

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«АВРОРА ЦЕНТР»

Руководство администратора. Часть 2

Подсистема «Маркет»

Версия документа 1.0

Листов 17

АННОТАЦИЯ

Настоящий документ является второй частью руководства администратора прикладного программного обеспечения «Аврора Центр» релиз 2.5.0 (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 обновления ОС».

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	4
1.1. Назначение и состав ППО.....	4
1.2. Назначение ПМ	5
1.3. Состав и функции ПМ.....	6
2. Среда функционирования ППО	7
2.1. Описание установки компонентов среды функционирования ППО.....	7
2.2. Действия по реализации функций безопасности среды функционирования ППО	7
2.2.1. Установка, настройка и эксплуатация средства защиты информации от несанкционированного доступа (СЗИ НСД)	7
2.2.2. Меры по межсетевому экранированию.....	8
3. Описание установки ПМ	9
3.1. Порядок действия по приемке.....	9
3.2. Установка	9
3.3. Настройки конфигурационных файлов.....	9
4. Описание настройки ПМ	10
5. Описание установки МП «Аврора Маркет»	12
5.1. Установка МП на МУ с помощью приложения «Терминал»	12
5.2. Установка МП на МУ с помощью подсистемы Платформа управления.....	13
Перечень терминов и сокращений	14

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Назначение и состав ППО

ППО предназначено для управления мобильными устройствами (МУ), функционирующими под управлением операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России, и управления жизненным циклом МП, 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 обновления ОС.

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 Pro¹ или PostgreSQL, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

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

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 ОС Аврора, 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;

– CentOS версии 8⁵ или выше;

– Альт 8 СП⁶.

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 ППО под управлением ОС CentOS 8 не допускается использовать в информационных системах, обрабатывающих информацию ограниченного доступа, требующую защиты в соответствии с законодательством РФ.

⁶ 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.

Подробная информация по межсетевому экранированию приведена в документе «Руководство администратора. Часть 1. Подсистема безопасности».

3. ОПИСАНИЕ УСТАНОВКИ ПМ

3.1. Порядок действия по приемке

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

3.2. Установка

Описание 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 НАСТРОЙКИ ПМ

Настройка ПМ заключается в настройке файлового хранилища ПМ.

Настройку файлового хранилища необходимо выполнять после установки ППО

Для настройки файлового хранилища ПМ необходимо выполнить следующие действия:

- на Сервере приложений ПМ создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, rpm-пакеты), загружаемые разработчиками, либо каталог, к которому будет монтироваться единое файловое хранилище;

- в случае если файлы МП будут храниться в каталоге на Сервере приложений ПМ, необходимо создать каталог в соответствии с параметром `filestorage_path` конфигурационного файла `config/vars/_vars.yml`, в созданном каталоге создать каталог `applications-api` и сделать владельцем данного каталога пользователя `ocs`, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs/appstore/applications-api
sudo chown ocs:ocs /ocs/appstore/applications-api
```

Параметр `filestorage_path` конфигурационного файла `config/vars/_vars.yml` может иметь следующий вид:

```
filestorage_path: "/ocs/appstore"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности»

- при использовании единого файлового хранилища для хранения файлов МП на Сервере приложений ПМ необходимо создать каталог `/ocs` и сделать владельцем данного каталога пользователя `ocs`, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs
sudo chown ocs:ocs /ocs
```

ВНИМАНИЕ! При эксплуатации ППО в кластерной конфигурации все ноды Сервера приложений ПМ должны иметь доступ к единому файловому хранилищу. Соответственно все ноды Сервера приложений ПМ должны быть настроены на работу с данным файловым хранилищем.

Пример настройки единого файлового хранилища и работы Сервера приложений ПМ (ноды Сервера приложений ПМ) приведен в документе «Руководство администратора. Часть 1. Подсистема безопасности».

5. 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.

5.1. 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);

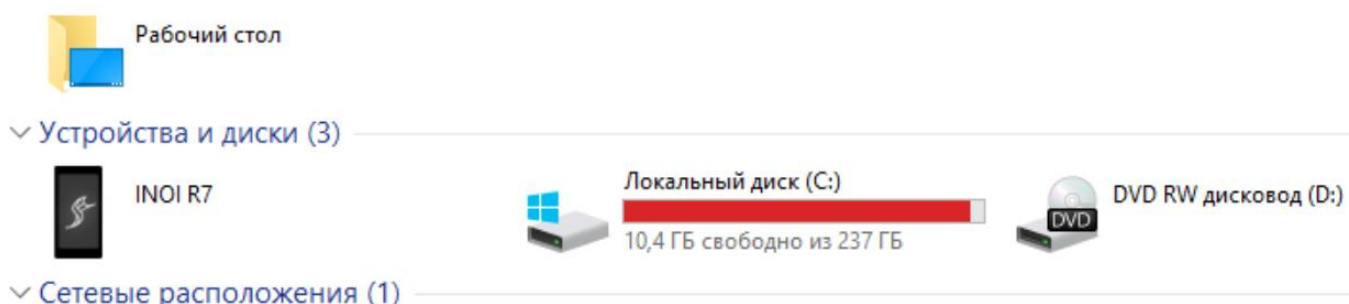


Рисунок 1

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


Загрузочный модуль МП «Аврора Маркет», в зависимости от версии ОС, находится на DVD с загрузочным модулем в каталоге:

- /mobile_apps/aurora_market/3.2.2/ (для ОС Аврора версии 3.2.2);
- /mobile_apps/aurora_market/3.4.0/ (для ОС Аврора версии 3.4.0);

- 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
```

5.2. 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 1).

Таблица 1

Термин/ Сокращение	Расшифровка
БД	База данных
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 несанкционированного доступа
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
Субъект доступа	<p>Лицо или процесс, действия которого регламентируются правилами разграничения доступа.</p> <p>Субъектами доступа являются пользователи и МП «Аврора Центр» (процесс МП «Аврора Центр») ППО. Субъекту доступа может быть назначена одна или несколько из следующих перечисленных ролей:</p> <ul style="list-style-type: none"> – МП «Аврора Центр» – роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ);

Термин/ Сокращение	Расшифровка
	<ul style="list-style-type: none"> – Администратор учетных записей – роль позволяет осуществлять управление учетными записями; – Оператор аудита – роль позволяет осуществлять действия по работе с журналом регистрации событий ППО; – Администратор Платформы Управления – роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО; – Администратор Аврора Маркет – роль позволяет осуществлять все действия по управлению ПМ через интерфейс ППО; – Разработчик – роль позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях; – Пользователь Аврора Маркет – роль позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
МТР	Media Transfer Protocol – аппаратно-независимый протокол, основанный на RTP
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

Термин/ Сокращение	Расшифровка
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	Иванова Н.	13.04.2021 г.