ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 2

Подсистема «Маркет»

Версия документа 1.0

Листов 17

2020

АННОТАЦИЯ

Настоящий документ является второй частью руководства администратора прикладного программного обеспечения «Аврора Центр» релиз 2.2.2 (далее — ППО).

Руководство администратора состоит из четырех частей:

– «Руководство администратора. Часть 1. Подсистема безопасности»;

– «Руководство администратора. Часть 2. Подсистема «Маркет»»;

– «Руководство администратора. Часть 3. Подсистема Платформа управления»;

– «Руководство администратора. Часть 4. Подсистема установки системных пакетов».

Настоящий документ содержит общую информацию о ППО, описание установки и конфигурационных файлов подсистемы «Маркет» (ПМ), а также описание установки мобильных приложений (МП) «Аврора Маркет».

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;

– подсистема установки системных пакетов.

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[1], PostgreSQL 10.4 или PostgreSQL 11.2, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

[1] СУБД «Postgres Pro» (сертификат соответствия ФСТЭК России № 3637, действителен до 05 октября 2019 г., техническая поддержка до 05.10.2029 г.)

1.2. Назначение ПМ

ПМ предназначен для обеспечения:

– управления жизненным циклом приложений (загрузка, согласование и публикация);

– управления дистрибуцией опубликованных приложений (скачивание, установка, обновление, удаление МП на МУ);

– предоставления интерфейса пользователям подсистемы.

1.3. Состав и функции ПМ

ПМ состоит из следующих компонентов:

– Консоль администратора ПМ;

– Консоль разработчика ПМ;

– МП «Аврора Маркет»;

– Сервер приложений ПМ.

С помощью Консоли администратора ПМ Администратор Аврора Маркет получает приложения и данные о приложениях, а также осуществляет согласование приложений с целью их публикации либо отказывает в публикации.

С помощью Консоли разработчика ПМ осуществляется добавление новых и обновление ранее загруженных приложений в ПМ, а также осуществляется доступ к данным о приложениях.

Компонент МП «Аврора Маркет» выполняется на МУ под управлением ЗМОС, служит для отображения данных о приложениях, а также для загрузки, установки, обновления и удаления приложений на МУ.

Сервер приложений ПМ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа ППО информацию о приложениях. Непосредственно сами приложения, а также иконки и скриншоты приложений хранятся в файловом хранилище.

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 «Руководство администратора. Часть 1. Подсистема безопасности».

2.2. Действия по реализации функций безопасности среды функционирования ППО

2.2.1. Установка, настройка и эксплуатация средства защиты информации от несанкционированного доступа (СЗИ НСД)

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

– CentOS версии 7 с установленными СЗИ НСД «Dallas Lock Linux»[2], или средства защиты информации (СЗИ) «Secret Net LSP»[3], или специальное программное обеспечение (СПО) СЗИ НСД «Аккорд-Х К»[4]

– Альт 8 СП[5].

Установка СЗИ НСД должна осуществляться после установки ППО.

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

[2] СЗИ НСД «Dallas Lock Linux» (сертификат соответствия ФСТЭК России № 3594, действителен до 04 июля 2024 г.)
[3] СЗИ «Secret Net LSP» (сертификат соответствия ФСТЭК России № 2790, действителен до 18 декабря 2023 г.)
[4] СПО СЗИ НСД «Аккорд-Х К» (сертификат соответствия ФСТЭК России № 3760, действителен до 04 июля 2020 г., техническая поддержка до 31.01.2025 г.)
[5] Альт 8 СП (сертификат соответствия ФСТЭК России № 3866, действителен до 10 августа 2023 г.)

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

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 «Руководство администратора. Часть 1. Подсистема безопасности»

3. ОПИСАНИЕ УСТАНОВКИ ПМ

3.1. Порядок действия по приемке

Описание порядка действия по приемке приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности».

3.2. Установка

Описания процесса установки приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности».

3.3. Настройки конфигурационных файлов

Описание конфигурационных файлов ПМ приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности».

4. ОПИСАНИЕ УСТАНОВКИ МП «АВРОРА МАРКЕТ»

ВНИМАНИЕ! При копировании команд в формате PDF из настоящего раздела будьте внимательны. Администратор/разработчик должен проверять результат копирования команды на экране.

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

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

1) подключить МУ к ПЭВМ с помощью USB-кабеля;

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

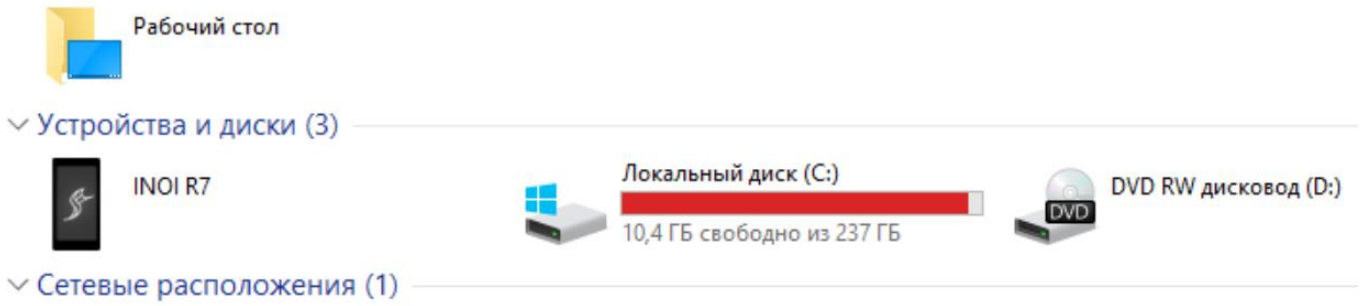

Рисунок 1

3) перейти в каталог Downloads и скопировать в него загрузочный модуль МП (RPM-пакеты);

Загрузочный модуль МП «Аврора Маркет» для Sailfish Mobile OS RUS находится в каталоге \mobile_app\aurora_market\OS_Sailfish\ DVD с загрузочным модулем.

Загрузочный модуль МП «Аврора Маркет» для ОС Аврора находится в каталоге \mobile_app\aurora_market\OS_Aurora\ DVD с загрузочным модулем.

4) используя МП МУ «Терминал», перейти в каталог с RPM-пакетами МП «Аврора Маркет», с помощью команды:

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

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

– провести по экрану снизу вверх на экране приложений и 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).

5) 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:

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

2) перейти в данный каталог и создать подкаталог rpm;

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

Загрузочный модуль МП «Аврора Маркет» для Sailfish Mobile OS RUS находится в каталоге \mobile_app\aurora_market\OS_Sailfish\ DVD с загрузочным модулем.

Загрузочный модуль МП «Аврора Маркет» для ОС Аврора находится в каталоге \mobile_app\aurora_market\OS_Aurora\ DVD с загрузочным модулем.

4) 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:

1) установить в ОС CentOS пакет fastboot, с помощью команды:

```
apt install fastboot
```

2) выключить МУ, выполнив следующие действия:

– коснуться 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;

3) запустить процесс прошивки с помощью команды:

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

4) после окончания процесса прошивки отсоединить USB-кабель от МУ;

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

4.3. Установка МП на МУ с помощью подсистемы Платформа управления

Установка МП «Аврора Маркет» также может осуществляться с помощью подсистемы Платформа управления, подробное описание приведено в документе «Руководство пользователя. Часть 2. Подсистема Платформа управления».

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
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ПБ	Подсистема безопасности
ПМ	Подсистема «Маркет»
ППО	Прикладное программное обеспечение «Аврора Центр»
ПЭВМ	Персональная электронная вычислительная машина
СЗИ	Средства защиты информации
СЗИ НСД	Средства защиты информации от несанкционированный доступ
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
Субъект доступа	Лицо или процесс, действия которого регламентируются правилами разграничения доступа. Субъектами доступа являются пользователи и МП «Аврора Центр» (процесс МП «Аврора Центр») ППО. Субъекту доступа может быть назначена одна или несколько из следующих

Термин/ Сокращение	Расшифровка
	перечисленных ролей: – роль МП «Аврора Центр» - роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ); – роль Администратора учетных записей позволяет осуществлять управление учетными записями; – роль Оператора аудита позволяет осуществлять действия по работе с журналом регистрации событий ППО; – роль Администратора Платформы Управления позволяет осуществлять все действия по управлению ПУ через интерфейс ППО; – роль Администратора Аврора Маркет позволяет осуществлять все действия по управлению ПМ через интерфейс системы; – роль Разработчика позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях; – роль Пользователя Аврора Маркет позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
MTP	Media Transfer Protocol - аппаратно-независимый протокол, основанный на PTP

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
USB-кабель	Universal Serial Bus - последовательный интерфейс для подключения периферийных устройств к вычислительной технике

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Содержание изменения	ФИО инициатора	Дата
1.0	Начальная версия	Шевченко Д.	06.07.2020 г.