ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 3

Подсистема Платформа управления

Версия документа 1.0

Листов 20

2021

АННОТАЦИЯ

Настоящий документ является третьей 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 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), 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 Pro[1] 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 ПУ

ПУ предназначена для обеспечения:

– управления отдельными МУ (оперативное управление);
– управления группами МУ;
– управления политиками;

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

- управления офлайн-сценариями;
- 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 ОС Аврора, служит для получения управляющих сообщений от Сервера приложений ПУ и передачи их компонентам ОС Аврора, а также передачи на Сервер приложений ПУ сведений о настройках и конфигурации ОС Аврора. В зависимости от управляющего сообщения или офлайн-сценария, полученного от Сервера приложений ПУ, МП «Аврора Центр» посредством вызова интерфейсных функций ОС Аврора имеет возможность:

- включать и выключать доступ к камере на МУ;
- включать и выключать доступ к браузеру на МУ;
- обновлять версию ОС на МУ;
- блокировать и разблокировать МУ;

- очищать данные (восстанавливать заводские настройки) МУ;
- устанавливать и удалять приложения на МУ;
- получать данные о состоянии МУ и событиях безопасности МУ;
- получать логи с МУ;
- устанавливать расписание обмена данными с МУ;
- включать и выключать доступ к управлению WLAN настройками;
- включать и выключать доступ к WLAN на МУ;
- включать и выключать доступ к точке доступа WLAN на МУ;
- ограничивать и предоставлять доступ к МТР;
- ограничивать и предоставлять доступ к Bluetooth (функционал доступен для версии ОС Аврора 4.0.1 и выше);
- изменять пароль учетной записи пользователя в ОС Аврора;
- блокировать МУ при смене SIM-карты (офлайн-сценарий);
- блокировать МУ при отсутствии связи с сервером (офлайн-сценарий);
- блокировать МУ при входе в зону действия WLAN (офлайн-сценарий);
- блокировать и разблокировать МУ при нахождении вне зоны действия WLAN (офлайн-сценарий).

Сервер приложений ПУ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа ППО данные о настройках ОС Аврора, 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 «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.

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

3. ОПИСАНИЕ УСТАНОВКИ ПУ

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 ПУ приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности».

4. ОПИСАНИЕ НАСТРОЙКИ ПУ

4.1. Настройка подключения ПУ к серверу LDAP

Для настройки взаимодействия ППО с сервером LDAP необходимо в секции «ldap_server» файла развертывания ПУ (файл: install-apps/config/vars/_vars.yml) задать требуемые значения:

- address — адрес расположения сервера LDAP;
- parent_group — группа, с которой будет производится экспорт данных из сервера LDAP;
- user_cn — логин технической учетной записи сервера LDAP;
- password — пароль от технической учетной записи сервера LDAP;
- page_size — количество элементов, которое будет импортировано за одну итерацию.

Подробное описание параметров приведено в документе «Руководство администратора. Часть 1. Подсистема безопасности».

Пример настройки подключения к серверу LDAP в _vars.yml:

```
    ldap_server:
    address:  "ldap://dc01.omptest.test"          # LDAP server address
    parent_group:   "ou=Test,DC=omptest,DC=local"         #   LDAP   root
organisation unit to sync from
    user_cn: "Admin"                                  # LDAP user name
    password: "Admin"                                 # LDAP password
    page_size: 1000                                  # how many entries will
be returned on LDAP queries
```

Описание требований к данным, содержащимся в Active Directory, приведено в таблице (Таблица 1).

Таблица 1

Параметр	Описание	Примечание
Group	Название группы пользователей. Формат: от 3 до 64 символов	Если группа пользователей МУ уже существует, то выполняется привязка группы к пользователям МУ
E-mail (обязательный)	Рабочая почта пользователя МУ. Формат: <логин>@<доменное_имя>, от 2 до 256 символов	Рабочая почта пользователя МУ должна быть уникальной
First_name (обязательный)	Имя пользователя МУ. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	
Last_name (обязательный)	Фамилия. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	
Patronymic	Отчество. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	
Job_title	Должность. Формат: от 2 до 256 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	
Phone_number	Номер телефона. Формат: от 2 до 64 символов. Только цифры	

Параметр	Описание	Примечание
IMEI	IMEI МУ. Формат: 15 символов. Пример: 356399111511206	Для МУ, которое нужно привязать к пользователю, обязательно должен быть указан IMEI, если не указан MACWLAN. Если МУ поддерживает работу двух SIM-карт, то в поле «IMEI» допускается ввод любого из двух значений IMEI. МУ должно быть предварительно добавлено в ПУ, чтобы выполнилась привязка пользователя к МУ
MACWLAN	MACWLAN МУ. Формат: 17 символов с разделителем «:». Пример: c9:2e:da:a2:46:f5	Для МУ, которое нужно привязать к пользователю, обязательно должен быть указан MACWLAN, если не указан IMEI. МУ должно быть предварительно добавлено в ПУ, чтобы выполнилась привязка пользователя к МУ

4.2. Настройка взаимодействия Сервера приложений ПУ с Сервисом уведомлений Аврора

При необходимости взаимодействия Сервера приложений ПУ с Сервисом уведомлений Аврора (СУА) необходимо выполнить следующие настройки:

4.2.1. Зарегистрировать в СУА проект и получить конфигурационные файлы с настройками: push-mobile-app.yml и push-server.yml

4.2.2. Скопировать полученные конфигурационные файлы в каталог config/subsystems/emm/vars/ сценариев установки ППО

4.2.3. В конфигурационном файле config/vars/_vars.yml задать значения следующих параметров:

– push_public_address - публичный адрес СУА (значение параметра должно соответствовать значению параметра push_public_address в конфигурационном файле push-server.yml);

– push_mobile_hostname - имя хоста СУА, к которому будет подключаться Push-клиент (Push-демон);

– push_mobile_port - номер порта СУА, к которому будет подключаться Push-клиент (Push-демон);

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

4.2.4. Переустановить подсистему ПУ в соответствии с документом «Руководство администратора. Часть 1. Подсистема безопасности».

5. ОПИСАНИЕ УСТАНОВКИ МП «АВРОРА ЦЕНТР»

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);

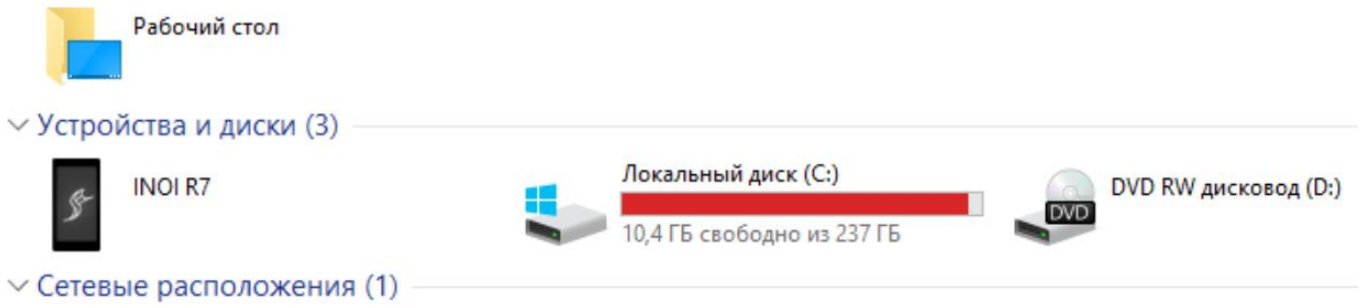

Рисунок 1

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

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

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

4) используя МП МУ «Терминал», перейти в каталог с RPM-пакетами МП «Аврора Центр», 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 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
```

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

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

Таблица 2

Термин/ Сокращение	Расшифровка
БД	База данных
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ПБ	Подсистема безопасности
ППО	Прикладное программное обеспечение «Аврора Центр»
ПУ	Подсистема Платформа управления
ПЭВМ	Персональная электронная вычислительная машина
СЗИ	Средства защиты информации
СЗИ НСД	Средства защиты информации от несанкционированного доступа
СПО	Специальное программное обеспечение
СУА	Сервис уведомлений Аврора
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 перечисленных ролей: – МП «Аврора Центр» - роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей,

Термин/ Сокращение	Расшифровка
	который управляет МУ); – 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 системы; – 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
MTP	Media Transfer Protocol - аппаратно-независимый протокол, основанный на PTP
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

Термин/ Сокращение	Расшифровка
	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	Иванова Н.	13.04.2021 г.