ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 4

Подсистема установки системных пакетов

Версия документа 1.1

Листов 16

2020

АННОТАЦИЯ

Настоящий документ является четвертой 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 установки системных пакетов (ПУСП).

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 ПУСП

ПУСП предназначен для обеспечения:

– предоставления информации о системных пакетах;

– управления дистрибуцией системных пакетов.

1.3. Состав и функции ПУСП

ПУСП состоит из следующих компонентов:

– Сервер приложений ПУСП.

Сервер приложений ПУСП представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять следующие данные о системных пакетах:

– информацию о версиях;

– адрес хранилища системных пакетов.

Для хранения и дистрибуции системных пакетов применяется файловый сервер, развернутый с использованием Nginx.

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
Файловый сервер ПУСП	http://<сервер приложения>:8030

Рекомендуется запретить доступ к ППО привилегированных пользователей из-за пределов контролируемой зоны, запретив доступ к Консоли администратора ПБ. Также 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 ПУСП

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

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».

Так как мобильное приложение не поддерживает работу с не стандартными портами, поэтому на сервере приложений ПУСП необходимо настроить перенаправление таких запросов на порт 8030 файлового сервера ПУСП. Для этой цели можно использовать либо отдельное доменное имя, либо дополнительный путь в URL.

Далее приведен пример настройки перенаправления запросов на порт 8030 файлового сервера ПУСП:

3.2.1. В каталоге /etc/nginx/conf.d/ сервера приложений ПУСП создать файл ssu.conf со следующим содержимым:

```
server {
  server_name <адрес сервера>;
  listen 80;
  access_log      /var/log/nginx/access_deault_server.log
main;
  client_max_body_size 200m;
```

```
    location / {
      proxy_redirect        off;
      proxy_set_header      Host $host;
      proxy_pass            http://localhost:8030;
    }
  }
```

В параметре server_name необходимо задать адрес файлового сервера ПУСП. Например:

```
server_name ocs-app.local;
```

3.2.2. Проверить правильность конфигурации балансировщика микросервисов Nginx Web Server и перезапустить его с помощью следующих команд:

```
sudo nginx –t
sudo systemctl restart nginx
```

3.2.3. В параметре config.updateServers.address конфигурационного файла /var/ocs/pkgrepo/ocs-pkgrepo-pkg-repo-api/ocs-pkgrepo-pkg-repo-api.yml задать следующее значение адреса сервера обновлений:

```
http://<адрес сервера>/pkgrepo/mobile
```

Например:

```
http://ocs-app.local/pkgrepo/mobile
```

3.2.4. Перезапустить сервис ocs-pkgrepo-pkg-repo-api с помощью команды:

```
sudo systemctl restart ocs-pkgrepo-pkg-repo-api*
```

3.3. Настройки конфигурационных файлов

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

4. ЗАГРУЗКА СИСТЕМНЫХ ПАКЕТОВ В ФАЙЛОВОЕ ХРАНИЛИЩЕ ПУСП

Для загрузки системных пакетов в файловое хранилище ПУСП необходимо выполнить следующие действия:

1) скопировать в произвольный каталог файлового хранилища ПУСП архив с системными пакетами и распаковать его в каталог, заданный в параметре root секции location /pkgrepo/mobile конфигурационного файла /etc/nginx/conf.d/locations-external/pkgrepo.nginx.location (по умолчанию каталог: /ocs/pkgrepo/repos), либо в параметре repos_root конфигурационного файла /install-apps/inventories-pkgrepo/deploy/vars/ocs-pkgrepo-nginx-static.yml скриптов развертывания ППО:

```
tar -xf <имя файла с архивом> -C /ocs/pkgrepo/repos
rm <имя файла с архивом>
```

2) зарегистрировать переданный релиз (версию), добавив в файл /ocs/pkgrepo/meta/main.json описание из переданного вместе с архивом meta-файла. Путь к файлу main.json задается в параметре alias секции location /pkgrepo/mobile/meta конфигурационного файла /etc/nginx/conf.d/locations-external/pkgrepo.nginx.location (по умолчанию каталог: /ocs/pkgrepo/meta), либо в параметре meta_root конфигурационного файла /install-apps/inventories-pkgrepo/deploy/vars/ocs-pkgrepo-nginx-static.yml скриптов развертывания ППО. Пример файла main.json:

```
{
  "brand": "OMPCert",
  "releases": [
    {
      "deviceModel": "p4903",
      "latest": "3.0.2.23",
```

```
    "versions": [
      {
        "version": "3.0.2.22",
    "from": []
      },
      {
        "version": "3.0.2.23",
        "from": [
            "3.0.2.22"
    ]
  }
    ]
},
{
    "deviceModel": "1801em",
    "latest": "3.0.2.23",
    "versions": [
      {
        "version": "3.0.2.22",
    "from": []
      },
      {
        "version": "3.0.2.23",
        "from": [
            "3.0.2.22"
    ]
  }
    ]
}
```

```
    ]
}
```

3) перезапустить сервис ocs-pkgrepo-pkg-repo-api с помощью команды:

```
sudo systemctl restart ocs-pkgrepo-pkg-repo-api*
```

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
МУ	Мобильное устройство
ОС	Операционная система
ПБ	Подсистема безопасности
ППО	Прикладное программное обеспечение «Аврора Центр»
ПУСП	Подсистема установки системных пакетов
СЗИ	Средства защиты информации
СЗИ НСД	Средства защиты информации от несанкционированный доступ
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Содержание изменения	ФИО инициатора	Дата
1.0	Начальная версия	Шевченко Д.	06.07.2020 г.
1.1	Внесение изменений: – подраздел 3.2; – раздел 4	Фомин П.	29.07.2020 г.