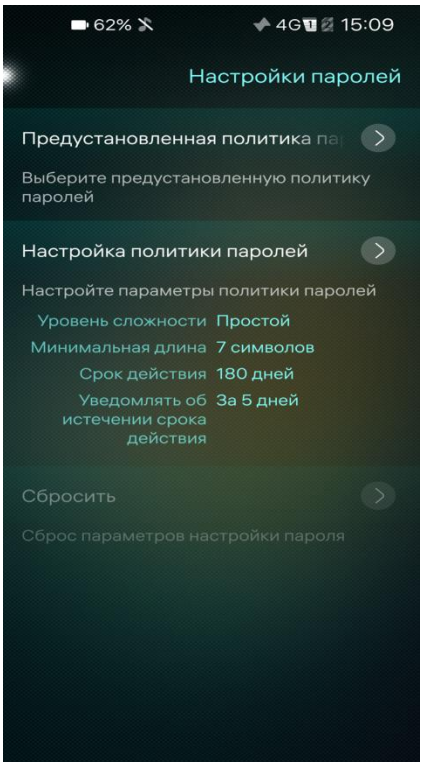

Рисунок 21

Для выбора предустановленной политики паролей необходимо выполнить следующие действия:

– коснуться поля «Предустановленная политика паролей» (Рисунок 21);

– на открывшейся странице выбрать необходимую политику, касанием соответствующего поля (Рисунок 22).

Для настройки политики паролей на открывшейся странице «Настройки парольной политики» задать необходимые параметры для кода безопасности (Рисунок 23):

– уровень сложности;

– длина;

– количество попыток;

– срок действия;

– уведомление об истечении срока действия.

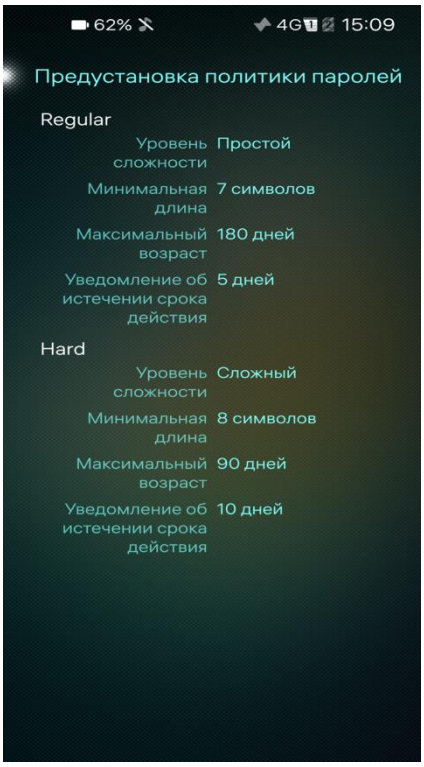

Рисунок 22

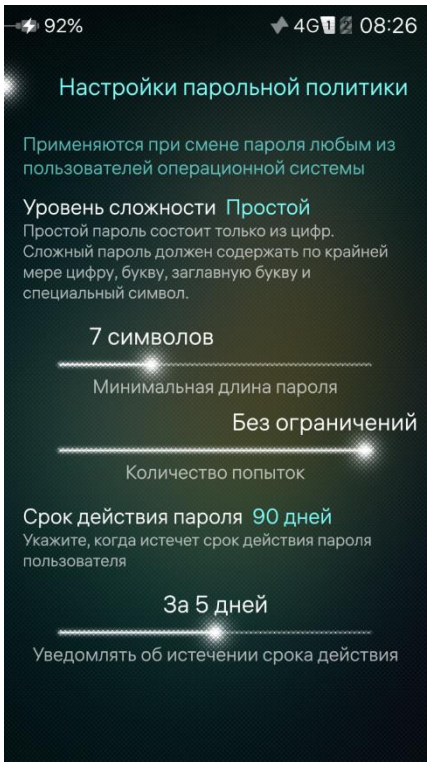

Рисунок 23

Для настройки уровня сложности кода безопасности необходимо выполнить следующие действия (Рисунок 24):

– 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 25):

– 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.

Предусмотрена возможность установить длину кода безопасности от 5 до 12 символов

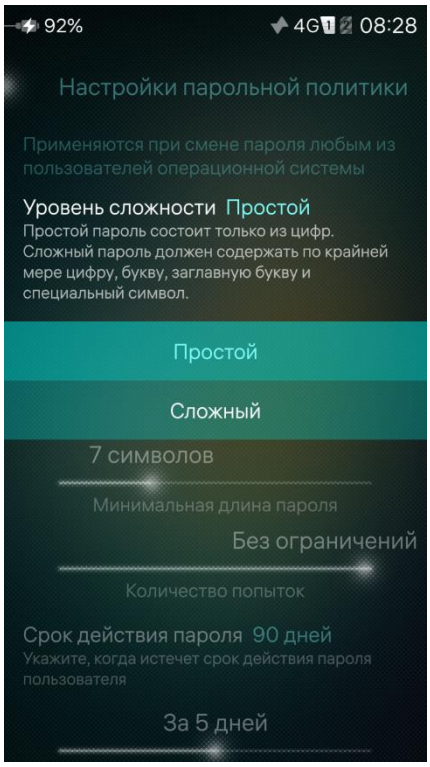

Рисунок 24

Рисунок 25

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

– влево для уменьшения (минимальное значение: 4 попытки);

– вправо для увеличения (максимальное значение: 10 попыток либо «Без ограничений»).

ВНИМАНИЕ! Максимальное значение слайдера «Количество попыток» зависит от варианта исполнения ОС Аврора

Для задания срока действия кода безопасности необходимо выполнить следующие действия:

– коснуться поля «Срок действия пароля» (см. Рисунок 25) и на отобразившейся странице выбрать одно из значений (Рисунок 26);

– подтвердить действие вводом текущего кода безопасности.

Для задания времени уведомления об истечении срока действия кода безопасности необходимо выполнить следующие действия (Рисунок 27):

– 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.

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

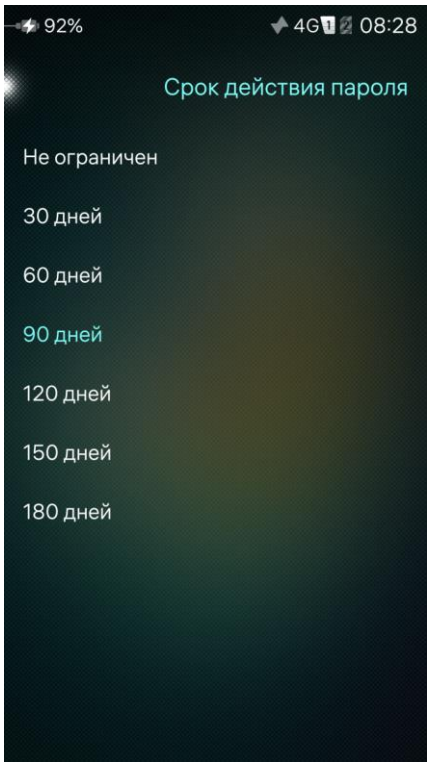

Рисунок 26

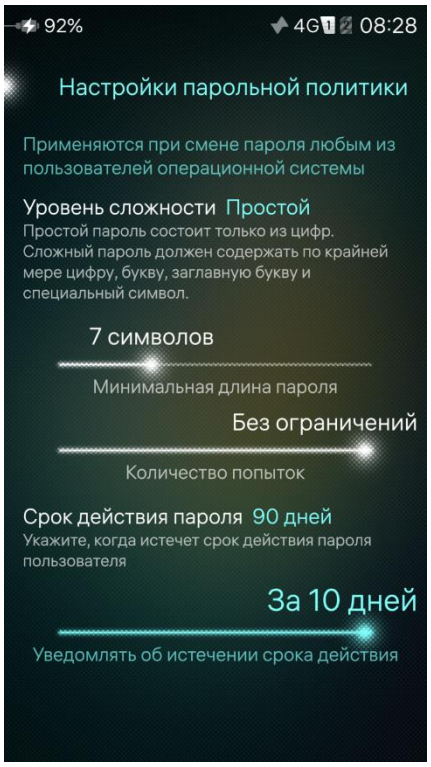

Рисунок 27

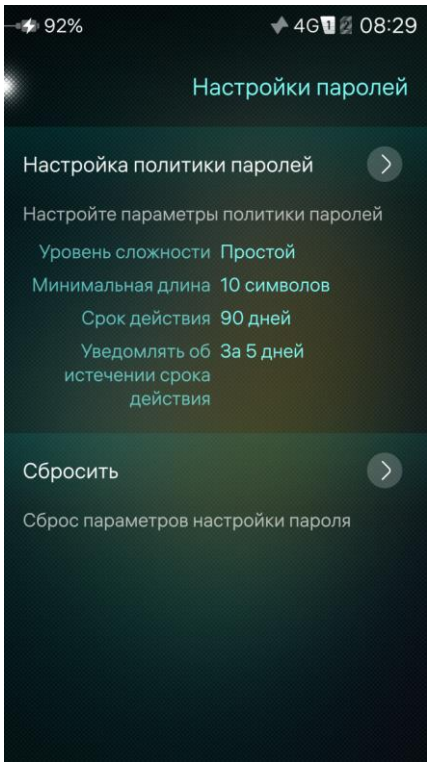

Рисунок 28

Для сброса парольной политики необходимо выполнить следующие действия:

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

– подтвердить действие вводом текущего кода безопасности.

1.3.3. Ограничения входа в систему

Изменения настроек безопасности применяется только к конкретной учетной записи пользователя

Для настройки безопасности учетной записи пользователя необходимо выполнить следующие действия:

– коснуться одной из созданных учетных записей пользователя (Рисунок 5);

– в контекстном меню коснуться пункта «Настройки безопасности»;

– отобразится страница «[Имя учетной записи пользователя]» (Рисунок 29), на которой возможно выполнить следующие действия:

- задать для учетной записи пользователя ограничения входа в систему;
- активировать и настроить двухфакторную аутентификацию (2ФА);
- задать одноразовый пароль.

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 30):

– срок действия учетной записи пользователя;

– дни входа в систему;

– время входа в систему.

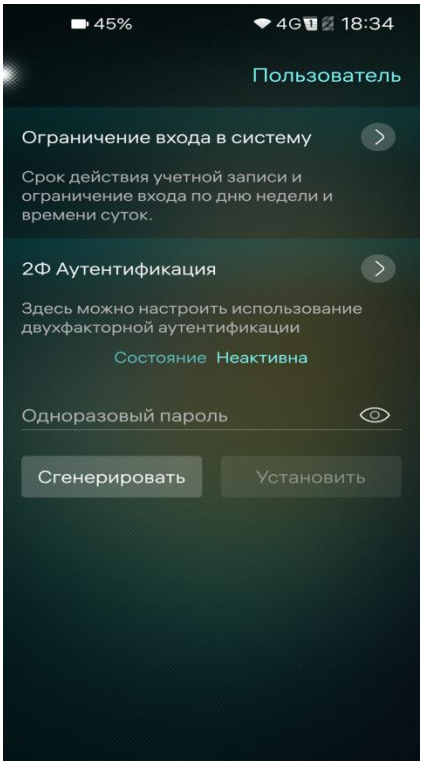

Рисунок 29

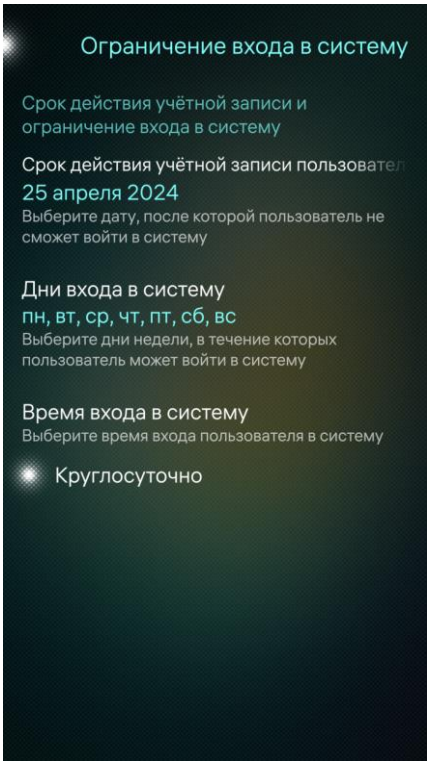

Рисунок 30

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 45);

– подтвердить действие вводом кода безопасности.

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

– коснуться поля «Дни входа в систему» и на отобразившейся странице выбрать дни недели, в течение которых пользователь сможет войти в систему (Рисунок 31);

– подтвердить действие вводом кода безопасности.

Для настройки времени входа в систему необходимо выполнить следующие действия:

– коснуться переключателя «Круглосуточно» для его деактивации, в результате чего отобразятся поля ввода диапазона времени, в течение которого пользователь сможет войти в систему (Рисунок 32);

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 выполнять вход 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 времен либо кнопки «Отменить» для отмены операции (см. Рисунок 46);

– подтвердить действие вводом кода безопасности.

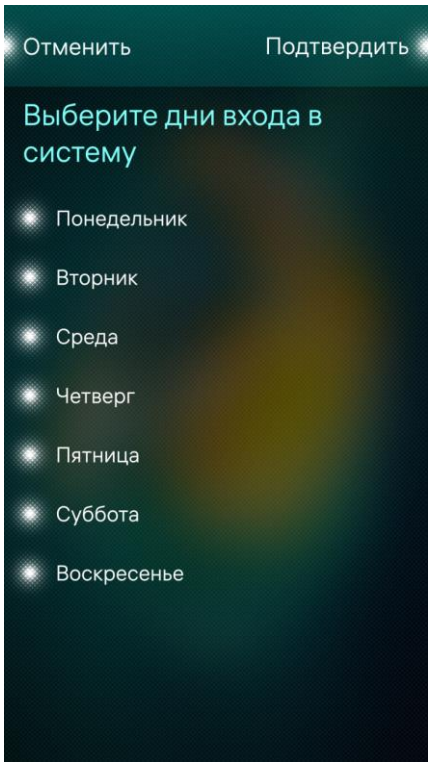

Рисунок 31

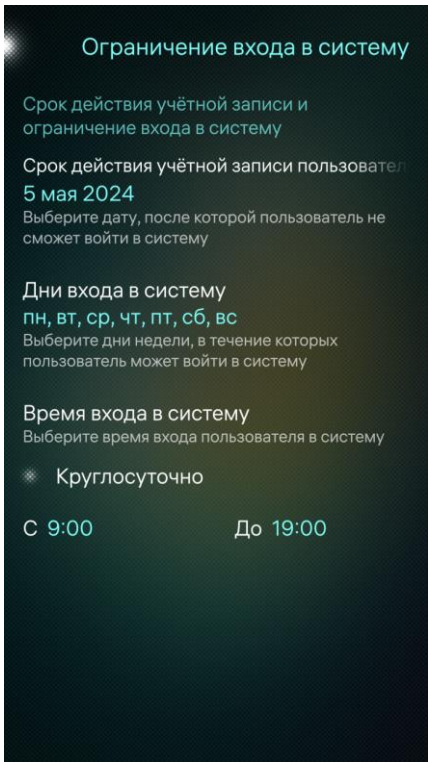

Рисунок 32

1.3.4. Настройка двухфакторной аутентификации

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

Для 2ФА в ОС Аврора применяются:

– в качестве первого фактора: пароль;

– в качестве второго фактора: токен, содержащий уникальную информацию пользователя.

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

1.3.4.1. Правила настройки и использования 2ФА

Необходимо учитывать следующие основные правила настройки и использования 2ФА:

– эксплуатацию токена необходимо осуществлять в соответствии с требованиями, указанными в соответствующей документации на него;

– для обеспечения подключения к МУ и последующей настройки токена необходимо 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. 1.2.1), созданных в ОС Аврора;

– проверка токена при входе пользователя происходит однократно – только при первичном входе.

1.3.4.2. Предварительная подготовка токена

Для настройки 2ФА токен должен иметь формат PKCS#15

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

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

при этом предварительно на ЭВМ должен быть установлен пакет opensc.

ВНИМАНИЕ! После переинициализации токена все данные с него будут удалены

1.3.4.3. Включение и выключение 2ФА

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 33);

– подключить токен (смарт-карту). После успешного подключения на экране отобразится соответствующее сообщение (Рисунок 34);

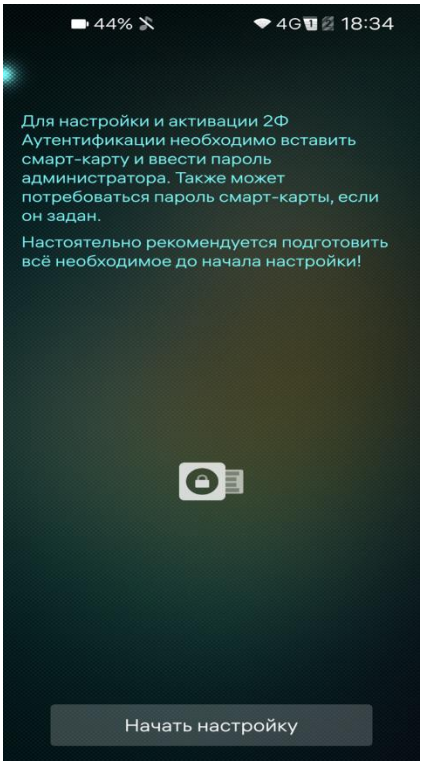

Рисунок 33

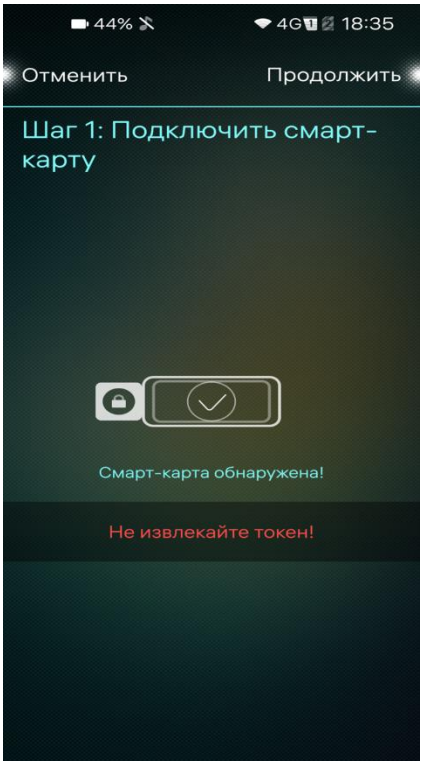

Рисунок 34

– на отобразившейся странице «Инициализация смарт-карты» коснуться кнопки «Ввести пароль» для ввода пароля от токена либо коснуться кнопки «Попробуйте другую смарт-карту» для подключения другого токена (Рисунок 35)

– в поле ввода ввести пароль от токена и коснуться значка  (Рисунок 36);

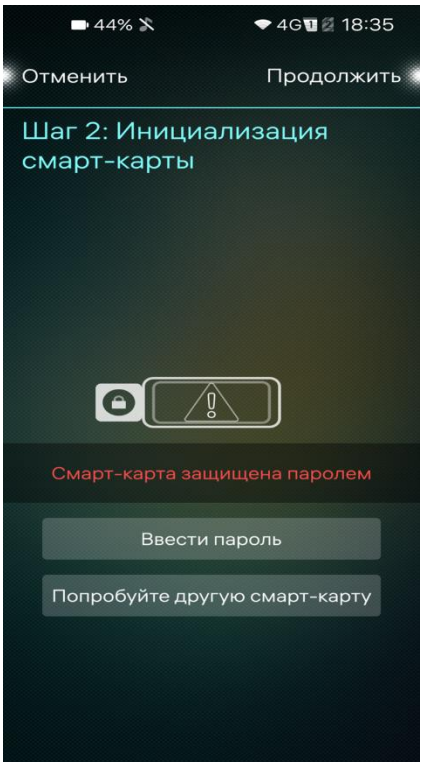

Рисунок 35

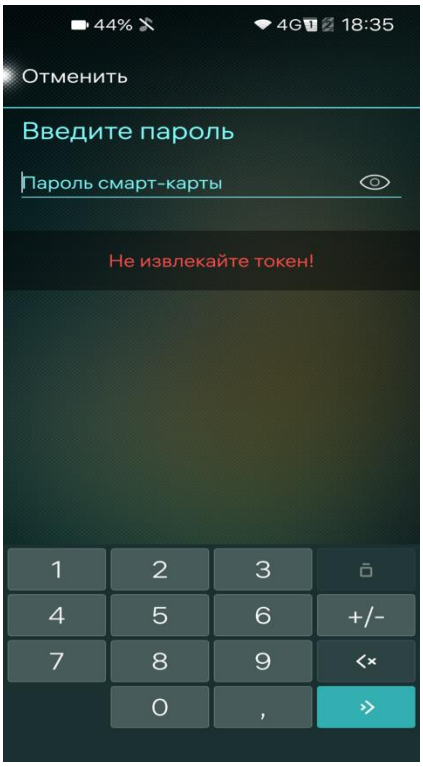

Рисунок 36

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

– коснуться кнопки «Подтвердить» для подтверждения либо кнопки «Отменить» для отмены операции (Рисунок 37);

– на отобразившейся странице коснуться кнопки «Завершить» для завершения настройки 2ФА (Рисунок 38), после чего значение поля «Состояние» изменится на «Активна» (см. Рисунок 39).

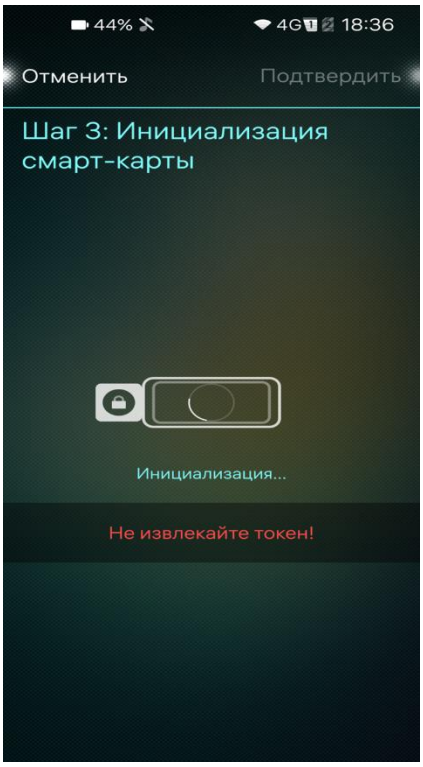

Рисунок 37

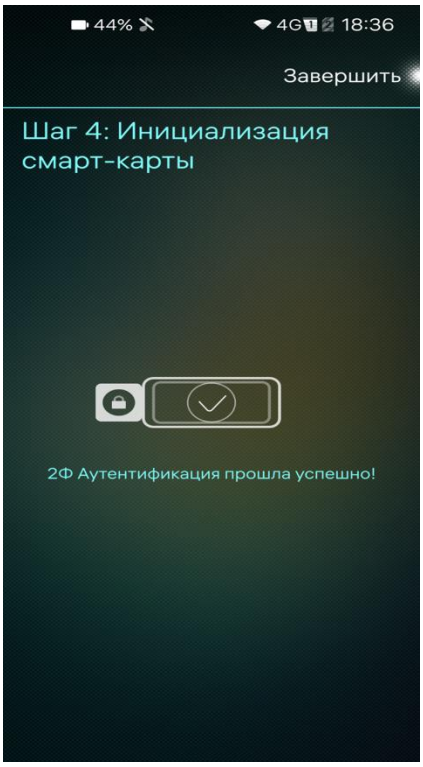

Рисунок 38

Для отключения 2ФА необходимо выполнить следующие действия:

– на странице «[Имя учетной записи пользователя]» (Рисунок 39) на которой коснуться пункта «2Ф Аутентификация»;

– на отобразившейся странице коснуться кнопки «Отключить» для отключения 2ФА (Рисунок 40), после чего значение поля «Состояние» изменится на «Неактивно» (см. Рисунок 29).

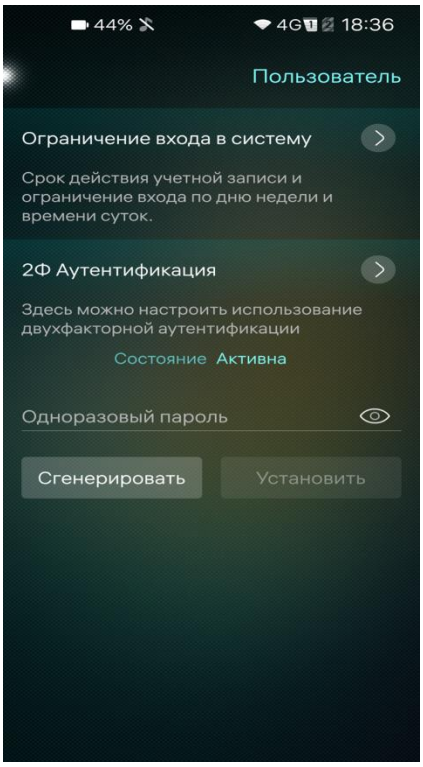

Рисунок 39

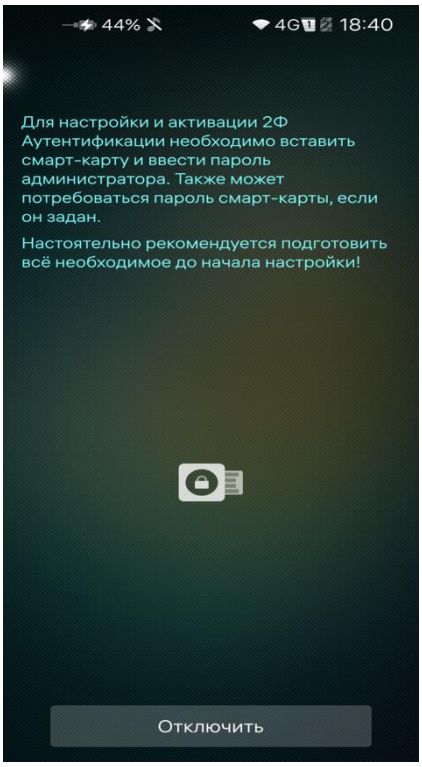

Рисунок 40

1.3.5. Задание одноразового пароля для учетной записи пользователя

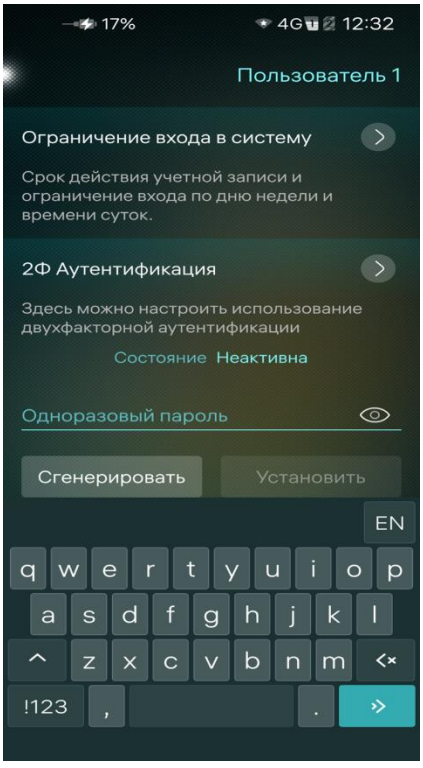

Рисунок 41

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;

– коснуться кнопки «Установить» для подтверждения действия (Рисунок 41)»;

– подтвердить действие вводом кода безопасности.

1.4. Дополнительные настройки

Администратору МУ доступны следующие дополнительные возможности:

- настройка времени и даты (п. 1.4.1);
- настройка USB-подключения (п. 1.4.2);
- активация/деактивация PIN-кода (п. 1.4.3);
- просмотр данных об учетной записи (п. 1.4.4).

1.4.1. Настройка времени и даты

Для 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 42), 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» (Рисунок 43), после чего значения полей часового пояса, даты и времени станут недоступными для редактирования (Рисунок 44), при этом в дальнейшем обновление даты и времени будет происходить автоматически.

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

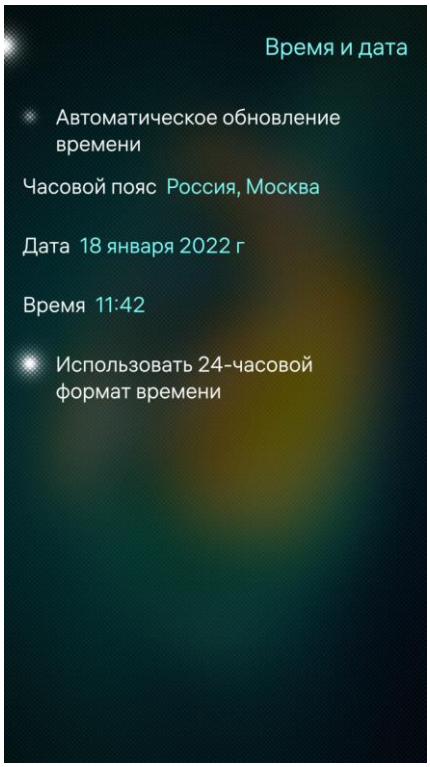

Рисунок 42

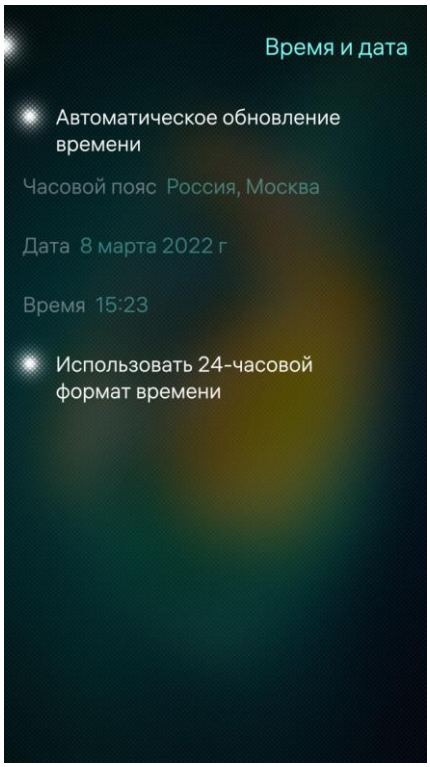

Рисунок 43

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

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

– для установки часового пояса вручную: коснуться поля «Часовой пояс» (см. Рисунок 42) и на открывшейся странице выбрать необходимое значение (Рисунок 44). Для ускорения процесса выбора можно воспользоваться полем поиска;

– выбрать формат времени, коснувшись переключателя «Использовать 24-часовой формат» (см. Рисунок 42) 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 42), на открывшейся странице коснуться текущей даты и выбрать из списка текущий год, месяц и число (Рисунок 45);

– 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;

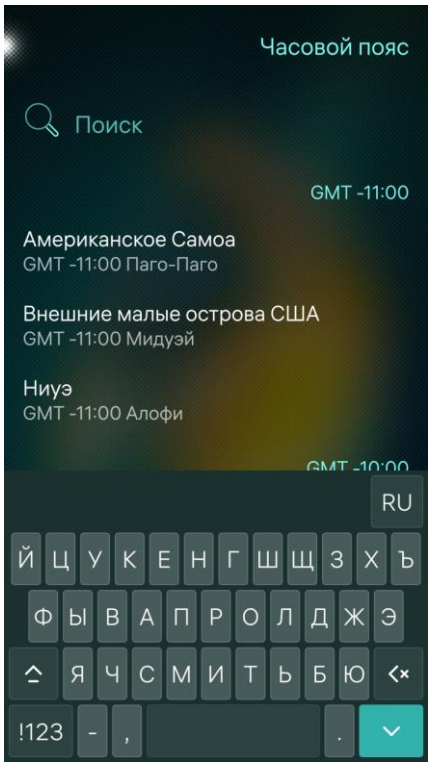

Рисунок 44

Рисунок 45

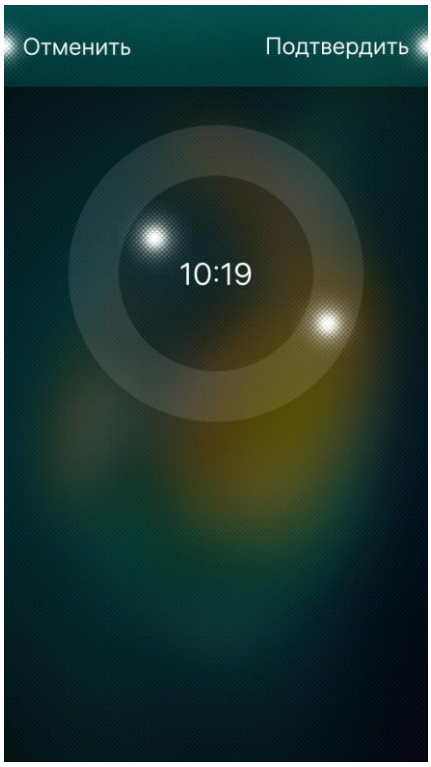

Рисунок 46

– для установки времени коснуться поля «Время» (см. Рисунок 42). Отобразится циферблат, метка во внутреннем круге которого играет роль часовой стрелки, во внешнем — минутной (Рисунок 46). 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.

1.4.2. Настройка USB-подключения

Для настройки USB-подключения необходимо коснуться пункта «USB» в меню настроек сети, после чего в открывшемся окне настроек USB-подключения (Рисунок 47) коснуться поля «Режим USB по умолчанию» и выбрать необходимое значение из раскрывающегося списка.

При подключении МУ к ЭВМ с помощью USB-кабеля на МУ отобразится окно с выбором режима USB-подключения (Рисунок 48).

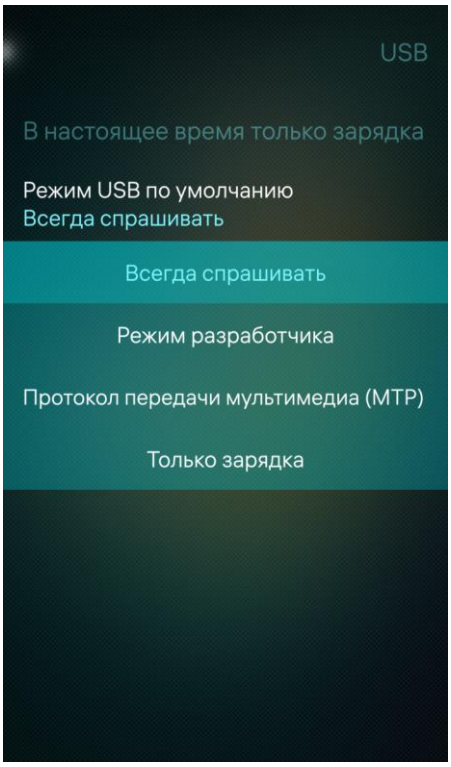

Рисунок 47

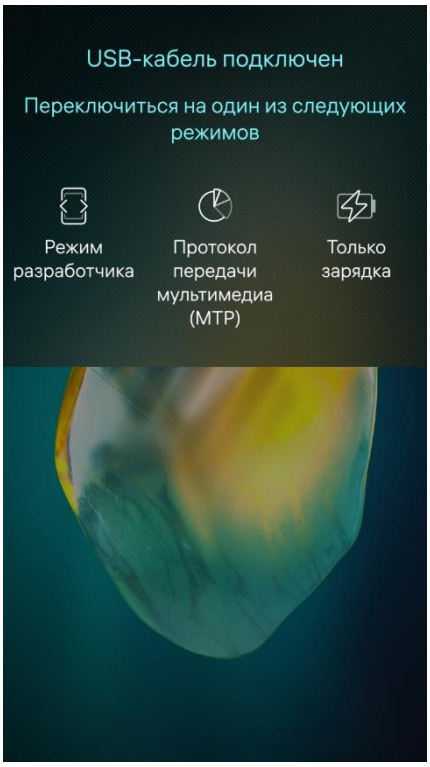

Рисунок 48

Значение «Режим разработчика» отображается только при активации соответствующего переключателя в разделе «Средства разработчика» системных настроек (подраздел 3.1)

1.4.3. Активация/деактивация PIN-кода

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

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

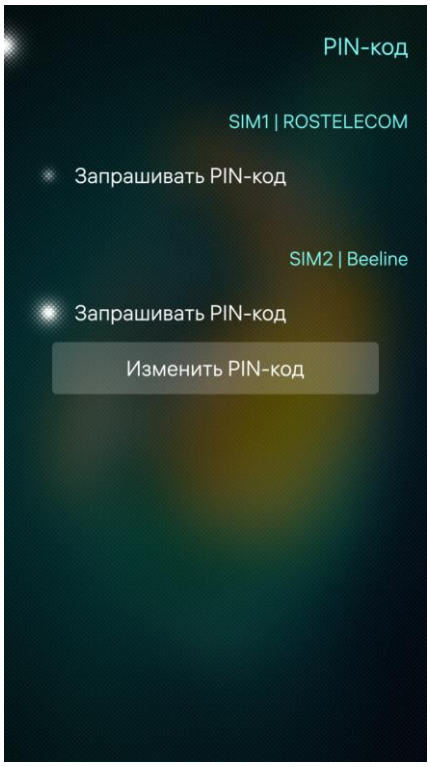

Рисунок 49

Для активации/деактивации PIN-кода необходимо выполнить следующие действия (Рисунок 49):

– 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.

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

После активации PIN-кода он будет запрашиваться при каждом включении МУ (Рисунок 50). 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 51).

PUK-код предоставляется оператором сотовой связи

После ввода верного PUK-кода отобразится страница для изменения PIN-кода (Рисунок 49), на которой необходимо выполнить следующие действия:

– коснуться кнопки «Изменить PIN-код»;

– внести соответствующие изменения в разделе SIM-карты, которую требуется защитить вводом PIN-кода.

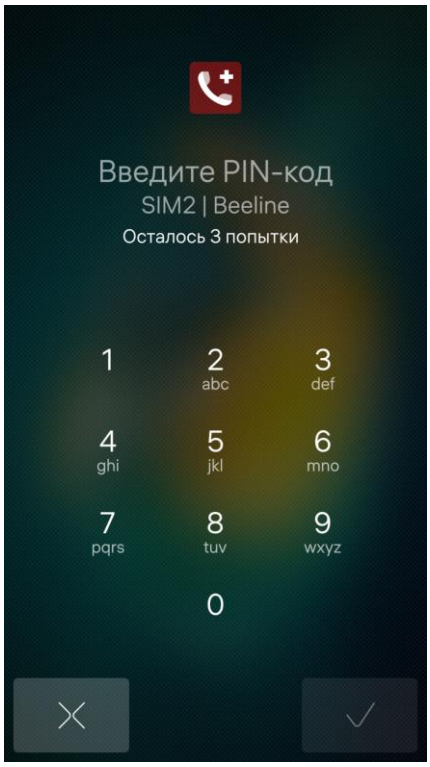

Рисунок 50

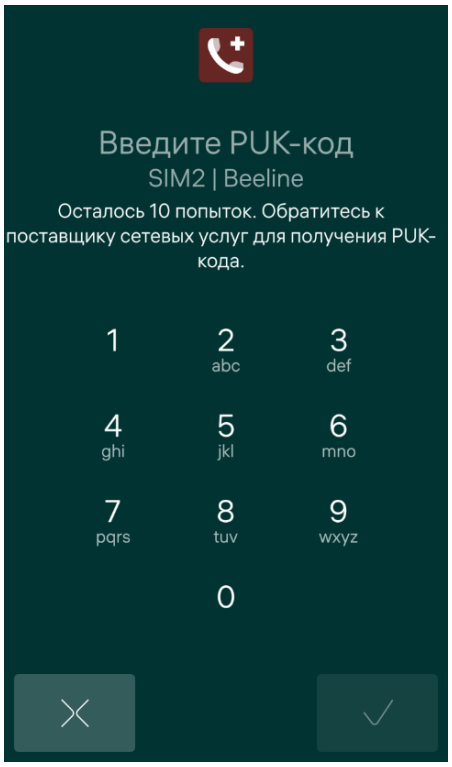

Рисунок 51

1.4.4. Просмотр данных об учетной записи

Для просмотра пароля учетной записи необходимо выполнить следующие действия:

– открыть меню настроек, коснувшись значка на Экране приложений, и перейти в раздел «Учетные записи»;

– коснуться необходимой учетной записи, после чего на отобразившейся странице открыть меню действий и коснуться пункта «Изменить настройки сервера».

– на странице «Настройки сервера» коснуться значка в поле «Пароль» для отображения пароля от учетной записи.

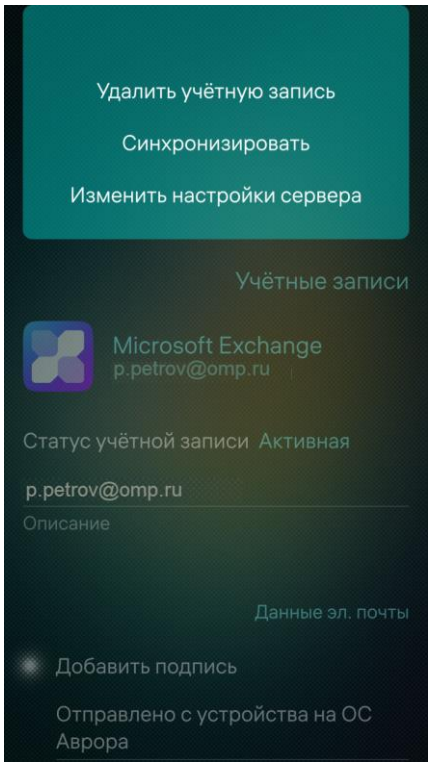

Рисунок 52

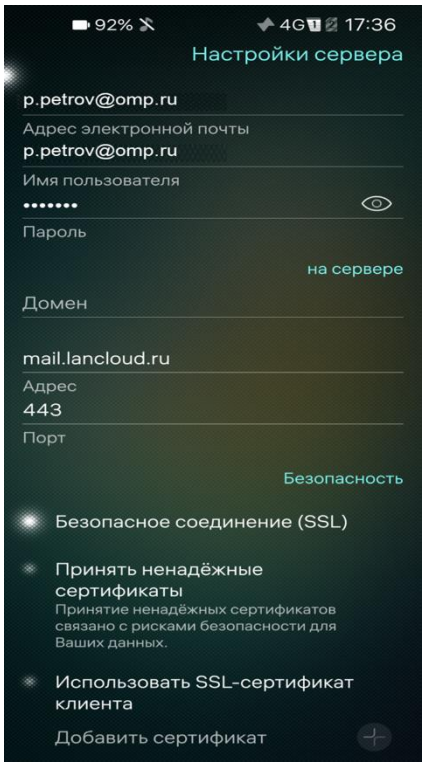

Рисунок 53

2. ВЫПОЛНЕНИЕ ПРОГРАММЫ

2.1. Настройка обновлений ОС Аврора

Обновление ОС Аврора может осуществляться администратором либо локально вручную, либо удаленно с использованием ППО.

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

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

– в меню системных настроек коснуться пункта «Обновления Аврора ОС» , в результате чего отобразится страница с настройками обновления;

– коснуться значка для проверки доступных обновлений. В результате отобразится сообщение: «Нет доступных обновлений», а также дата и время последней проверки (Рисунок 54) либо доступное обновление (Рисунок 55);

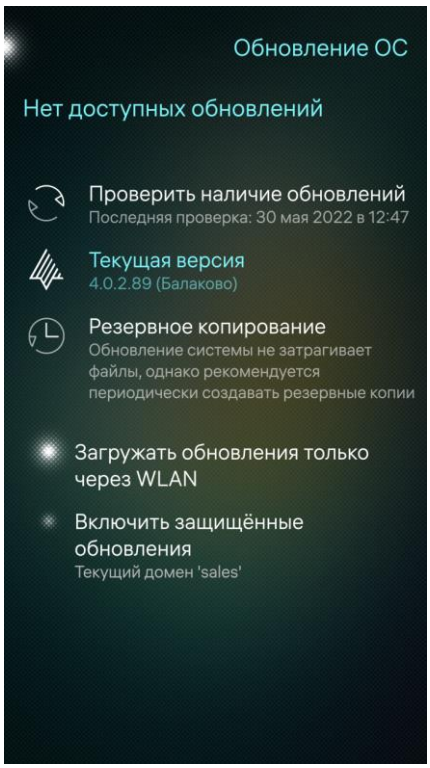

Рисунок 54

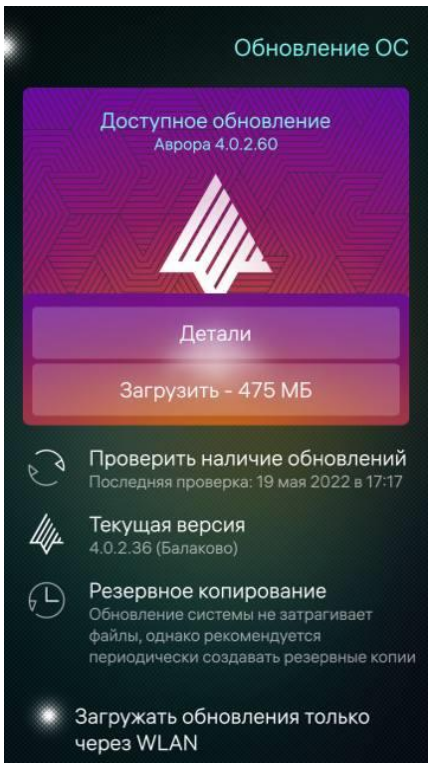

Рисунок 55

– при наличии доступного обновления коснуться кнопки «Загрузить - [Размер обновления]» для его загрузки. В случае необходимости загрузку обновления можно отменить касанием кнопки «Отменить загрузку» (Рисунок 56);

– коснуться кнопки «Детали» и на открывшейся странице ознакомится с подробной информацией об обновлении (Рисунок 57).

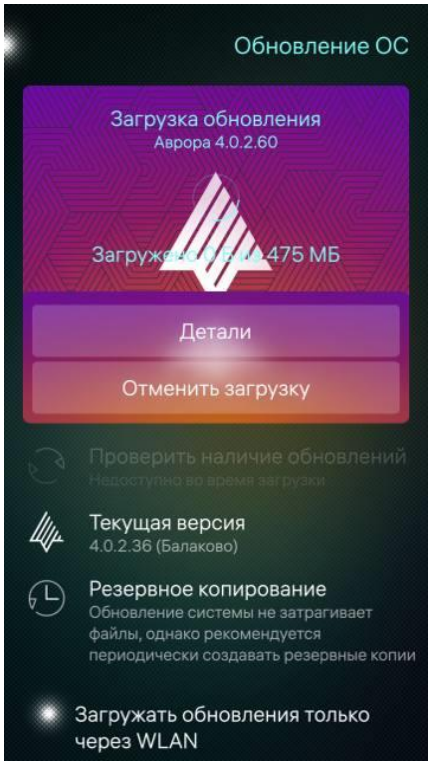

Рисунок 56

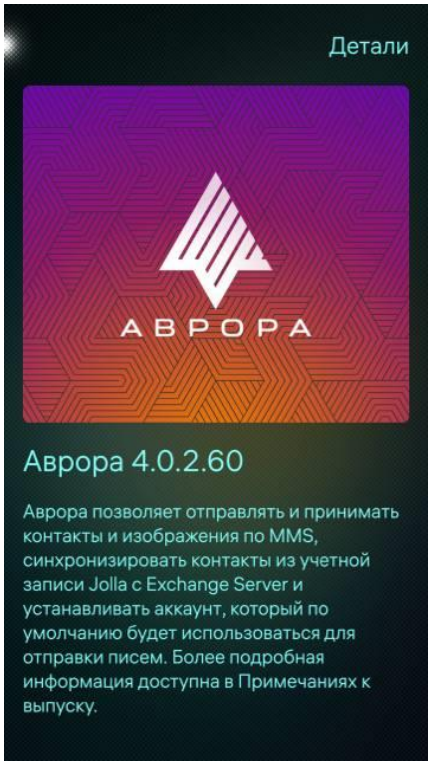

Рисунок 57

– после успешной загрузки обновления коснуться кнопки «Установить обновление» (Рисунок 58);

– на открывшейся странице коснуться кнопки «Установить» (Рисунок 59), после чего МУ автоматически будет перезагружено, либо кнопки «Отменить» для отмены действий.

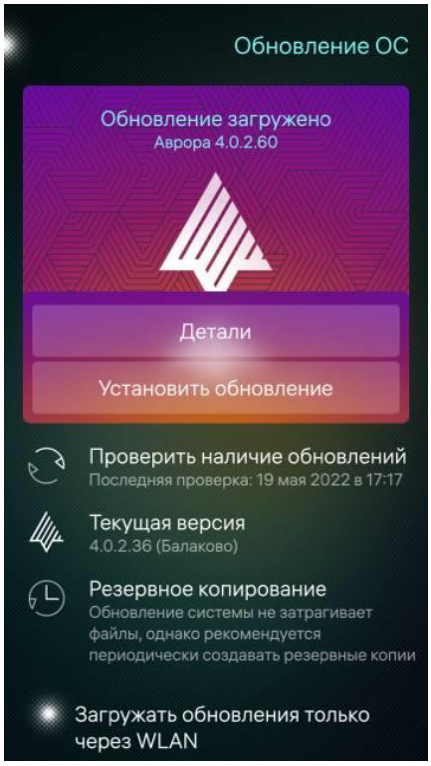

Рисунок 58

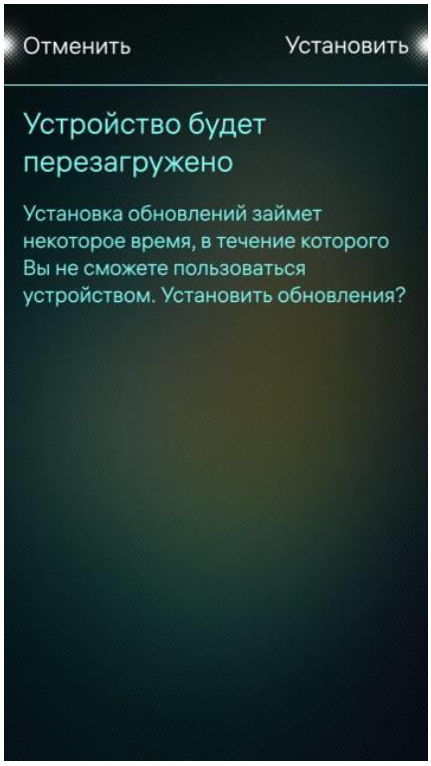

Рисунок 59

На странице «Обновление ОС» администратору также доступны следующие действия (см. Рисунок 54):

– просмотреть информацию о текущей версии ОС ;

– выполнить резервное копирование перед обновлением ОС, коснувшись значка ;

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

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

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

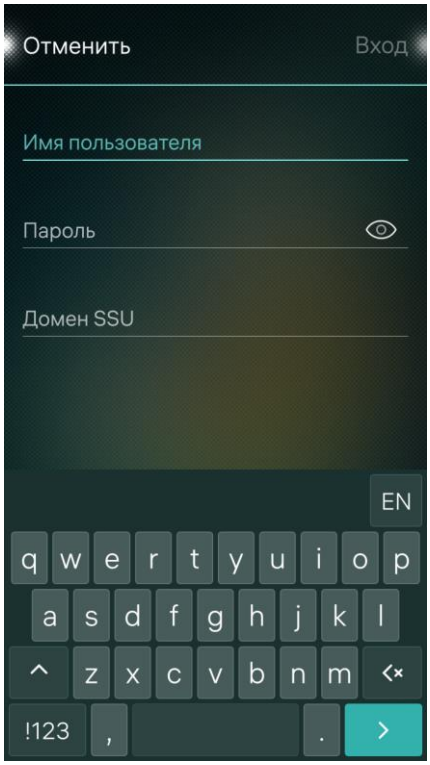

Рисунок 60

Для настройки обновлений ОС коснуться переключателя «Включить защищенные обновления» (см. Рисунок 54) и на открывшейся странице заполнить необходимые поля (Рисунок 60) для регистрации доступа к репозиториям, после чего коснуться кнопки «Вход» для выполнения входа либо кнопки «Отменить» для отмены действия.

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

2.2. Сброс настроек мобильного устройства

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 61);

– коснуться кнопки «Подтвердить» для подтверждения сброса настроек МУ либо кнопки «Отменить» для отмены операции (Рисунок 62);

– при необходимости коснуться переключателя «Автоматически перезагрузить устройство после сброса» для последующей перезагрузки МУ;

– при необходимости коснуться переключателя «Стереть все данные» для удаления данных.

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»

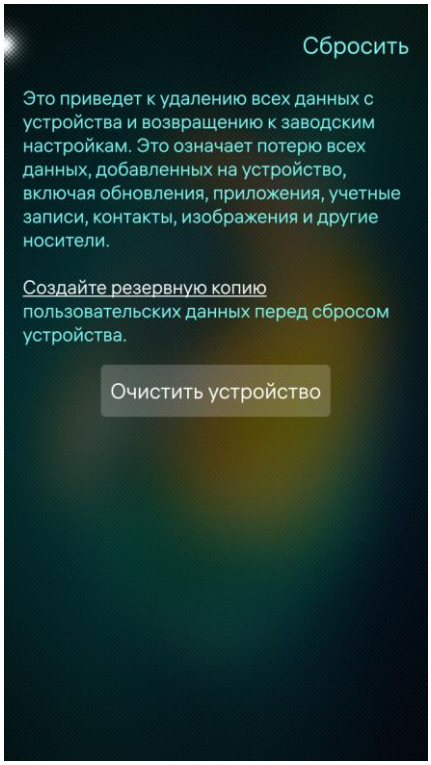

Рисунок 61

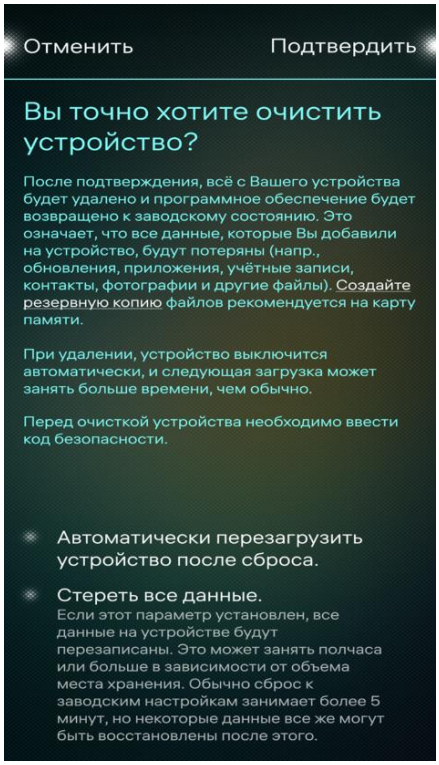

Рисунок 62

2.3. Мобильное приложение «Terminal»

2.3.1. Включение отображения МП «Terminal»

В МП «Terminal» выводится поток данных, а также диагностические и отладочные сообщения в текстовом виде.

МП «Terminal» не отображается на Экране приложений при первой загрузке МУ. Для его отображения необходимо выполнить следующие действия:

– коснуться пункта «Администрирование» в меню системных настроек;

– на открывшейся странице коснуться переключателя «Включить терминал» (Рисунок 63) для отображения МП на Экране приложений;

– коснуться поля ввода либо кнопки «Сгенерировать», чтобы задать пароль, который в дальнейшем будет использоваться для получения прав суперпользователя;

Необходимо запомнить установленный пароль

– коснуться кнопки «Сохранить» (Рисунок 64).

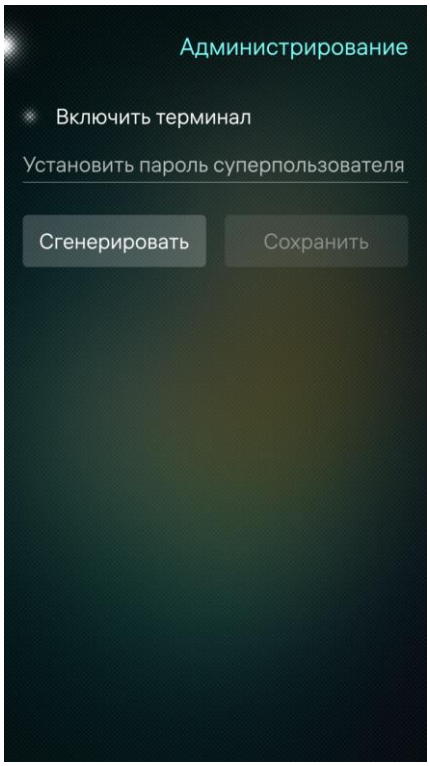

Рисунок 63

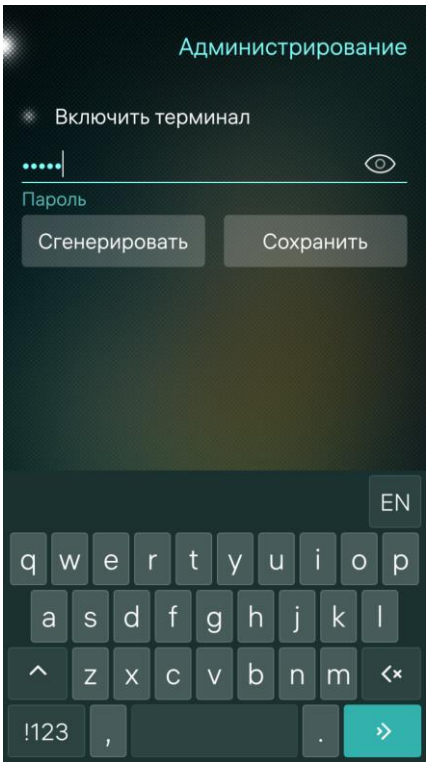

Рисунок 64

2.3.2. Получение прав суперпользователя

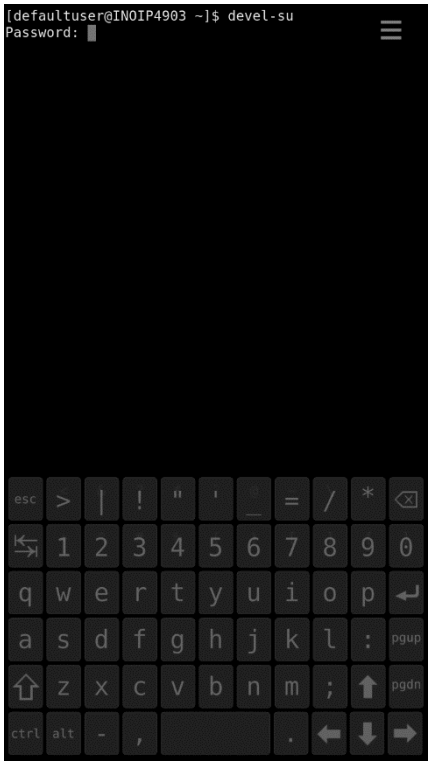

Рисунок 65

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

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

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

– на открывшейся странице выполнить команду: `devel-su;`

– указать заданный ранее пароль, в результате чего будет выполнен переход в режим суперпользователя.

2.3.3. Настройка МП «Terminal»

Для настройки интерфейса МП «Terminal» необходимо:

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

– коснуться значка для отображения меню с настройками интерфейса, в котором можно выполнить следующие действия (Рисунок 66):

- коснуться кнопок «Копировать» или «Вставить» для копирования или вставки фрагмента текста;
- коснуться кнопки «Обнаруженные URL-ссылки» для поиска URL-ссылок;

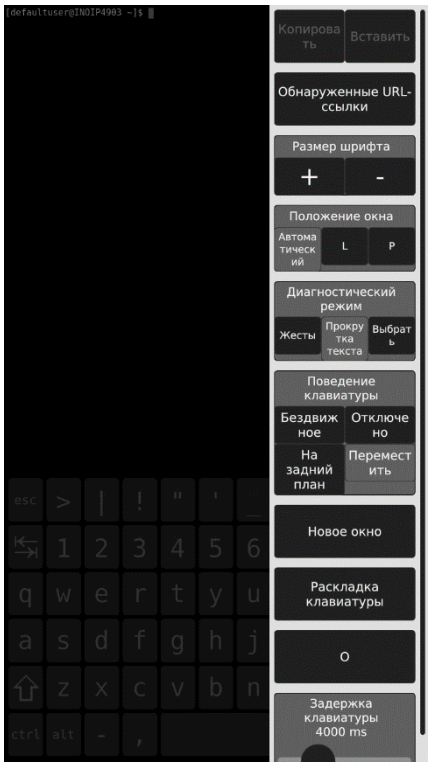

Рисунок 66

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

2.4. Управление сторонним программным обеспечением

2.4.1. Установка стороннего ПО

Администратор имеет возможность устанавливать на МУ дополнительные сторонние программы и МП, являющиеся не базовыми и встроенными в ОС Аврора, а разрабатываемыми с использованием официального набора инструментов разработки ПО для ОС Аврора, подробная информация о котором приведена на ресурсе: https://community.omprussia.ru

Установка и управление сторонним ПО может осуществляться администратором следующими способами:

– локально через графический интерфейс следующих МП:
- МП «Файлы» (п.п. 2.4.1.2);
- МП «Terminal» (п.п. 2.4.1.3).

– удаленно с использованием Прикладного программного обеспечения «Аврора Центр» (ППО), следующими способами:
- принудительная установка МП;
- установка МП из предварительно сформированного списка (витрины приложений).

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

2.4.1.1. Разрешение установки

Для разрешения установки стороннего ПО необходимо выполнить следующие действия:

– открыть меню системных настроек, коснувшись значка  на Экране приложений;

– в подразделе «Безопасность» коснуться пункта меню «Недоверенные программы»  , в результате чего отобразится страница «Недоверенное программное обеспечение» (Рисунок 67);

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

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

– подтвердить действия вводом текущего кода безопасности (Рисунок 5);

– коснуться кнопки «Подтвердить» для подтверждения принятия условий использования стороннего ПО либо кнопки «Отменить» для отмены операции (Рисунок 68).

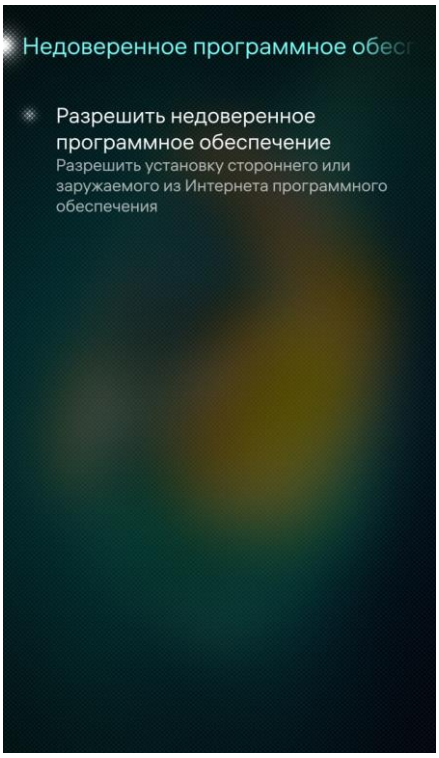

Рисунок 67

Рисунок 68

Для снятия разрешения на установку стороннего ПО необходимо выполнить аналогичные действия.

2.4.1.2. МП «Файлы»

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

– активировать переключатель «Разрешить недоверенное программное обеспечение» в разделе «Недоверенные программы» системных настроек (п.п. 2.4.1.1);

– открыть МП «Файлы», коснувшись значка  на Экране приложений;

– коснуться файла, установку которого необходимо выполнить;

– в открывшемся окне коснуться кнопки «Установить» (Рисунок 69).

После успешной установки на Домашнем экране отобразится соответствующее сообщение «Установка успешна» (Рисунок 70), а значок установленного МП будет отображаться на Экране приложений.

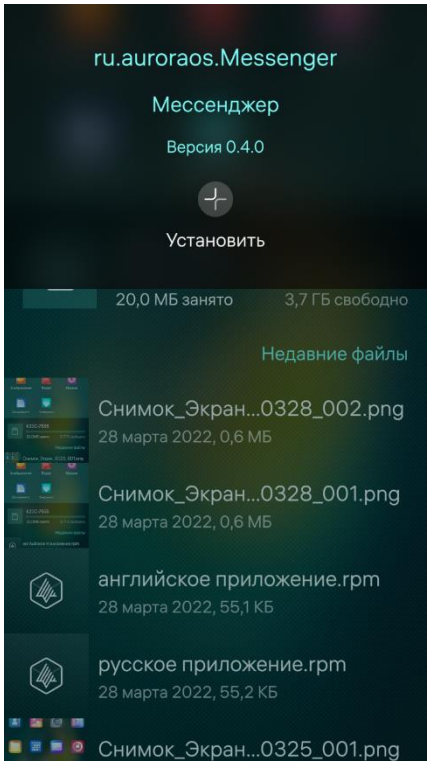

Рисунок 69

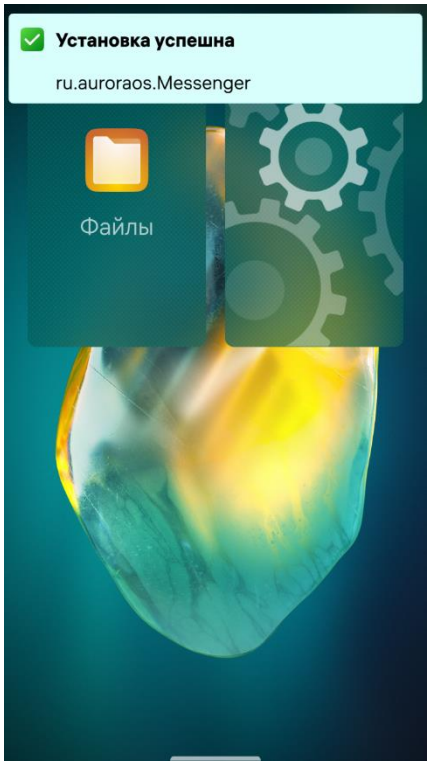

Рисунок 70

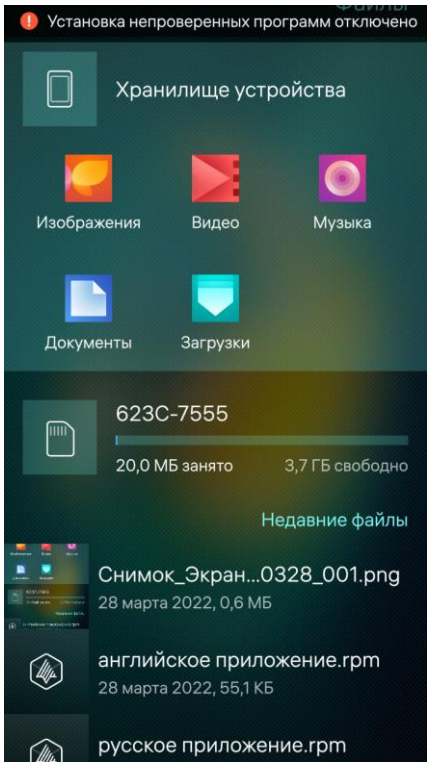

Рисунок 71

В процессе установки стороннего ПО при отключенной опции «Разрешить недоверенное программное обеспечение» на экране МУ отобразится соответствующее сообщение: «Установка недоверенных программ отключено» (Рисунок 71).

2.4.1.3. МП «Terminal»

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

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

– для установки скачанного RPM-пакета:

```
#rpm -ihv имя_пакета
```

– для удаления RPM-пакета:

```
#rpm -e имя_пакета
```

– для просмотра перечня установленных RPM-пакетов:

```
#rpm -qa
```

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

```
#rpm -help
```

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

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

– добавление корневого сертификата УЦ в доверенные (п.п. 2.4.2.2);
– проверка сертификатов (п.п. 2.4.2.3);
– подпись МП (п.п. 2.4.2.4);
– проверка подписи МП (п.п. 2.4.2.5);
– проверка подписи RPM-пакета (п.п. 2.4.2.6);
– запуск МП (2.4.2.7).

2.4.2.1. Общая информация

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

Таблица 1

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

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

Пример команды для генерации ключевых пар и запросов на сертификаты:

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

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

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

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:

– коснуться пункта «Средства разработчика»  в меню системных настроек, в результате чего откроется страница «Инструменты разработчика», на которой необходимо задать пароль;

– подключить МУ к ЭВМ с помощью USB-кабеля;

– скопировать сертификат на МУ посредством протокола передачи медиафайлов (MTP);

– открыть МП «Terminal» и выполнить следующие команды:

```
devel-su
cp <название нового корневого сертификата> /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://путь_к_сертификату/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 необходимо выполнить команду:

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

2.4.2.4. Подпись МП

Для подписи МП его разработчику необходимо выполнить следующую команду:

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

где:

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

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

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

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

где:

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

2.4.2.5. Проверка подписи 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`.

При проверке подписи МП может потребоваться перезагрузка МУ

2.4.2.6. Проверка подписи RPM-пакета

Для проверки подписи пакета необходимо выполнить команду:

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

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

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

2.4.2.7. Запуск МП

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

При запуске МП может потребоваться перезагрузка МУ

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

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! Режим разработчика невозможно отключить после активации!
После активации режима разработчика не допускается использование МУ в ИС, требующих аттестации!

3.1. Активация режима разработчика

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 72) и подтвердить действие вводом кода безопасности;

– на открывшейся странице ознакомится с условиями разработчика и коснуться кнопки «Подтвердить» для подтверждения активации режима разработчика либо кнопки «Отменить» для отмены операции (Рисунок 73).

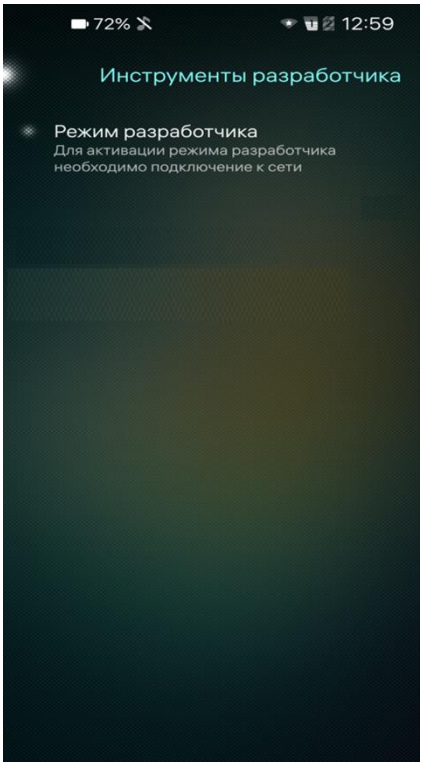

Рисунок 72

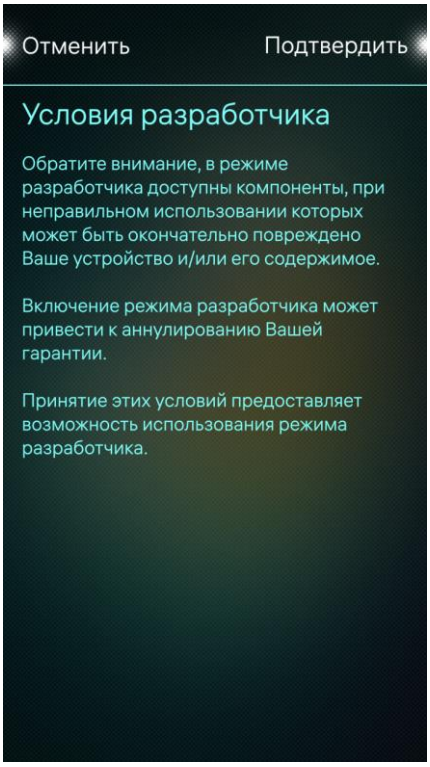

Рисунок 73

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 74) и подтвердив действие вводом кода безопасности;

– задать либо сгенерировать пароль, коснувшись поля «Установить пароль для SSH и доступа», после чего коснуться кнопки «Сохранить» и подтвердить действие вводом кода безопасности (Рисунок 74);

Поле «Установить пароль для SSH и доступа» отображается после активации переключателя «Удаленное соединение».
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 75);

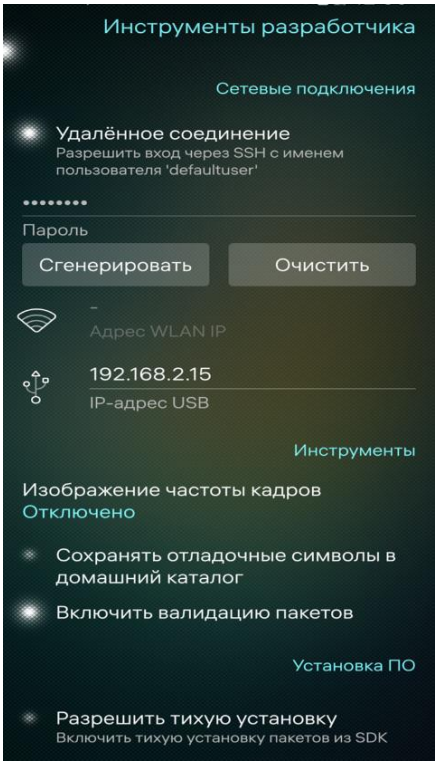

Рисунок 74

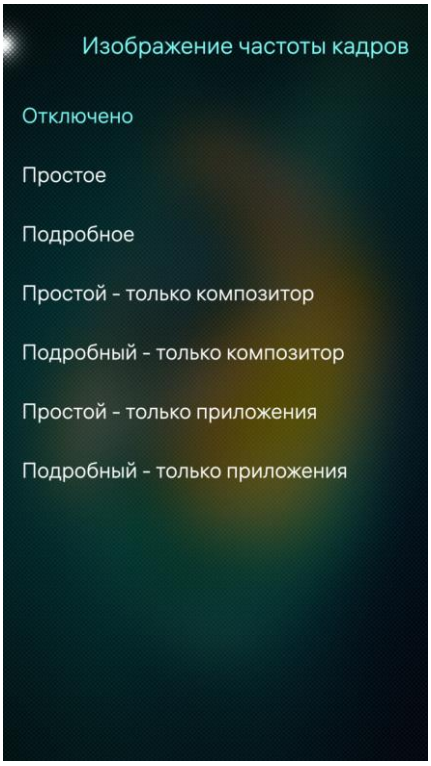

Рисунок 75

– разрешить либо запретить сохранение отладочных символов в домашнем каталоге, коснувшись переключателя «Сохранять отладочные символы в домашний каталог» в подразделе «Инструменты» (см. Рисунок 74);

– включить либо отключить валидацию пакетов, коснувшись переключателя «Включить валидацию пакетов» в подразделе «Инструменты» (см. Рисунок 74);

– разрешить либо запретить тихую установку пакетов из SDK, коснувшись переключателя «Разрешить тихую установку» в подразделе «Установка ПО» (см. Рисунок 74) и подтвердить действие вводом кода безопасности.

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

4. ОПИСАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ

4.1. Регистрация событий безопасности (аудит)

4.1.1. Основная информация

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

ОС Аврора осуществляет регистрацию и хранение:

– сообщений из системного журнала (syslog), ядра (kernel log);

– сообщений, которые процессы служб выводят на стандартные потоки вывода (stdout);

– ошибок (stderr).

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

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

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

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

– результат попытки входа в систему;

– блокирование интерактивного сеанса как по запросу пользователя, так и по истечении установленного периода неактивности пользователя;

– блокировка доступа после установленного количества неуспешных попыток ввода аутентификационной информации;

– истечение срока действия пароля;

– смена пароля;

– запуск процедуры и результат проверки контроля целостности;

– обнаружение нарушения целостности;

– постоянная блокировка МУ;

– результат попытки установки, удаления или обновления пакетов;

– подключение и отключение внешних носителей информации;

– переполнение журнала событий безопасности;

– старт, перезагрузка и выключение ОС;

– добавление правил сетевого фильтра;

– запуск, завершение и изменение конфигурации службы аудита;

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

Каждое событие содержит в себе следующую информацию:

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

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

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

– программу `journalctl`, имеющую интерфейс командной строки;

– программу `dmesg`, имеющую интерфейс командной строки;

– конфигурационный файл `/etc/omp/sdjd`.;

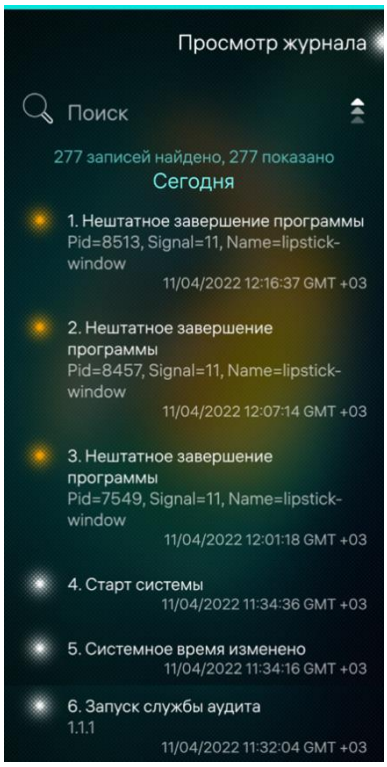

Рисунок 76

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

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

В МП «Журнал» отображается как информация о событиях аудита, так и различная системная информация (Рисунок 76). Подробное описание работы МП приведено в документе «Руководство пользователя»

4.1.4. Просмотр сообщений аудита

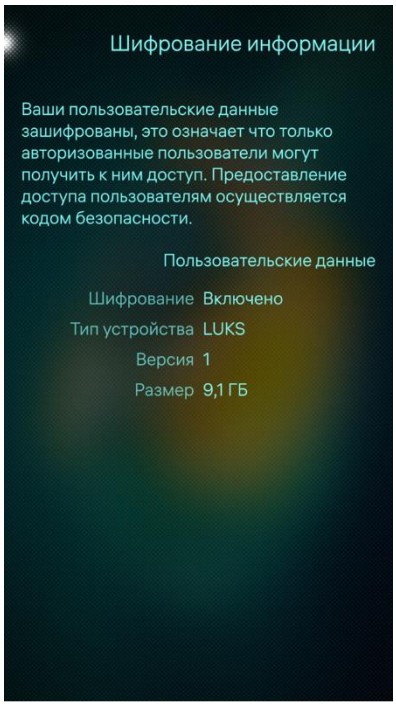

Рисунок 77

Для просмотра шифрованных пользовательских данных (Рисунок 77) 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.

4.2. Идентификация и аутентификация

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

Для работы с объектами системы администратору присваиваются следующие идентификаторы:

– символьный: defaultuser;

– числовой: 100000.

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

– в случае шифрования раздела с домашними каталогами пользователей будет храниться в LUKS-слоте, соответствующем идентификатору пользователя;

– в иных случаях будет храниться в виде свертки, полученной с помощью алгоритма криптографического преобразования sha1.

Для задания кода безопасности при первичной загрузке МУ:

– в корпоративном варианте исполнения[4] пользователю будет необходимо установить код безопасности для доступа к МУ;

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

Необходимо запомнить установленный код безопасности, т.к. он потребуется для дальнейшей работы с МУ.
В случае утраты и/или раскрытия кода безопасности, его необходимо немедленно обновить

В целях предотвращения несанкционированного доступа к МУ с установленной 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;

[4] Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 4).

– просмотра данных учетных записей;
– сброса настроек МУ.

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

4.3. Управление доступом (политики безопасности)

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

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).

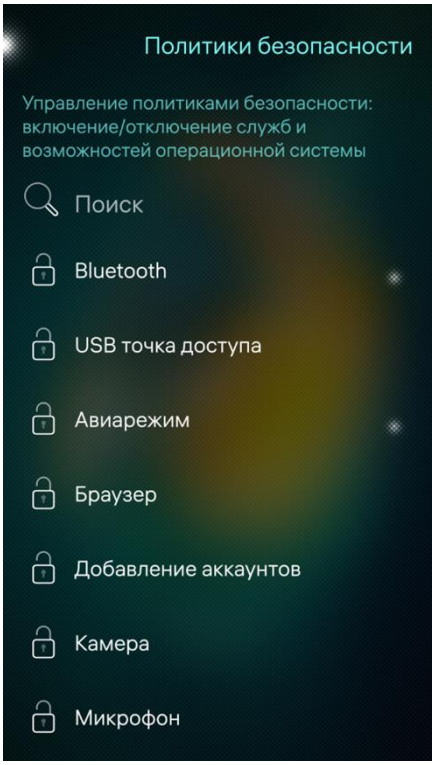

Рисунок 78

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.

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

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

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

Таблица 2

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

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
12	Авиарежим	Использование режима полета	FlightModeToggleEnabled	Разблокирована	GUI
13	Микрофон	Использование микрофона	MicrophoneEnabled	Разблокирована	GUI
14	Браузер	Работа пользователя с браузером	BrowserEnabled	Разблокирована	GUI
15	Добавление аккаунтов	Добавление данных учетных записей	AccountCreationEnabled	Разблокирована	GUI
16	Настройка VPN	Управление VPN-соединениями	VpnConnectionSettingsEnabled	Разблокирована	GUI
17	Настройка VPN-соединения	Настройка/редактирование VPN-соединений	VpnConfigurationSettingsEnabled	Разблокирована	GUI
18	Настройки прокси	Настройка proxy-сервера	NetworkProxySettingsEnabled	Заблокирована	GUI
19	-	Использование Android Debug Bridge	UsbAdbEnabled	Разблокирована	policy.conf
20	-	Настройка мобильных точек доступа	MobileDataAccessPointSettingsEnabled	Разблокирована	policy.conf
21	-	Работа с обновлением ОС	OsUpdatesEnabled	Разблокирована	policy.conf
22	-	Принятие решений о загрузке сторонних пакетов	SideLoadingSettingsEnabled	Разблокирована	policy.conf
23	-	Активация режима разработчика	DeveloperModeSettingsEnabled	Разблокирована	policy.conf
24	-	Установка МП	ApplicationInstallationEnabled	Заблокирована	policy.conf
25	-	Использование режима USB Mass Storage	UsbMassStorageEnabled	Разблокирована	policy.conf

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
26	-	Работа со статистикой интернет-данных	NetworkDataCounterSettingsEnabled	Разблокирована	policy.conf
27	-	Работа со статистикой звонков	CallStatisticsSettingsEnabled	Разблокирована	policy.conf
28	-	Изменение типа технологии мобильной передачи данных	CellularTechnologySettingsEnabled	Разблокирована	policy.conf
29	-	Режим разработчика	UsbDeveloperModeEnabled	Разблокирована	policy.conf
30	-	Режим сетевого адаптера	UsbHostEnabled	Разблокирована	policy.conf
31	-	Режим отладки	UsbDiagnosticModeEnabled	Разблокирована	policy.conf

4.4. Идентификация и аутентификация

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

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

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

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

Таблица 3

№	Элемент	Описание
1	Accounts	Просмотр, модификация и синхронизация учетных записей
2	Ambience	Установка и редактирование тем
3	AppLaunch	Запуск и остановка сервисов systemd
4	ApplicationInstallation	Установка и удаление МП
5	Audio	Воспроизведение и запись аудио, изменение конфигурации

№	Элемент	Описание
6	Bluetooth	Подключение и использование устройств по Bluetooth®
7	Calendar	Просмотр и модификация событий календаря
8	CallRecordings	Доступ к записанным вызовам
9	Camera	Доступ к камере, съемка фото и видео
10	CommunicationHistory	Доступ к истории вызовов и сообщений
11	Contacts	Просмотр и модификация данных контактов
12	Documents	Доступ к каталогу "Documents"
13	Downloads	Доступ к каталогу "Downloads"
14	E-mail	Чтение и отправка электронной почты, доступ к вложениям
15	Internet	Использование сети Интернет
16	Location	Использование геопозиционирования
17	MediaIndexing	Доступ к перечню файлов на МУ
18	Messages	Доступ к чтению и отправке SMS
19	Microphone	Запись аудио с помощью микрофона
20	Music	Доступ к каталогу "Music", плейлистам и обложкам
21	NFC	Подключение и использование устройств NFC
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 данные об устройстве
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

4.5. Изоляция процессов

Решение задачи изоляции адресных пространств процессов основано на архитектуре ядра ОС Аврора, которое обеспечивает собственное изолированное адресное пространство для каждого процесса в системе. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и 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.

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.

4.6. Защита памяти

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

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

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

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

4.7. Подписи RPM-пакетов

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

– для пакетов отключены и не используются GPG подписи;

– подпись разработчика подписывает пакет целиком;

– клиентская подпись подписывает область подписи разработчика;

– каждая последующая подпись добавляется в конец и подписывает предыдущую.

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

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

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

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

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

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

4.8. Фильтрация сетевого потока

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

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

4.9. Контроль целостности

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

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

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

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

4.10. Шифрование раздела с домашними директориями пользователей

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

– 1 слот используется администратором;

– 6 слотов доступны создаваемым учетным записям пользователя;
– 1 слот резервируется для смены паролей.

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

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

– разблокировка домашней директории при загрузке МУ;
– разблокировка UI Lipstick.

Старт пользовательской сессии невозможен без ввода корректного кода безопасности, при превышении количества попыток неверного ввода которого МУ автоматически будет заблокировано.
Время блокировки является фиксированным и составляет 15 минут

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

В настоящем документе приняты следующие термины и сокращения (Таблица 4).

Таблица 4

Термин/ Сокращение	Расшифровка
Администратор	Пользователь, обладающий правами на выполнение операций, связанных с администрированием системы
Варианты исполнения ОС Аврора	1. Корпоративный вариант исполнения – релиз, предназначенный для использования компаниями, у которых есть потребность в использовании доверенных мобильных рабочих мест, на которых не происходит обработка конфиденциальной информации; 2. Сертифицированный вариант исполнения – набор готовых к сертификации и серийному производству артефактов сертифицированного изделия, имеющих сертификат, находящихся на сертификационных испытаниях или подготовленных к проведению сертификационных испытаний. Сертифицированный релиз может поставляться по Лицензионному договору в период прохождения сертификации в согласованной комплектации. После получения сертификата соответствия поставки релиза не осуществляются, а поставляется Сертифицированное изделие
2ФА	Двухфакторная аутентификация
Квота	Объем дискового пространства, выделяемого администратором для записи данных учетных записей пользователей
Криптоконтейнер	Криптографический контейнер
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
Переключатель	Элемент интерфейса ОС Аврора, представляющий собой светящуюся точку, расположенную в поле, и позволяющий выбрать одно из состояний, чаще всего включение или выключение. При активации переключателя точка начинает светиться ярче, чем в неактивном состоянии

Термин/ Сокращение	Расшифровка
Пользователь	Лицо, использующее систему для выполнения заложенных в ней функций
Предприятие-разработчик	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение «Аврора Центр»
ПРД	Правила разграничения доступа
СКЗИ СледопытSSL	Программное средство криптографической защиты информации СледопытSSL
Суперпользователь	Пользователь, обладающий правами на выполнение всех без исключения операций в системе (в системе имеет логин «root»)
Токен	Аутентификационные данные, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам
ФС	Файловая система
ЭВМ	Электронно-вычислительная машина
GUI	Graphical User Interface - разновидность пользовательского интерфейса, в котором элементы интерфейса (меню, кнопки, значки, списки), представленные пользователю на дисплее, исполнены в виде графических изображений
MTP	Media Transfer Protocol – основанный на 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

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Описание изменения	ФИО инициатора	Дата
1.0	Начальная версия	Аносов С. Белянкина Н. Андронова К.	28.04.2022 г.
1.1	Внесены изменения	Аносов С. Белянкина Н. Андронова К.	25.05.2022 г.
1.2	Внесены изменения	Аносов С. Белянкина Н. Андронова К.	31.05.2022 г.
1.3	Внесены изменения	Андронова К.	06.06.2022 г.