ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 3

Версия документа 1.0

Листов 17

2020

АННОТАЦИЯ

Настоящий документ является третьей частью руководства администратора прикладного программного обеспечения «Аврора Центр» релиз 2.2.0 (далее — ППО).

Руководство администратора состоит из трех частей:

– «Руководство администратора. Часть 1»;

– «Руководство администратора. Часть 2»;

– «Руководство администратора. Часть 3».

Настоящий документ содержит общую информацию о ППО, описание установки и конфигурационных файлов подсистемы Платформа управления (ПУ), а также описание установки мобильных приложений (МП) Аврора Центр.

СОДЕРЖАНИЕ

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Назначение и состав ППО

ППО предназначено для управления мобильными устройствами (МУ) под управлением защищенной мобильной операционной системы общего назначения на базе Sailfish Mobile OS RUS, имеющей действительный сертификат соответствия ФСТЭК России, и/или операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России, (далее — ЗМОС) и управления жизненным циклом приложений, а также для автоматизированной обработки следующих видов информации:

– общедоступная информация;

– информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, подлежащая защите в соответствии с требованиями действующего законодательства Российской Федерации в области информационной безопасности.

ППО является прикладным программным обеспечением с встроенными механизмами защиты информации от несанкционированного доступа. ППО предназначено для использования:

– в государственных информационных системах, не содержащих информации, составляющей государственной тайны, до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;

– в информационных системах персональных данных до 1 уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21;

– в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 августа 2014 г. № 31.

ППО состоит из следующих подсистем:

– подсистема безопасности;

– подсистема «Маркет»;

– подсистема Платформа управления.

Взаимодействие между подсистемами и компонентами подсистем осуществляется с использованием протокола HTTP стандарт RFC 2616, при этом обмен данными осуществляется в формате RFC 8259 (JSON).

В качестве сервера базы данных (БД) используется сервер с установленной системой управления базами данных (СУБД) Postgres Pro или PostgreSQL 11, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

1.2. Назначение ПУ

ПУ предназначен для обеспечения:

– управления отдельными МУ (оперативное управление);

– управления группами МУ;

– управления политиками;

– управления записями о МУ;
– управления записями о пользователях МУ;
– управления приложениями на МУ;
– контроля состояния устройств;
– контроля применения политик на МУ;
– мониторинга событий и предоставление отчетности;
– предоставления интерфейса пользователям подсистемы.

1.3. Состав и функции ПУ

ПУ состоит из следующих компонентов:

– Консоль администратора ПУ;
– МП Аврора Центр;
– Сервер приложений ПУ.

С помощью Консоли администратора ПУ осуществляется взаимодействие Администратора Платформы Управления с ПУ.

С помощью МП Аврора Центр осуществляется активация МУ в ППО.

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

– включать и выключать доступ к камере на МУ;
– блокировать и разблокировать МУ;
– очищать данные (восстанавливать заводские настройки) МУ;
– устанавливать и удалять приложения на МУ;
– получать данные о состоянии МУ;
– устанавливать расписание обмена данными с МУ;
– включать и выключать доступ к управлению WLAN настройками;

- включать и выключать доступ к WLAN на МУ;
- устанавливать настройки стандартного почтового клиента;
- изменять пароль учетной записи пользователя в ЗМОС.

С помощью МП Аврора Центр осуществляется активация МУ ППО.

Сервер приложений ПУ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа ППО данные о настройках ЗМОС, а также формировать управляющие сообщения для МП Аврора Центр.

2. СРЕДА ФУНКЦИОНИРОВАНИЯ ППО

2.1. Описание установки компонентов среды функционирования ППО

Описание среды функционирования ППО и описание процесса установки среды функционирования приведено в документе «Прикладное программное обеспечение «Аврора Центр» «Руководство администратора. Часть 1».

2.2. Действия по реализации функций безопасности среды функционирования ППО

2.2.1. Установка, настройка и эксплуатация СЗИ от НСД

Эксплуатация ППО и СУБД должна осуществляться в одной из следующих ОС:

– CentOS версии 7 с установленными СЗИ от НСД Dallas Lock Linux, или СЗИ от НСД Secret Net LSP, или СЗИ от НСД Аккорд ХК;

– Альт 8 СП (сертификат соответствия ФСТЭК России № 3866, действителен до 10 августа 2023 г.).

Установка СЗИ от НСД должна осуществляться после установки ППО.

Установка, настройка и эксплуатация СЗИ от НСД и ОС Альт 8 СП должна осуществляться в соответствии с эксплуатационной документацией на СЗИ (ОС).

2.2.2. Меры по межсетевому экранированию

В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы с использованием межсетевого экрана требуемого класса защиты.

Межсетевой экран должен пропускать трафик только на внешние порты ППО, приведенные в таблице (Таблица 1), остальной трафик должен быть запрещен.

Таблица 1

Сервис (модуль)	Порт
Auth public API gateway	http://<сервер приложения>:8018
Auth admin API gateway	http://<сервер приложения>:8019
AMM device API gateway	http://<сервер приложения>:8012
AMM admin API gateway	http://<сервер приложения>:8011
Aurora market admin API gateway	http://<сервер приложения>:8015
Aurora market development API gateway	http://<сервер приложения>:8014
Aurora market client API gateway	http://<сервер приложения>:8016

ПРИМЕЧАНИЕ. Рекомендуется запретить доступ к ППО привилегированных пользователей из-за пределов контролируемой зоны, запретив доступ к Консоли администратора ПБ. Так же при необходимости можно запретить доступ к остальным веб-консолям. Для этого необходимо запретить трафик на требуемых портах в соответствии с информацией из Таблицы 8 документа «Прикладное программное обеспечение «Аврора Центр» «Руководство администратора. Часть 1».

3. ОПИСАНИЕ УСТАНОВКИ ПУ

3.1. Порядок действия по приемке

Описание порядка действия по приемке приведено в документе «Прикладное программное обеспечение «Аврора Центр» «Руководство администратора. Часть 1».

3.2. Установка

Описания процесса установки приведено в документе «Прикладное программное обеспечение «Аврора Центр» «Руководство администратора. Часть 1».

3.3. Настройки конфигурационных файлов

Описание конфигурационных файлов ПУ приведено в документе «Прикладное программное обеспечение «Аврора Центр» «Руководство администратора. Часть 1».

4. ОПИСАНИЕ УСТАНОВКИ МП АВРОРА ЦЕНТР

4.1. Установка МП на МУ с помощью приложения «Терминал»

Для установки МП на МУ с помощью приложения «Терминал» необходимо выполнить следующие действия:

– подключить МУ к ПЭВМ с помощью USB-кабеля;

– на МУ переключиться в режим «Протокол передачи мультимедиа (MTP)», в результате в ОС отобразится внешний носитель «INOI R7» (Рисунок 1);

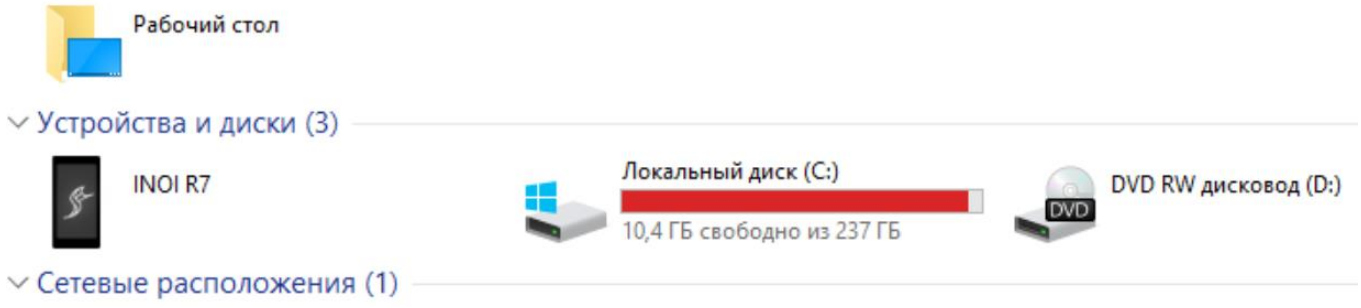

Рисунок 1

– перейти в каталог Downloads и скопировать в него загрузочный модуль МП (RPM-пакеты), при этом:

1) при установке МП на защищенную мобильную операционную систему общего назначения на базе Sailfish Mobile OS RUS необходимо скопировать следующие файлы загрузочных модулей:

- libomp-crypto-storage-1.3.2+1-1.armv7hl.rpm;
- libomp-oauth2-rp-1.3.3+1-1.armv7hl.rpm;
- omp-appmanager-0.2.2+2-1.armv7hl.rpm;
- omp-emm-client-0.11.26+1-1.54.1.omp.armv7hl.rpm;
- qzxing-2.4-1.armv7hl.rpm;

2) при установке МП на ОС Аврора необходимо скопировать следующие файлы загрузочных модулей:

- libomp-crypto-storage-1.3.2+1-1.armv7hl.rpm;

- libomp-oauth2-rp-1.3.3+1-1.armv7hl.rpm;
- omp-appmanager-0.2.2+2-1.armv7hl.rpm;
- omp-emm-client-0.11.26+1-1.54.1.omp.armv7hl.rpm;

– используя МП МУ «Терминал», перейти в каталог, где расположены собранные RPM-пакеты, подписанные ключом предприятия-разработчика.

Необходимо перейти в каталог /home/nemo/Downloads с помощью команды:

```
cd /home/nemo/Downloads/
```

Предварительно необходимо задать пароль для приложения «Терминал». Для чего необходимо выполнить следующие действия:

– провести по экрану снизу вверх в сетке приложений коснуться значка  . Отобразится меню настроек;

– в меню настроек перейти к разделу «Настройка защиты»;

– выбрать пункт «Доступ к терминалу» и сгенерировать пароль (либо задать пароль вручную).

– установить пакеты, с помощью команды:

```
devel-su pkcon install-local *.rpm
```

4.2. Установка МП на МУ с помощью образа vendor-data.img

Раздел vendor-data является разделом в файловой системе МУ, в который помещаются приложения (обновления приложений). Установка МП, хранящихся в разделе vendor-data, осуществляется во время запуска МУ.

4.2.1. Сборка раздела vendor-data

Сборка раздела vendor-data должна осуществляться в ОС Ubuntu версии 16.04.

Для сборки раздела vendor-data необходимо выполнить следующие действия:

– создать каталог с произвольным именем, в котором приводится сборка раздела vendor-data;

– перейти в данный каталог и создать подкаталог rpm;

– скопировать RPM-пакеты (загрузочный модуль МП) в каталог rpm;

– запустить скрипт сборки раздела vendor-data:

```
dd if=/dev/zero of=vendor-data.img bs=1M count=10
mkfs.ext4 vendor-data.img
mkdir -p temp
mount vendor-data.img temp
rm -rf temp/*
mkdir temp/rpm
cp rpm/*.rpm temp/rpm
umount temp
rm -rf temp
```

4.2.2. Подпись образа vendor-data.img

Подписание образа vendor-data.img осуществляется в соответствии с эксплуатационной документацией на утилиту (программу) используемую для подписания образа.

4.2.3. Прошивка образа vendor-data.img на МУ

Для прошивки образа vendor-data.img на МУ необходимо выполнить следующие действия:

– установить в ОС CentOS пакет fastboot, с помощью команды:

```
apt install fastboot
```

– выключить МУ, выполнив следующие действия:

- нажать и удерживать кнопку питания на торцевой стороне корпуса до появления окна интерфейса выключения;
- коснуться кнопки выключения  на экране МУ;
- зажать кнопку увеличения громкости и одновременно подсоединить МУ к ПЭВМ с помощью USB-кабеля;

- нажать и удерживать кнопку увеличения громкости до появления в верхнем углу экрана надписи «long press power key 8s reboot phone». Это означает, что МУ загрузилось в режиме прошивки;
- отпустить кнопку увеличения громкости;

– запустить процесс прошивки с помощью команды:

```
sudo fastboot flash cache vendor-data-sign.img
```

– после окончания процесса прошивки отсоединить USB-кабель от МУ;

– включить МУ, нажать и удерживать кнопку питания в течение 8-10 секунд.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

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

Таблица 2

Термин/ Сокращение	Расшифровка
БД	База данных
ЗМОС	Защищенная мобильная операционная система общего назначения на базе Sailfish Mobile OS RUS, имеющая действительный сертификат соответствия ФСТЭК России, и/или операционная система Аврора, имеющая действительный сертификат соответствия ФСТЭК России
ИС	Информационная система
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение «Аврора Центр»
Предприятие-разработчик	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ПУ	Подсистема Платформа управления
ПЭВМ	Персональная электронная вычислительная машина
СУБД	Система управления базами данных
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

Термин/ Сокращение	Расшифровка
HTTP	HyperText Transfer Protocol – протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
RPM-пакет	Файл формата RPM, позволяющий устанавливать, удалять и обновлять приложение на МУ

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Описание изменения	ФИО инициатора	Дата
1.0	Начальная версия	Шевченко Д.	13.03.2020 г.