ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

УТВЕРЖДЕН

АДМГ.20134-01 31 01-ЛУ

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Описание применения

АДМГ.20134-01 31 01

Листов 63

Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата

2021

АННОТАЦИЯ

Настоящий документ является описанием применения прикладного программного обеспечения «Аврора Центр» АДМГ.20134-01 релиз 2.5.1 (далее – ППО).

В документе приведено назначение ППО, условия применения и описание задачи. Кроме того, в документе определены угрозы безопасности и описаны меры защиты информации, а также приведены входные и выходные данные.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

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

ПРИМЕЧАНИЕ. Под обновлением ОС понимается инициализация в ОС процессов получения пакетов с изменениями ОС (образа ОС) из доверенного хранилища и их установки. Получение пакетов с изменениями ОС и их установка осуществляется штатными средствами ОС. ППО не гарантирует успех получения пакетов с изменениями ОС и их установки.

ППО является прикладным программным обеспечением с встроенными механизмами защиты информации от несанкционированного доступа (НСД). ППО может быть использовано, но не ограничиваться, в следующих системах и объектах:

– в государственных информационных системах (ГИС), 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 (ИС) персональных данных (ИСПДн) 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;

– на значимых объектах критической информационной инфраструктуры до 1 категории включительно в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239.

1.2. Состав

ППО состоит из следующих подсистем:

– подсистема безопасности (ПБ);

– подсистема «Маркет» (ПМ);

– подсистема Платформа управления (ПУ);

– подсистема обновления ОС (ПООС).

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

1.2.1. Подсистема безопасности

В ПБ реализованы функции безопасности ППО.

ПБ состоит из следующих компонентов:

– Консоль администратора ПБ;

– Консоль входа пользователей;

– Сервер приложений ПБ.

С помощью Консоли администратора ПБ осуществляется управление учетными записями пользователей и работа с журналом регистрации событий.

С помощью Консоли входа пользователей осуществляется ввод идентификационной и аутентификационной информации пользователями ППО.

Сервер приложений ПБ представляет собой совокупность веб-приложений, реализующих функции безопасности, а также позволяющих хранить в БД и предоставлять субъектам доступа ППО доступ к данным об учетных записях пользователей и записях пользователей и журналу регистрации событий.

1.2.2. Подсистема «Маркет»

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.

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.

1.2.3. Подсистема Платформа управления

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».

1.2.4. Подсистема обновления ОС

ПООС состоит из следующих компонентов:

– Сервер приложений ПООС.

Сервер приложений ПООС представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять следующие данные о пакетах ОС (загрузочный модуль ОС):

– информацию о версиях;

– адрес хранилища пакетов ОС.

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

1.3. Описание взаимодействия подсистем

Описание взаимодействия подсистем между собой представлено в таблице (Таблица 1).

Таблица 1

Компонент подсистемы	**Компонент подсистемы, с которым происходит взаимодействие**
ПБ	
Консоль администратора ПБ	Сервер приложений ПБ
Управление учетными записями субъектов доступа, работа с журналом регистрации событий (запросы доступные пользователям с ролью Администратор учетных записей ПБ и ролью Оператор аудита). Процесс идентификации/аутентификации/ авторизации	
Консоль входа пользователей	Сервер приложений ПБ
Идентификация и аутентификация пользователей по логину и паролю	
ПМ	
Консоль администратора ПМ	Сервер приложений ПМ
Получение приложений и данных о приложениях, согласование приложений (запросы доступные пользователям с ролью Администратор Аврора Маркет), управление ключевой информацией, используемой для создания ЭП МП	
Консоль администратора ПМ	Сервер приложений ПБ
Процесс идентификации/аутентификации/авторизации	
Консоль разработчика ПМ	Сервер приложений ПМ
Загрузка приложений и данных о приложениях на Сервер приложений ПМ, публикация приложений (запросы доступные пользователям с ролью Разработчик)	
Консоль разработчика ПМ	Сервер приложений ПБ
Процесс идентификации/аутентификации/авторизации	
МП «Аврора Маркет»	Сервер приложений ПМ
Получение приложений и данных о приложениях с Сервера приложений ПМ	
МП «Аврора Маркет»	Сервер приложений ПБ
Процесс идентификации/аутентификации/авторизации	

Компонент подсистемы	Компонент подсистемы, с которым происходит взаимодействие
ПУ	
Консоль администратора ПУ	Сервер приложений ПУ
Управление МУ (запросы доступные пользователям с ролью Администратор Платформы Управления)	
Консоль администратора ПУ	Сервер приложений ПБ
Процесс идентификации/аутентификации/авторизации	
МП «Аврора Центр»	Сервер приложений ПУ
Получение управляющих воздействий с Сервера приложений ПУ, передача событий на Сервер приложений ПУ	
МП «Аврора Центр»	Сервер приложений ПБ
Процесс идентификации/аутентификации/авторизации	
Сервер приложений ПУ	Сервер приложений ПМ
Получение списка приложений, процесс идентификации/аутентификации/авторизации	
Сервер приложений ПУ	Сервер приложений ПБ
Создание в ПБ учетных записей МУ (учетных записей с ролью МП «Аврора Центр»)	
ПООС	
Консоль администратора ПУ	Сервер приложений ПООС
Получение информации о версиях (релизах) пакетов ОС, а также адресов файловых хранилищ ПООС	
МП «Аврора Центр»	Сервер приложений ПООС
Получение данных о пакетах ОС и адресах их хранения	
Сервер приложений ПООС	Сервер приложений ПБ
Проверка токенов, получаемых от файлового сервера Nginx (файлового хранилища)	

1.4. Субъекты доступа (роли)

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, 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 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;

– Редактор приложений - роль позволяет осуществлять обновление любых ранее загруженных приложений в ПМ, а также получать о них информацию;

– Пользователь Аврора Маркет позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях;

– Администратор Платформы Управления - роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО.

ПРИМЕЧАНИЕ. В ППО в обязательном порядке должна присутствовать предустановленная учетная запись пользователя admin с ролью Администратора учетных записей.

1.5. Общее описание интерфейса ППО

Описание интерфейсов подсистем, входящих в состав Изделия, приведено в следующих документах:

– «Руководство пользователя. Часть 1. Подсистема безопасности» АДМГ.20134-01 90 01-1;

– «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2;

– «Руководство пользователя. Часть 3. Подсистема Платформа Управления» АДМГ.20134-01 90 01-3;

Описание работы МП приведено в документах:

– «Руководство пользователя. Часть 4. Мобильное приложение «Аврора Маркет» АДМГ.20134-01 90 01-4;

– «Руководство пользователя. Часть 5. Мобильное приложение «Аврора Центр» АДМГ.20134-01 90 01-5.

Описание назначения разделов интерфейса ППО приведено в далее в таблице (Таблица 2).

Таблица 2

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
Мониторинг	Индикаторы	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Индикаторы» Консоли администратора ПУ представляет собой аналитическую панель и предназначен для мониторинга показателей, контроля отклонений показателей и перехода к управлению пользователями МУ и устройствами, которые вызвали отклонения. Права на доступ: Администратор Платформы Управления
	Аудит	ПБ	АДМГ.20134-01 90 01-1	Назначение: Подраздел «Аудит» Консоли администратора ПБ предназначен для отображения, фильтрации и поиска записей о действиях и событиях в системе для выполнения разбора инцидентов и контроля хода выполнения работы. Права на доступ: Оператор аудита
Управление	Устройства	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Устройства» Консоли администратора ПУ предназначен для работы со списком всех МУ, переданных под управление ПУ. С помощью подраздела «Устройства» возможно выполнять следующие действия: – добавление МУ и группы МУ вручную и с помощью импорта CSV-файла; – создание динамических групп МУ;

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
				– просмотр списка МУ и информации по любому МУ; – поиск МУ и групп МУ; – редактирование информации о МУ и группе МУ; – создание QR-кода для активации МУ на сервере ПУ; – просмотр списка заданных политик, назначенных на МУ или группу МУ; – назначение политик на группу МУ; – назначение офлайн-сценариев на группу МУ; – оперативное управление МУ (обновление состояния, установка одноразового пароля пользователя и администратора МУ, очистка МУ, блокировка экрана, запрос логов с МУ, установка расписания получения событий безопасности); – исключение МУ от группы МУ; – удаление (архивирование) МУ. Права на доступ: Администратор Платформы Управления
	Пользователи	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Пользователи» Консоли администратора ПУ предназначен для управления пользователями МУ. С помощью подраздела «Пользователи» возможно выполнять следующие действия: – добавление пользователя МУ и группы пользователей МУ вручную и с помощью импорта CSV-файла;

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
				– импорт пользователей с привязкой к группам пользователей и МУ; – просмотр списка пользователей МУ и группы пользователей МУ; – привязку МУ к пользователю; – просмотр МУ пользователя; – создание групп пользователей МУ; – редактирование информации о пользователе МУ; – просмотр информации о группах пользователей и пользователях МУ; – обновление списка учетных записей пользователей МУ с помощью CSV-файла; – назначение политик на группу пользователей МУ; – поиск учетной записи пользователя МУ. Права на доступ: Администратор Платформы Управления
	Политики	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Политики» Консоли администратора ПУ предназначен для работы и управления политиками и корпоративным шаблоном политик, которые могут быть назначены на группы устройств и группы пользователей МУ. С помощью подраздела «Политики» возможно выполнить: – просмотр списка созданных политик и информации по ним;

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
				– добавление политики на группы пользователей МУ и группы устройств или корпоративного шаблона политик; – редактирование политик и корпоративного шаблона политик (если шаблон уже создан, то в подразделе «Политики» кнопка «Добавить корпоративный шаблон» сменится на «Редактировать корпоративный шаблон»); – просмотр групп пользователей МУ или групп устройств, на которые назначены политики; – добавление в политику: правила, содержания правила и категории правила; – фильтрацию списка политик по названию и дате добавления; – просмотр подробной информации по каждому правилу. Права на доступ: Администратор Платформы Управления
	Сценарии	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Сценарии» Консоли администратора ПУ предназначен для создания сценариев команд по событию для офлайн применения на МУ. С помощью подраздела «Сценарии» возможно: – просматривать офлайн-сценарии;

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
				– создавать офлайн-сценарии команд с указанием события, по которому она будет применена; – назначать офлайн-сценарии на группы устройств или группы пользователей МУ; – удалять сценарии. Права на доступ: Администратор Платформы Управления
	Приложения	ПМ	АДМГ.20134-01 90 01-2	Назначение: Подраздел «Приложения» Консоли администратора ПМ предназначен для работы с перечнем приложений и их релизов, созданных Разработчиком в Консоли разработчика ПМ. Права на доступ: Администратор Аврора Маркет
	Витрины	ПМ	АДМГ.20134-01 90 01-2	Назначение: Подраздел «Витрины» Консоли администратора ПМ предназначен для управления витринами приложений. Права на доступ: Администратор Аврора Маркет
	Связки ключей	ПМ	АДМГ.20134-01 90 01-2	Назначение: Подраздел «Связки ключей» Консоли администратора ПМ предназначен для управления связками ключей. С помощью связки ключей Администратор Аврора Маркет имеет возможность подписывать приложения. Права на доступ: Администратор Аврора Маркет

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
Администрирование	Учетные записи	ПБ	АДМГ.20134-01 90 01-1	Назначение: Подраздел «Учетные записи» Консоли администратора ПБ предназначен для управления учетными записями, определяющими возможность и уровень доступа к системе операторов, пользователей МУ. Права на доступ: Администратор учетных записей
	Настройки	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Настройки» Консоли администратора ПУ предназначен для просмотра информации о Сервере приложений ПМ, о сервере LDAP, Push-сервере, об обновлении ОС, а также для возможности переключения отображения архивных МУ. Права на доступ: Администратор Платформы Управления
	Орг. структура	ПУ	АДМГ.20134-01 90 01-3	Назначение: Подраздел «Орг. структура» Консоли администратора ПУ предназначен для просмотра, добавления и обновления организационной структуры компании в формате LDIF, а также получения данных с сервера LDAP, с которым установлено соединение. Права на доступ: Администратор Платформы Управления

Раздел	Подраздел	Подсистема	Документ, содержащий описание	Основное назначение
Консоль разработчика ПМ		ПМ	АДМГ.20134-01 90 01-2	Назначение: Консоль разработчика ПМ предназначена для взаимодействия разработчика приложений с функционалом МП «Аврора Маркет» для размещения приложений (и их конкретных версий), а также для осуществления действий на определенных системой этапах жизненного цикла МП. Права на доступ: Разработчик, Редактор приложений
МП «Аврора Маркет»		ПМ	АДМГ.20134-01 90 01-4	Назначение: МП «Аврора Маркет» предназначено для отображения данных о приложениях, а также для загрузки, установки, обновления и удаления МП на МУ. Права на доступ: Пользователь Аврора Маркет
МП «Аврора Центр»		ПУ	АДМГ.20134-01 90 01-5	Назначение: МП «Аврора Центр» предназначено для получения сообщений от ПУ, передачи сообщений компонентам ОС Аврора и компонентам ПУ сведений о настройках и состоянии МУ. Права на доступ: сервис/процесс МП «Аврора Центр»

2. УСЛОВИЯ ПРИМЕНЕНИЯ

В таблице (Таблица 3) приведены аппаратные характеристики серверов приложений ППО.

Таблица 3

Параметр	**Количество МУ**				
	10 000	**50 000**	**100 000**	**275 000**	**550 000**
Процессор	2 ядра	3 ядра	3 ядра	6 ядер	6 ядер
Объем оперативной памяти	4 Гб	4 Гб	6 Гб	8 Гб	8 Гб
Объем жесткого диска	HDD 60 Гб	HDD 80 Гб	HDD 110 Гб	HDD 130 Гб	HDD 160 Гб
Количество серверов	3	3	3	3	6

В таблице (Таблица 4) приведены программные характеристики серверов приложений ППО.

Таблица 4

Параметр	**Значение**
Операционная система	Одна из следующих ОС: – CentOS версии 7 или выше; – CentOS версии 8 или выше; – Альт 8 СП[1]
Балансировщик микросервисов	Nginx Web Server версии 1.18 или выше
Система обнаружения сервисов	Consul версии 1.9 или выше
Средство управления конфигурациями микросервисов	Consul Template версии 0.25 или выше
Сервис гарантированной доставки сообщений	Nats Streaming Server версии 0.20.0 или выше
Прикладное программное обеспечение	ППО «Аврора Центр»

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

В таблице (Таблица 5) приведены аппаратные характеристики серверов БД.

Таблица 5

Параметр	**Количество МУ**						
	10 000 ПБ, ПМ, ПУ	**50 000 ПБ, ПМ, ПУ**	**100 000 ПБ, ПМ, ПУ**	**275 000**		**550 000**	
				ПБ	**ПМ, ПУ**	**ПБ**	**ПМ, ПУ**
Процессор	2 ядра	3 ядра	3 ядра	3 ядра	4 ядра	3 ядра	6 ядер
Объем оперативной памяти	3 Гб	6 Гб	8 Гб	12 Гб	12 Гб	24 Гб	24 Гб
Объем жесткого диска	SSD 275Гб	SSD 1.3ТБ	SSD 3ТБ	SSD 5.5ТБ	SSD 2ТБ	SSD 11ТБ	SSD 3.5ТБ
Количество серверов	1	1	1	1	1	1	1

В таблице (Таблица 6) приведены программные характеристики серверов БД.

Таблица 6

Параметр	**Значение**
Операционная система	Одна из следующих ОС: – CentOS версии 7 или выше; – CentOS версии 8 или выше; – Альт 8 СП
СУБД	Одна из следующих СУБД: – Postgres Pro 11; – Postgres Pro 12; – PostgreSQL 11.11 или выше (для ОС CentOS); – PostgreSQL 12.6 или выше (для ОС CentOS)
СУБД для хранения сессий	Redis 6.0.10 или выше
Расширение СУБД PostgreSQL для партиционирования таблиц БД	pg_partman 4 или выше
Расширение СУБД PostgreSQL поддерживающее быстрый поиск схожих строк	pg_trgm

В таблице (Таблица 7) приведены программные характеристики МУ.

Таблица 7

Параметр	Значение
Операционная система	ОС Аврора, имеющая действительный сертификат соответствия ФСТЭК России
Прикладное программное обеспечение	– МП «Аврора Центр»; – МП «Аврора Маркет»

ПРИМЕЧАНИЯ:

1. Для работы пользователей с веб-интерфейсом ППО должны использоваться веб-браузеры, поддерживающие технологии: TLS, CSS3, HTML5, ECMAScript 5 и Cookie. Рекомендуется использовать веб-браузер Chrome версии 75 или выше;

2. В ИС, обрабатывающих информацию ограниченного доступа, требующую защиты в соответствии с законодательством РФ, необходимо использовать веб-браузер из состава ОС, имеющей сертификат соответствия ФСТЭК России. Рекомендуется использовать веб-браузер Firefox версии 52 или выше.

Варианты конфигурации среды функционирования, в которых проводилось тестирование ППО, приведены в таблице (Таблица 8).

Таблица 8

ОС	СУБД	СЗИ НСД
Сервер приложений		
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64		СЗИ НСД «Dallas Lock Linux»[2]
CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64		Специальное программное обеспечение (СПО) СЗИ НСД «Аккорд-Х К» [3]
CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64		СЗИ «Secret Net LSP» версия 1.10.1[4]
CentOS-8.0, kernel: 4.18.0-80.el8.x86_64		СЗИ «Secret Net LSP» версия 1.10.1
Альт 8 СП		

[2] СЗИ НСД «Dallas Lock Linux» (сертификат соответствия ФСТЭК России № 3594, действителен до 04 июля 2024 г.).

[3] СПО СЗИ НСД «Аккорд-Х К» (сертификат соответствия ФСТЭК России № 3760, действителен до 04 июля 2020 г., техническая поддержка до 31.01.2025 г.).

[4] СЗИ «Secret Net LSP» (сертификат соответствия ФСТЭК России № 2790, действителен до 18 декабря 2023 г.).

ОС	СУБД	СЗИ НСД
Сервер БД/сервер БД и сервер приложений		
CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64	PostgreSQL 11.11	СПО СЗИ НСД «Аккорд-Х К»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 11.11	СЗИ НСД «Dallas Lock Linux»
CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64	PostgreSQL 11.11	СЗИ «Secret Net LSP» версия 1.10.1
CentOS-8.0, kernel: 4.18.0-80.el8.x86_64	PostgreSQL 11.11	СЗИ «Secret Net LSP» версия 1.10.1
CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64	PostgreSQL 12.6	СПО СЗИ НСД «Аккорд-Х К»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 12.6	СЗИ НСД «Dallas Lock Linux»
CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64	PostgreSQL 12.6	СЗИ «Secret Net LSP» версия 1.10.1
CentOS-8.0, kernel: 4.18.0-80.el8.x86_64	PostgreSQL 12.6	СЗИ «Secret Net LSP» версия 1.10.1
Альт 8 СП	Postgres Pro	

3. ОПИСАНИЕ ЗАДАЧИ

ППО обеспечивает выполнение следующих задач:

– управление МУ, функционирующими под управлением ОС Аврора;

– управления жизненным циклом МП и обновлением ОС;

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– регистрация событий безопасности;

– автоматизированная обработка общедоступной информации и информации ограниченного доступа, не содержащая сведений, составляющих государственную тайну, подлежащая защите в соответствии с требованиями действующего законодательства Российской Федерации в области ИБ.

ПРИМЕЧАНИЕ. Под обновлением ОС понимается инициализация в ОС процессов получения пакетов с изменениями ОС (образа ОС) из доверенного хранилища и их установки. Получение пакетов с изменениями ОС и их установка осуществляется штатными средствами ОС. ППО не гарантирует успех получения пакетов с изменениями ОС и их установки.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Взаимодействие пользователей с ППО осуществляется с помощью его графического интерфейса.

Сведения о входных и выходных данных графического интерфейса ППО приведены в документах:

– «Руководство пользователя. Часть 1. Подсистема безопасности» АДМГ.20134-01 90 01-1;

– «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2;

– «Руководство пользователя. Часть 3. Подсистема Платформа Управления» АДМГ.20134-01 90 01-3;

– «Руководство пользователя. Часть 4. Мобильное приложение «Аврора Маркет» АДМГ.20134-01 90 01-4;

– «Руководство пользователя. Часть 5. Мобильное приложение «Аврора Центр» АДМГ.20134-01 90 01-5.

5. ОПРЕДЕЛЕНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ВЫБОР МЕР ЗАЩИТЫ

Описание возможных угроз безопасности, которым подвержено ППО, приведено в документе «Модель угроз безопасности информации прикладного программного обеспечения «Аврора Центр».

В таблице (Таблица 9) приведены меры защиты информации, направленные на нейтрализацию угроз безопасности информации.

Таблица 9

№ п/п	Название угрозы (способ реализации)	Источник угрозы (идентификатор нарушителя)	Объект воздействия	Результат НСД	Мера защиты информации	
					ППО	Среда функционирования
1.	Перехват информации, передаваемой по каналам связи	Н.1	Канал связи за пределами КЗ	Конфиденциальность		Защита канала связи с использованием СКЗИ
2.	Перехват информации, передаваемой по каналам связи	Н.2	Канал связи внутри КЗ	Конфиденциальность		Защита канала связи с использованием СКЗИ
3.	Перехват парольной информации, передаваемой по каналам связи	Н.1	Канал связи за пределами КЗ	Конфиденциальность, целостность, доступность		Защита канала связи с использованием СКЗИ
4.	Перехват парольной информации, передаваемой по каналам связи	Н.2	Канал связи внутри КЗ	Конфиденциальность, целостность, доступность		Защита канала связи с использованием СКЗИ
5.	Модификация и навязывание (ввод ложной информации) при ее передаче по каналам связи	Н.1	Канал связи за пределами КЗ	Целостность, доступность		Защита канала связи с использованием СКЗИ

№ п/п	Название угрозы (способ реализации)	Источник угрозы (идентификатор нарушителя)	Объект воздействия	Результат НСД	Мера защиты информации	
					ППО	Среда функционирования
6.	Модификация и навязывание (ввод ложной информации) при ее передаче по каналам связи	Н.2	Канал связи внутри КЗ	Целостность, доступность		Защита канала связи с использованием СКЗИ
7.	Загрузка ОС с внешнего носителя информации. Получение доступа к файловой системе, включая файлы БД, содержащие информацию	Н.2	Серверы	Конфиденциальность, целостность, доступность		СДЗ
8.	Загрузка ОС с внешнего носителя информации. Получение доступа к файловой системе, включая файлы БД, содержащие информацию	Н.2	АРМ, МУ	Конфиденциальность, целостность		ОС Аврора, СДЗ
9.	Получение доступа к ИС в обход правил разграничения доступа	Н.1	Серверы	Конфиденциальность, целостность, доступность	ИАФ.1, ИАФ.2, ИАФ.3, УПД.1, УПД.2, УПД.11	МЭ, СОВ
10.	Получение доступа к ИС в обход правил разграничения доступа	Н.2	Серверы	Конфиденциальность, целостность, доступность	ИАФ.1, ИАФ.2, ИАФ.3, УПД.1, УПД.2, УПД.11	МЭ, СДЗ, организационно-режимные меры
11.	Подбор паролей к учетной записи ППО	Н.1, Н.2	ППО	Конфиденциальность, целостность, доступность	ИАФ.4, УПД.6	

№ п/п	Название угрозы (способ реализации)	Источник угрозы (идентификатор нарушителя)	Объект воздействия	Результат НСД	Мера защиты информации	
					ППО	Среда функционирования
12.	Подбор паролей к учетной записи ОС при наличии физического доступа к системе	Н.2	Сервер	Конфиденциальность, целостность, доступность		сертифицированная ОС, СДЗ
13.	Подбор паролей к учетной записи ОС при наличии физического доступа к системе	Н.2	ОС на АРМ и ОС Аврора	Конфиденциальность, целостность, доступность		ОС Аврора, СДЗ, сертифицированная (доверенная) ОС
14.	Внедрение вредоносных программ	Н.1	Канал связи	Конфиденциальность, целостность, доступность		защита канала связи
15.	Внедрение вредоносных программ	Н.2	Сервер, АРМ, ОС Аврора	Конфиденциальность, целостность, доступность	ИАФ.1, ИАФ.2, ИАФ.3, УПД.1, УПД.2, УПД.11	СДЗ, ОС Аврора, АВЗ, защита канала связи, организационно-режимные меры
16.	Внесение изменений в логику работы ПО путем подмены библиотек и / или изменения конфигурационных файлов приложения	Н.2	Сервер, ОС Аврора	Конфиденциальность, целостность, доступность		МЭ, СДЗ, ОС Аврора, организационно-режимные меры
17.	Получение доступа к содержимому БД в обход существующих правил разграничения доступа путем эксплуатации	Н.1, Н.2	СУБД	Конфиденциальность, целостность, доступность		МЭ, СДЗ

№ п/п	Название угрозы (способ реализации)	Источник угрозы (идентификатор нарушителя)	Объект воздействия	Результат НСД	Мера защиты информации	
					ППО	Среда функционирования
	уязвимостей СУБД					
18.	Использование уязвимостей системного ПО	Н.2	Сервер	Конфиденциальность, целостность, доступность		Регулярные обновления системного ПО
19.	Перехват парольной информации при ее вводе	Н.1, Н.2	АРМ, ОС Аврора	Конфиденциальность, целостность, доступность	ИАФ.5	
20.	Получение доступа нарушителя к незаблокированному АРМ/ОС Аврора пользователя	Н.2	АРМ, ОС Аврора	Конфиденциальность, целостность, доступность	УПД.10	
21.	Использование нарушителем полученной/перехваченной аутентификационной информации для входа в ИС	Н.1, Н.2		Конфиденциальность, целостность, доступность	УПД.9	
22.	Невозможность восстановления (выяснения) причин нарушения ИБ				РСБ.3, РСБ.7	

6. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

ППО реализует меры защиты информации, приведенные в таблице (Таблица 10).

Таблица 10

Условное обозначение и номер меры в нотации				**Мера защиты информации**
17-ого приказа ФСТЭК России (ГИС)	**21-ого приказа ФСТЭК России (ИСПДн)**	**31-ого приказа ФСТЭК России (АСУ)**	**239-ого приказа ФСТЭК России (КИИ)**	
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	ИАФ.1	ИАФ.1	ИАФ.1	Идентификация и аутентификация пользователей
ИАФ.2	ИАФ.2	ИАФ.2	ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3 (с усилением 1б, 2б)	ИАФ.3	ИАФ.3	ИАФ.3	Управление идентификаторами
ИАФ.4 (с усилением 1г)	ИАФ.4	ИАФ.4	ИАФ.4	Управление средствами аутентификации
ИАФ.5	ИАФ.5			Защита обратной связи при вводе аутентификационной информации
Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.1 (с усилением 3б)	УПД.1	УПД.1	УПД.1	Управление учетными записями пользователей
УПД.2 (с усилением 4)	УПД.2	УПД.2	УПД.2	Разграничения доступа субъектов к объектам системы
УПД.6 (с усилением 1)	УПД.6	УПД.6	УПД.6	Ограничение неуспешных попыток входа
УПД.9 (с усилением 1а, 3)	УПД.9	УПД.9	УПД.9	Ограничение числа параллельных сеансов
УПД.10 (с усилением 1б, 3)	УПД.10	УПД.10	УПД.10	Блокирование сеанса доступа пользователя при неактивности

Условное обозначение и номер меры в нотации				Мера защиты информации
17-ого приказа ФСТЭК России (ГИС)	**21-ого приказа ФСТЭК России (ИСПДн)**	**31-ого приказа ФСТЭК России (АСУ)**	**239-ого приказа ФСТЭК России (КИИ)**	
УПД.11	УПД.11	УПД.11	УПД.11	Запрета действий пользователей, разрешенных до идентификации и аутентификации
Регистрация событий безопасности (РСБ)				
РСБ.3	РСБ.3	АУД.4	АУД.4	Регистрация событий безопасности
РСБ.7	РСБ.7	АУД.6	АУД.6	Защита информации о событиях безопасности

ПРИМЕЧАНИЕ. Все приведенные меры защиты реализуются в рамках ПБ.

6.1. Идентификация и аутентификация субъектов доступа и объектов доступа

ППО является многопользовательской системой. Субъектами доступа являются пользователи и МУ (процесс на МУ). Для каждого субъекта доступа в ППО заводится отдельная учетная запись с уникальным идентификатором, который однозначно идентифицирует пользователя и/или МУ. Учетные записи пользователей заводятся Администратором учетных записей, либо непосредственно самими пользователями с последующей их активацией Администратором учетных записей. Учетные записи МУ заводятся в процессе процедуры активации МУ в ППО.

ППО реализует протокол аутентификации OpenID Connect 1.0. Аутентификация субъектов доступа, при отсутствии активной сессии, осуществляется по паролю, вводимому пользователем или предоставляемым МП.

Пароли хранятся в виде хэш-кода, полученного с помощью алгоритма криптографического преобразования HKDF-SHA-256. Вводимые пользователями символы пароля, в зависимости от веб-браузера, отображаются условными знаками «*» или «•» (ИАФ.5). В случае успешной аутентификации субъекту доступа выдается токен. Дальнейшая идентификация/аутентификация запросов субъектов доступа осуществляется с использованием токенов. В случае успешной аутентификации МУ токены сохраняются на МУ и в дальнейшем передаются в каждом запросе. В случае

успешной аутентификации пользователя токены сохраняются в ПБ и связаны с сессией пользователя (веб-браузера).

В ППО реализованы механизмы управления идентификаторами (ИАФ.3) в части:

– создания идентификатора пользователя и(или) МУ;

– исключения повторного использование идентификатора пользователя в течение – не менее трех лет (усиление ИАФ.3 1б);

– блокирование идентификатора пользователя через заданный в настройках ППО период времени неиспользования.

В ППО реализованы механизмы управления аутентификационной информацией (ИАФ.4) в части:

– изменение аутентификационной информации;

– генерация и выдача начальной аутентификационной информации;

– установление характеристик пароля.

ППО позволяет устанавливать и(или) контролировать следующие характеристики пароля:

– минимальная сложность пароля с определяемыми требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

– минимальное количество измененных символов при создании новых паролей (должна обеспечиваться невозможность повторения текущего пароля и требоваться изменения как минимум 1 символа относительно старого пароля);

– максимальное время действия пароля;

– минимальное время действия пароля;

– число последних использованных паролей, которые запрещено использовать пользователями при создании новых паролей;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки;

– время, на которое осуществляется блокировка учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации.

Параметры механизма идентификации и аутентификации приведены в документе АДМГ.20134-01 90 01-1.

6.2. Управление доступом субъектов доступа к объектам доступа

6.2.1. Описание реализуемых политик управления доступом

ППО реализует ролевой метод управления доступа (УПД.2) в части:

– реализации ролевого управления доступом для субъектов ППО к объектам ППО;

– правила разграничения доступа обеспечивают управление доступом субъектов при входе в ППО (усиление УПД.2 1);

– правила разграничения доступа обеспечивают управление доступом субъектов к объектам, создаваемым ППО (усиление УПД.2 4).

Администратор учетных записей с помощью Консоли администратора ПБ осуществляет назначение или удаление прав (ролей) учетным записям пользователей. Учетные записи МУ по умолчанию создаются с ролью МП и не могут быть наделены другой ролью.

Доступ к объектам доступа ППО осуществляется посредством вызова функций, каждая из которых реализована в виде отдельного прикладного обработчика. Функции имеют свое представление в интерфейсе пользователя. Перечень функций и объектов доступа приведен в таблице (Таблица 11).

Возможные роли субъектов доступа перечислены в разделе 1 настоящего документа. Для каждой пары (субъект-объект) задается явное и недвусмысленное перечисление допустимых типов доступа (читать, писать, удалять и т. д.), т. е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному объекту.

Таблица 11

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
ПБ						
Получение списка записей аудита	GET	/v1/auditEvents	Записи аудита (регистрируемые события)	Получение списка	Оператор аудита	2.1.x
Получение списка учетных записей	GET	/v1/accounts	Информация об учетной записи пользователя ППО	Получение списка	Администратор учетных записей	2.1.x
Создание учетной записи	POST	/v1/accounts	Информация об учетной записи пользователя ППО	Создание	Администратор учетных записей	2.1.x
Создание или модификация учетной записи	PUT	/v1/accounts/{account_id}	Информация об учетной записи пользователя ППО	Обновление	Администратор учетных записей	2.1.x
Удаление учетной записи	DELETE	/v1/accounts/{account_id}	Информация об учетной записи пользователя ППО	Удаление	Администратор учетных записей	2.1.x
Получение данных учетной записи	GET	/v1/accounts/{account_id}	Информация об учетной записи пользователя ППО	Чтение	Администратор учетных записей	2.1.x
Изменение пароля учетной записи	POST	/v1/realms/user/accounts/{account_id}/changePassword	Информация об учетной записи пользователя ППО	Обновление	Администратор учетных записей	2.1.x
Получение списка ролей учетной записи	GET	/v1/accounts/{account_id}/roles	Информация о ролях учетной записи	Получение списка	Администратор учетных записей	2.1.x
Назначение роли для учетной записи	PUT	/v1/accounts/{account_id}/roles/{code}	Информация о ролях учетной	Создание	Администратор учетных записей	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
			записи			
Удаление роли для учетной записи	DELETE	/v1/accounts/{account_id}/roles/{code}	Информация о ролях учетной записи	Удаление	Администратор учетных записей	2.1.x
Получение списка ролей	GET	/v1/roles	Информация о роли(ях)	Получение списка	Администратор учетных записей	2.1.x
Блокирование учетной записи	PUT	/v1/accounts/{account_id}/block	Информация о блокировке учетной записи	Обновление	Администратор учетных записей	2.1.x
Разблокирование (активация) учетной записи	PUT	/v1/accounts/{account_id}/unblock	Информация о блокировке учетной записи	Обновление	Администратор учетных записей	2.1.x
Разблокирование (активация) учетной записи МУ	PUT	/v1/accounts/{account_id}/unblock	Информация о блокировке учетной записи	Разблокирование учетной записи	Администратор учетных записей	2.2.0
ПМ						
Получение списка приложений разработчик	GET	/v1/applications	Информация о приложении(ях)	Получение списка	Разработчик/Редактор приложений	2.1.x
Добавление (создание) приложения	POST	/v1/applications	Информация о приложении(ях)	Создание	Разработчик/Редактор приложений	2.1.x
Обновление информации о приложении	PUT	/v1/applications/{application_id}	Информация о приложении(ях)	Обновление	Разработчик/Редактор приложений	2.1.x
Получение информации о приложении	GET	/v1/applications/{application_id}	Информация о приложении(ях)	Чтение	Разработчик/Редактор приложений	2.1.x
Получение списка релизов (версий) приложения	GET	/v1/applications/{application_id}/releases	Информация о приложении	Получение списка	Разработчик/Редактор приложений	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение информации о релизе приложения	GET	/v1/applications/{application_id}/releases/{release_id}	Информация о приложении	Чтение	Разработчик/Редактор приложений	2.1.x
Добавление (создание) релиза приложения	POST	/v1/applications/{application_id}/releases	Информация о приложении	Создание	Разработчик	2.1.x
Обновление информации о релизе приложении	PUT	/v1/applications/{application_id}/releases/{release_id}	Информация о приложении	Обновление	Разработчик/Редактор приложений	2.1.x
Получение списка категорий приложений	GET	/v1/categories	Информация о категориях приложений	Получение списка	Разработчик/Редактор приложений	2.1.x
Передача релиза МП на согласование	POST	/v1/applications/{application_id}/releases/{release_id}/sendForReview	Информация о приложении	Отправка релиза приложения на согласование	Разработчик/Редактор приложений	2.1.x
Удаление приложения	DELETE	/v1/applications/{application_id}	Информация о приложении(ях)	Удаление	Разработчик/Редактор приложений	2.2.1
Загрузка сборки (загрузочных модулей) приложения	POST	/v1/applications/{application_id}/builds	Загрузочные модули приложения	Создание	Разработчик/Редактор приложений	2.1.x
Загрузка зависимых библиотек МП	POST	/v1/applications/{application_id}/dependencies	Загрузочные модули приложения (библиотека)	Создание	Разработчик/Редактор приложений	2.4.0
Загрузка файла иконки релиза приложения	POST	/v1/applications/{application_id}/icons	Иконка (файл)	Создание	Разработчик/Редактор приложений	2.1.x
Получение иконок релиза приложения	GET	/v1/applications/{application_id}/icons/{icon_id}/content	Иконка (файл)	Чтение	Разработчик/Редактор приложений	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Загрузка файла скриншота релиза приложения	POST	/v1/applications/{application_id}/screenshots	Скриншот (файл)	Создание	Разработчик/Редактор приложений	2.1.x
Получение скриншотов релиза приложения	GET	/v1/applications/{application_id}/screenshots/{screenshot_id}/content	Скриншот (файл)	Чтение	Разработчик/Редактор приложений	2.1.x
Получение списка приложений витрины	GET	/v1/dashboards/default/applications	Информация о приложении(ях)	Получение списка	Пользователь Аврора Маркет	2.1.x
Получение списка релизов приложения	GET	/v1/dashboards/default/applications/{application_id}/releases	Информация о приложении	Получение списка	Пользователь Аврора Маркет	2.1.x
Получение файла сборки релиза приложения	GET	/v1/dashboards/default/applications/{application_id}/releases/{release_id}	Информация о приложении	Чтение	Пользователь Аврора Маркет	2.1.x
Получение списка витрин приложений	GET	/v1/dashboards	Информация о витрине приложений	Получение списка	Пользователь Аврора Маркет	2.1.x
Получение информации о витрине приложений	GET	/v1/dashboards/{dashboard_id}	Информация о витрине приложений	Чтение	Пользователь Аврора Маркет	2.1.x
Получение загрузочного модуля МП	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/releases/{release_id}/builds/{build_id}/content	Загрузочные модули приложения	Чтение	Пользователь Аврора Маркет	2.1.x
Получение зависимых библиотек МП	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/dependencies/{dependency_id}/co	Загрузочные модули приложения (библиотека)	Чтение	Пользователь Аврора Маркет	2.5.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
		ntent				
Проверка доступности загрузочного модуля релиза приложения	GET	/empty.html	Загрузочные модули приложения	Чтение	Пользователь Аврора Маркет	2.4.0
Проверка доступности зависимых библиотек МП	GET	/empty.html	Загрузочные модули приложения (библиотека)	Чтение	Пользователь Аврора Маркет	2.5.0
Получение иконок релиза приложения	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/icons/{icon_id}/content	Иконка (файл)	Чтение	Пользователь Аврора Маркет	2.1.x
Проверка доступности иконок релиза приложения	GET	/empty.html	Иконка (файл)	Чтение	Пользователь Аврора Маркет	2.4.0
Получение скриншотов релиза приложения	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/screenshots/{screenshot_id}/content	Скриншот (файл)	Чтение	Пользователь Аврора Маркет	2.1.x
Проверка доступности скриншотов релиза приложения	GET	/empty.html	Скриншот (файл)	Чтение	Пользователь Аврора Маркет	2.4.0
Получение списка категорий приложений	GET	/v1/categories	Информация о категориях приложений	Получение списка	Пользователь Аврора Маркет	2.1.x
Получение списка приложений витрины	GET	/v1/dashboards/{dashboard_id}/applications	Информация о приложении(ях)	Получение списка	Пользователь Аврора Маркет	2.1.x
Получение списка релизов приложения	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/releases	Информация о приложении	Получение списка	Пользователь Аврора Маркет	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение файла сборки релиза приложения	GET	/v1/dashboards/{dashboard_id}/applications/{application_id}/releases/{release_id}	Информация о приложении	Чтение	Пользователь Аврора Маркет	2.1.x
Получение информации о владельце приложения	GET	/auth/admin/api/realms/user/accounts	Информация об учетной записи пользователя ППО	Получение списка	Администратор Аврора Маркет	2.4.0
Получение списка релизов (версий) приложения	GET	/v1/applications/{application_id}/releases	Информация о приложении	Получение списка	Администратор Аврора Маркет	2.1.x
Получение иконок релиза приложения	GET	/v1/applications/{application_id}/icons/{icon_id}/content	Иконка (файл)	Чтение	Администратор Аврора Маркет	2.1.x
Согласование релиза приложения	POST	/v1/applications/{application_id}/releases/{release_id}/approve	Информация о приложении	Согласование релиза приложения	Администратор Аврора Маркет	2.1.x
Возврат релиза на доработку	POST	/v1/applications/{application_id}/releases/{release_id}/sendForRework	Информация о приложении	Отправка релиза приложения на доработку	Администратор Аврора Маркет	2.1.x
Отклонение релиза приложения	POST	/v1/applications/{application_id}/releases/{release_id}/decline	Информация о приложении	Отклонение релиза приложения	Администратор Аврора Маркет	2.1.x
Получения файла архива с данными по релизу приложения	GET	/v1/applications/{application_id}/releases/{release_id}/archive	Информация о приложении	Чтение	Администратор Аврора Маркет	2.1.x
Получение списка приложений разработчика	GET	/v1/applications	Информация о приложении(ях)	Получение списка	Администратор Аврора Маркет	2.1.x
Получение списка	GET	/v1/categories	Информация о	Получение	Администратор	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
категорий приложений			категориях приложений	списка	Аврора Маркет	
Получение списка ключевых пар заказчика	GET	/v1/customerKeyPairs	Ключевая пара заказчика	Получение списка	Администратор Аврора Маркет	2.4.0
Создание ключевой пары заказчика	POST	/v1/customerKeyPairs	Ключевая пара заказчика	Создание	Администратор Аврора Маркет	2.4.0
Обновление ключевой пары заказчика	PUT	/v1/customerKeyPairs/{customer_key_pair_id}	Ключевая пара заказчика	Обновление	Администратор Аврора Маркет	2.4.0
Получение информации о ключевой паре заказчика	GET	/v1/customerKeyPairs/{customer_key_pair_id}	Ключевая пара заказчика	Чтение	Администратор Аврора Маркет	2.4.0
Удаление ключевой пары заказчика	DELETE	/v1/customerKeyPairs/{customer_key_pair_id}	Ключевая пара заказчика	Удаление	Администратор Аврора Маркет	2.4.0
Создание витрины приложений	POST	/v1/dashboards	Информация о витрине приложений	Создание	Администратор Аврора Маркет	2.4.0
Получение списка витрин приложений	GET	/v1/dashboards	Информация о витрине приложений	Получение списка	Администратор Аврора Маркет	2.4.0
Получение информации о витрине приложений	GET	/v1/dashboards/{dashboard_id}	Информация о витрине приложений	Чтение	Администратор Аврора Маркет	2.4.0
Изменение данных витрины приложений	PUT	/v1/dashboards/{dashboard_id}	Информация о витрине приложений	Обновление	Администратор Аврора Маркет	2.4.0
Удаление витрины	DELETE	/v1/dashboards/{dashboard_id}	Информация о витрине приложений	Удаление	Администратор Аврора Маркет	2.5.0
Получение перечня	GET	/v1/dashboards/{dashbo	Информация о	Получить	Администратор	2.4.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
ключевых пар заказчика		ard_id}/customerKeyPairs	витрине приложений	список ключевых пар	Аврора Маркет	
Изменение ключевой пары заказчика	PUT	/v1/dashboards/{dashboard_id}/customerKeyPairs/{customer_key_pair_id}	Информация о витрине приложений	Задание ключевой пары	Администратор Аврора Маркет	2.4.0
Удаление ключевой пары витрины (при удалении ключевой пары через подраздел «Связки ключей»)	DELETE	/v1/dashboards/{dashboard_id}/customerKeyPairs/{customer_key_pair_id}	Информация о витрине приложений	Удаление ключевой пары	Администратор Аврора Маркет	2.4.0
Удаление ключевой пары витрины	DELETE	/v1/dashboards/{dashboard_id}/customerKeyPairs	Информация о витрине приложений	Удаление ключевых пар	Администратор Аврора Маркет	2.4.0
Получение информации о правилах фильтрации приложений витрины	GET	/v1/dashboards/{dashboard_id}/filterRules	Информация о витрине приложений	Получение правил фильтрации	Администратор Аврора Маркет	2.4.0
Назначение (изменение) правил фильтрации приложений	PUT	/v1/dashboards/{dashboard_id}/filterRules	Информация о витрине приложений	Задание правил фильтрации	Администратор Аврора Маркет	2.4.0
ПУ						
Получение сообщения (команды) МУ	GET	/v1/devices/{id}/operations/next	Информация об операции для МУ	Чтение	МП «Аврора Центр»	2.1.x
Получение от МУ ответа на сообщение (команду)	POST	/v1/devices/{id}/operations/{opId}/acknowledges	Информация об операции для МУ	Обновление	МП «Аврора Центр»	2.1.x
Получение информации об активации МУ	POST	/v1/enrollments/{enrollment_id}/complete	Информация о результате выполнения активации от МУ	Создание	МП «Аврора Центр»	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение лог-файла с МУ	POST	/v1/files	Лог-файл МУ	Создание	МП «Аврора Центр»	2.1.x
Получение файла зависимой библиотеки	GET	/appstore/api/v1/dashboards/{dashboard_id}/applications/{application_id}/dependencies/{dependency_id}/content	Загрузочные модули приложения (библиотека)	Чтение	МП «Аврора Центр»	2.5.0
Проверка доступа к зависимой библиотеке	GET	/empty.html	Загрузочные модули приложения (библиотека)	Чтение	МП «Аврора Центр»	2.5.0
Получение информации о релизе МП	GET	/appstore/api/v1/dashboards/default/applications/{application_id}/releases/{release_id}	Информация о приложении	Чтение	МП «Аврора Центр»	2.1.x
Получение файла сборки релиза приложения	GET	/appstore/api/v1/dashboards/{dashboard_id}/applications/{application_id}/releases/{release_id}	Информация о приложении	Чтение	МП «Аврора Центр»	2.1.x
Получение загрузочного модуля МП	GET	/appstore/api/v1/dashboards/{dashboard_id}/applications/{application_id}/releases/{release_id}/builds/{build_id}/content	Загрузочные модули приложения	Чтение	МП «Аврора Центр»	2.1.x
Проверка доступа к загрузочному модулю МП	GET	/empty.html	Загрузочные модули приложения	Чтение	МП «Аврора Центр»	2.4.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение загрузочных модулей пакетов обновлений	GET	/pkgrepo/api/targetRelease	Информация о пакетах обновления	Чтение	МП «Аврора Центр»	2.2.0
Получение параметров доступа к серверу приложений ПМ	GET	/v1/settings	Информация о настройках	Чтение	Администратор Платформы Управления	2.1.x
Получение перечня политик назначенных на группу МУ, либо перечня групп МУ, на которые назначена политика	GET	/v1/assignments	Информация о группах/политиках МУ	Получение списка	Администратор Платформы Управления	2.1.x
Создание корпоративного шаблона политик	POST	/v1/corporatePolicyTemplate	Информация о корпоративном шаблоне	Создание	Администратор Платформы Управления	2.4.0
Получение корпоративного шаблона политик	GET	/v1/corporatePolicyTemplate	Информация о корпоративном шаблоне	Чтение	Администратор Платформы Управления	2.5.0
Обновление корпоративного шаблона политик	PUT	/v1/corporatePolicyTemplate	Информация о корпоративном шаблоне	Обновление	Администратор Платформы Управления	2.5.0
Получение списка витрин приложений	GET	/v1/dashboards	Информация о витрине приложений	Получение списка	Администратор Платформы Управления	2.5.0
Получение информации о витрине приложений	GET	/v1/dashboards/{dashboard_id}	Информация о витрине приложений	Чтение	Администратор Платформы Управления	2.5.0
Получение списка приложений витрины	GET	/v1/dashboards/{dashboard_id}/applications	Информация о приложении(ях)	Получение списка	Администратор Платформы Управления	2.5.0
Получение списка	GET	/v1/dashboards/{dashbo	Информация о	Получение	Администратор	2.5.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
опубликованных релизов приложения		ard_id}/applications/{id}/releases	релизе(ах) приложения	списка	Платформы Управления	
Получение информации о релизе МП	GET	/v1/dashboards/{dashboard_id}/applications/{id}/releases/{release_id}	Информация о релизе(ах) приложения	Чтение	Администратор Платформы Управления	2.5.0
Получение списка групп МУ	GET	/v1/groups	Информация о группе МУ	Получение списка	Администратор Платформы Управления	2.1.x
Создание группы МУ	POST	/v1/groups	Информация о группе МУ	Создание	Администратор Платформы Управления	2.1.x
Получение информации о группе МУ	GET	/v1/groups/{id}	Информация о группе МУ	Чтение	Администратор Платформы Управления	2.1.x
Удаление группы МУ	DELETE	/v1/groups/{id}	Информация о группе МУ	Удаление	Администратор Платформы Управления	2.1.x
Редактирование (обновление) информации о группе МУ	PATCH	/v1/groups/{id}	Информация о группе МУ	Обновление	Администратор Платформы Управления	2.1.x
Добавление устройства в группу МУ	PUT	/v1/groups/{id}/devices	Информация о МУ и группах МУ	Создание	Администратор Платформы Управления	2.1.x
Удаление устройства из группы МУ	DELETE	/v1/groups/{id}/devices	Информация о МУ и группах МУ	Удаление	Администратор Платформы Управления	2.1.x
Назначение оффлайн-сценария на группу МУ	POST	/v1/deviceGroups/{id}/offlineScenarios	Информация об оффлайн сценарии	Назначение оффлайн сценария на группу МУ	Администратор Платформы Управления	2.4.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Назначение политики на группу МУ	PUT	/v1/deviceGroups/{id}/policies	Информация о группах/политиках МУ	Создание	Администратор Платформы Управления	2.2.0
Удаление политик	DELETE	/v1/deviceGroups/{id}/policies	Информация о группах/политиках МУ	Удаление	Администратор Платформы Управления	2.1.x
Комбинирование политик (получение пересечений множеств МУ для переданной группы МУ)	PUT	/v1/deviceGroups/{id}/policies/preview	Информация о комбинировании политик (информация о МУ, группе пользователей МУ и о политиках)	Чтение	Администратор Платформы Управления	2.1.x
Получить пересечения при удалении политики, назначенной на группу МУ	POST	/v1/deviceGroups/{id}/policies/unassignPreview	Информация о комбинировании политик (информация о МУ, группе пользователей МУ и о политиках)	Чтение	Администратор Платформы Управления	2.2.0
Импорт МУ, групп МУ, связей между группами МУ и МУ из файла в формате CSV	POST	/v1/imports	Информация о МУ	Импорт информации из файла	Администратор Платформы Управления	2.1.x
Получение списка групп МУ, в которые входит МУ	GET	/v1/deviceMemberships	Информация о МУ и группах МУ	Получение списка	Администратор Платформы Управления	2.1.x
Получение списка моделей МУ	GET	/v1/models	Информация о моделях МУ	Получение списка	Администратор Платформы Управления	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение информации о связях МУ и пользователях МУ	GET	/v1/deviceUsers	Информация о МУ и пользователях МУ	Получение списка	Администратор Платформы Управления	2.1.x
Получение списка фильтров по МУ	GET	/v1/persistentFilters	Информация о фильтре для списка МУ	Получение списка	Администратор Платформы Управления	2.4.0
Сохранение списка фильтров по МУ	POST	/v1/persistentFilters	Информация о фильтре для списка МУ	Создание	Администратор Платформы Управления	2.4.0
Изменение фильтра по МУ	PATCH	/v1/persistentFilters/{id}	Информация о фильтре для списка МУ	Обновление	Администратор Платформы Управления	2.4.0
Удаление фильтра по МУ	DELETE	/v1/persistentFilters/{id}	Информация о фильтре для списка МУ	Удаление	Администратор Платформы Управления	2.4.0
Получение списка МУ, в соответствии с параметрами, указанными в запросе	GET	/v1/devices	Информация о МУ	Получение списка	Администратор Платформы Управления	2.1.x
Добавление нового МУ в список МУ (создать запись об МУ)	POST	/v1/devices	Информация о МУ	Создание	Администратор Платформы Управления	2.1.x
Удаление МУ из списка МУ	DELETE	/v1/devices	Информация о МУ	Удаление	Администратор Платформы Управления	2.1.x
Получение информации о МУ	GET	/v1/devices/{id}	Информация о МУ	Чтение	Администратор Платформы Управления	2.1.x
Изменение статуса МУ	PATCH	/v1/devices/{id}	Информация о МУ	Обновление	Администратор Платформы	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
					Управления	
Отправка команды на МУ	POST	/v1/devices/{id}/actions	Информация о команде для МУ	Создание	Администратор Платформы Управления	2.1.x
Получение политик, назначенных на МУ	GET	/v1/devices/{id}/assignments	Информация о группах/политиках МУ	Получение списка	Администратор Платформы Управления	2.1.x
Запрос у МУ его состояние	POST	/v1/devices/{id}/infos	Информация о МУ	Создание	Администратор Платформы Управления	2.1.x
Получение комбинированной политики для МУ	GET	/v1/devices/{id}/policy	Информация о политике	Чтение	Администратор Платформы Управления	2.5.0
Получение состояния МУ	GET	/v1/devices/{id}/state	Информация о МУ	Чтение	Администратор Платформы Управления	2.1.x
Отправка QR-кода на электронную почту	POST	/v1/enrollments/email	QR-код	Создание	Администратор Платформы Управления	2.1.x
Формирование QR-кодов	POST	/v1/enrollments/qrcodes	QR-код	Создание	Администратор Платформы Управления	2.1.x
Формирование QR-кода для группы МУ	POST	/v1/enrollments/groups/qrcodes	QR-код	Создание	Администратор Платформы Управления	2.2.0
Получение статуса процесса создания активаций для групп устройств	GET	/v1/enrollments/requests/{id}	Информация о статусе процесса активации МУ	Чтение	Администратор Платформы Управления	2.2.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Получение списка задач	GET	/v1/jobs	Информация о задаче	Получение списка	Администратор Платформы Управления	2.4.0
Получение задачи по идентификатору	GET	/v1/jobs/{id}	Информация о задаче	Чтение	Администратор Платформы Управления	2.4.0
Получение результата выполнения асинхронной задачи	GET	/v1/jobs/{id}/response	Информация о задаче	Чтение	Администратор Платформы Управления	2.4.0
Получение журнала регистрируемых событий МУ	GET	/v1/journal	Журнал регистрируемых событий МУ	Получение списка	Администратор Платформы Управления	2.2.0
Получение настроек доступа к LDAP серверу	GET	/v1/ldapServerSettings	Информация о настройках	Чтение	Администратор Платформы Управления	2.4.0
Получение информации о настройках взаимодействия с СУА (Push-сервис)	GET	/v1/pushServerSettings	Информация о настройках взаимодействия с СУА	Чтение	Администратор Платформы Управления	2.5.0
Получение списка оффлайн-сценариев	GET	/v1/offlineScenarios	Информация об оффлайн-сценарии	Получение списка	Администратор Платформы Управления	2.4.0
Создание оффлайн-сценария	POST	/v1/offlineScenarios	Информация об оффлайн-сценарии	Создание	Администратор Платформы Управления	2.4.0
Удаление оффлайн-сценария	DELETE	/v1/offlineScenarios/{id}	Информация об оффлайн-сценарии	Удаление	Администратор Платформы Управления	2.5.0
Получении информации об оффлайн-сценарии	GET	/v1/offlineScenarios/{id}	Информация об оффлайн-сценарии	Чтение	Администратор Платформы	2.5.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
					Управления	
Получение информации о связи группы (пользователей, устройств) и оффлайн-сценария	GET	/v1/offlineScenariosAssignments	Информация о связи группы (пользователей, МУ) и оффлайн-сценария	Получение списка	Администратор Платформы Управления	2.4.0
Получение адресов серверов обновлений пакетов	GET	/pkgrepo/api/hosts	Адреса серверов обновлений пакетов	Получение списка	Администратор Платформы Управления	2.2.0
Получение списка политик в соответствии с параметрами, заданными в запросе	GET	/v1/policies	Информация о политике	Получение списка	Администратор Платформы Управления	2.1.x
Создание политики	POST	/v1/policies	Информация о политике	Создание	Администратор Платформы Управления	2.1.x
Получение информации о политике	GET	/v1/policies/{id}	Информация о политике	Чтение	Администратор Платформы Управления	2.2.0
Получение информации о политике	PUT	/v1/policies/{id}/preview	Информация о политике	Чтение	Администратор Платформы Управления	2.1.x
Изменение (редактирование) политики	PUT	/v1/policies/{id}	Информация о политике	Обновление	Администратор Платформы Управления	2.1.x
Сохранение фильтра по политикам	POST	/v1/persistentFilters	Информация о фильтре политик	Создание	Администратор Платформы Управления	2.4.0
Получение списка фильтров по политикам	GET	/v1/persistentFilters	Информация о фильтре политик	Получение списка	Администратор Платформы	2.4.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
					Управления	
Изменение фильтра по политикам	PATCH	/v1/persistentFilters/{id}	Информация о фильтре политик	Обновление	Администратор Платформы Управления	2.4.0
Удаление фильтра по политикам	DELETE	/v1/persistentFilters/{id}	Информация о фильтре политик	Удаление	Администратор Платформы Управления	2.4.0
Получение релизов пакетов обновлений	GET	/pkgrepo/api/releases	Информация о пакетах обновления	Получение списка	Администратор Платформы Управления	2.2.0
Получение информации о количестве МУ, соответствующих/не соответствующих политике за запрошенный период	GET	/v1/compliance	Аналитическая информация	Чтение	Администратор Платформы Управления	2.1.x
Получение информации о количестве подключающихся к серверу МУ за запрошенный период времени	GET	/v1/connectedDevices	Аналитическая информация	Чтение	Администратор Платформы Управления	2.1.x
Получение информации о количестве созданных и выполненных активаций МУ за определенный период	GET	/v1/enrollments	Аналитическая информация	Чтение	Администратор Платформы Управления	2.1.x
Получение информации о последнем подключении МУ	GET	/v1/lastConnections/{deviceId}	Информация о последнем подключении МУ	Чтение	Администратор Платформы Управления	2.4.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
Восстановление записи о МУ из архива	POST	/v1/unarchiveDevices	Информация о МУ	Восстановление из архива	Администратор Платформы Управления	2.4.0
Получение списка групп пользователей МУ в соответствии с параметрами, переданными в запросе	GET	/v1/groups	Информация о группе пользователей МУ	Получение списка	Администратор Платформы Управления	2.1.x
Создание группы пользователей МУ	POST	/v1/groups	Информация о группе пользователей МУ	Создание	Администратор Платформы Управления	2.1.x
Получение информации о группе пользователей МУ	GET	/v1/groups/{id}	Информация о группе пользователей МУ	Чтение	Администратор Платформы Управления	2.1.x
Удаление группы пользователей МУ	DELETE	/v1/groups/{id}	Информация о группе пользователей МУ	Удаление	Администратор Платформы Управления	2.1.x
Обновление информации о группе пользователей МУ	PATCH	/v1/groups/{id}	Информация о группе пользователей МУ	Обновление	Администратор Платформы Управления	2.1.x
Назначение оффлайн-сценария на группу пользователей МУ	POST	/v1/userGroups/{id}/offlineScenarios	Информация об оффлайн-сценарии	Назначение оффлайн-сценария на группу пользователей МУ	Администратор Платформы Управления	2.4.0
Назначение политики на группу пользователей МУ	PUT	/v1/userGroups/{id}/policies	Информация о группах/политиках МУ	Создание	Администратор Платформы Управления	2.2.0
Удаление политик	DELETE	/v1/userGroups/{id}/poli	Информация о	Удаление	Администратор	2.2.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
		cies	группах/политиках МУ		Платформы Управления	
Комбинирование политик (получение пересечений множества устройств для переданной группы пользователей МУ при назначении политик)	PUT	/v1/userGroups/{id}/policies/preview	Информация о комбинировании политик (информация о МУ, группе пользователей МУ и о политиках)	Чтение	Администратор Платформы Управления	2.1.x
Получение пересечения при удалении, назначенной на группу пользователей МУ, политик	POST	/v1/userGroups/{id}/policies/unassignPreview	Информация о комбинировании политик (информация о МУ, группе пользователей МУ и о политиках)	Чтение	Администратор Платформы Управления	2.2.0
Добавление пользователей МУ в группу пользователей МУ	PUT	/v1/groups/{id}/users	Информация о пользователе МУ	Создание	Администратор Платформы Управления	2.1.x
Удаление пользователей МУ из группы пользователей МУ	DELETE	/v1/groups/{id}/users	Информация о пользователе МУ	Удаление	Администратор Платформы Управления	2.1.x
Импорт пользователей МУ, групп пользователей МУ, связей между группами и пользователями МУ из файла в формате CSV	POST	/v1/imports	Информация о пользователе(ях) МУ	Импорт информации из файла	Администратор Платформы Управления	2.1.x
Импорт пользователей,	POST	/v1/ldapimport	Информация о	Импорт	Администратор	2.2.0

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
подразделений, связей между группами и пользователями МУ в формате LDIF			пользователе(ях) МУ	информации из файла	Платформы Управления	
Запуск процесса импорта орг. структуры	POST	/v1/ldapSync	Информация о пользователе(ях) МУ	Импорт информации из файла	Администратор Платформы Управления	2.4.0
Получение списка групп пользователей МУ, в которых состоит пользователь МУ	GET	/v1/userMemberships	Информация о пользователе МУ	Получение списка	Администратор Платформы Управления	2.2.0
Получение списка фильтров для списка пользователей МУ	GET	/v1/persistentFilters	Информация о фильтре для списка пользователей МУ	Получение списка	Администратор Платформы Управления	2.4.0
Создание фильтра для списка пользователей МУ	POST	/v1/persistentFilters	Информация о фильтре для списка пользователей МУ	Создание	Администратор Платформы Управления	2.4.0
Изменение фильтра для списка пользователей МУ	PATCH	/v1/persistentFilters/{id}	Информация о фильтре для списка пользователей МУ	Обновление	Администратор Платформы Управления	2.4.0
Удаление фильтра для списка пользователей МУ	DELETE	/v1/persistentFilters/{id}	Информация о фильтре для списка пользователей МУ	Удаление	Администратор Платформы Управления	2.4.0
Получение списка пользователей МУ	GET	/v1/users	Информация о пользователе(ях) МУ	Получение списка	Администратор Платформы Управления	2.2.0
Создание (добавление) пользователя МУ	POST	/v1/users	Информация о пользователе(ях) МУ	Создание	Администратор Платформы Управления	2.1.x
Получение информации	GET	/v1/users/{id}	Информация о	Чтение	Администратор	2.1.x

Функция	Конечная точка		Объект доступа	Тип доступа	Роль	Версия ППО
о пользователе МУ			пользователе(ях) МУ		Платформы Управления	
Изменение (редактирование) информации о пользователе МУ	PUT	/v1/users/{id}	Информация о пользователе(ях) МУ	Обновление	Администратор Платформы Управления	2.1.x
Удаление связи устройства и пользователя	DELETE	/v1/users/{id}/devices	Информация о МУ и пользователях МУ	Удаление	Администратор Платформы Управления	2.4.0
Связать МУ и пользователя МУ	PUT	/v1/users/{id}/devices	Информация о МУ и пользователях МУ	Создание	Администратор Платформы Управления	2.1.x
Получение перечня политик, назначенных на пользователя МУ	GET	/v1/users/{id}/assignments	Информация о группах/политиках МУ	Получение списка	Администратор Платформы Управления	2.1.x
Получение информации о подключениях устройств	GET	/v1/connectedDevices?since={since}	Аналитическая информация	Чтение	Администратор Платформы Управления	2.4.0

Механизм разграничения доступа реализован на основе управления HTTP запросами (далее – запросы). В частности, все запросы между субъектами доступа и защищаемыми информационными ресурсами (ПБ, ПУ, ПМ) проходят через шлюзы (gateway) ПБ. Каждый из шлюзов предназначен для обработки определенных типов запросов (запросы в ПУ с МУ, запросы в ПУ из Консоли администратора ПУ и т.п.). При получении запроса каждый шлюз (с использованием компонента ПБ «OpenID Connect Provider») осуществляет:

- идентификацию/аутентификацию запроса с использованием токена;
- проверку актуальности токена;
- авторизацию запроса.

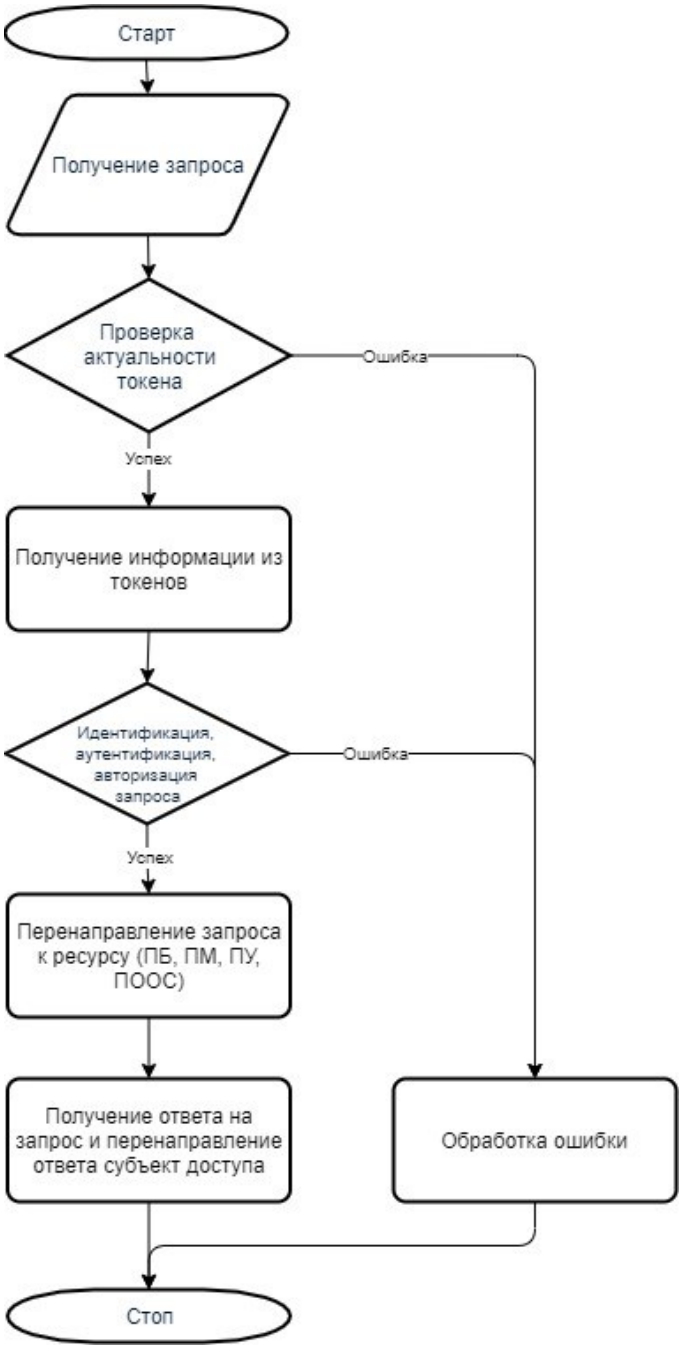

Рисунок 1

Запросы, не прошедшие идентификацию/аутентификацию/авторизацию, содержащие не актуальные токены, а также запросы без токенов шлюз доступа не пропускает (Рисунок 1).

Запросы, прошедшие идентификацию/аутентификацию/авторизацию шлюз доступа направляет по заданному маршруту.

Правила маршрутизации запросов и разграничения доступа задаются в конфигурационных файлах шлюзов доступа:

– /var/ocs/auth/ocs-auth-public-api-gw/ocs-auth-public-api-gw.json;

– /var/ocs/auth/ocs-auth-admin-api-gw/ocs-auth-admin-api-gw.json;

– /var/ocs/appstore/ocs-appstore-admin-api-gw/ocs-appstore-admin-api-gw.json;

– /var/ocs/appstore/ocs-appstore-dev-api-gw/ocs-appstore-dev-api-gw.json;

– /var/ocs/appstore/ocs-appstore-client-api-gw/ocs-appstore-client-api-gw.json;

– /var/ocs/emm/ocs-emm-admin-api-gw/ocs-emm-admin-api-gw.json;

– /var/ocs/emm/ocs-emm-device-api-gw/ocs-emm-device-api-gw.json;

– /var/ocs/pkgrepo/ocs-pkgrepo-admin-api-gw/ocs-pkgrepo-admin-api-gw.json;

– /var/ocs/pkgrepo/ocs-pkgrepo-device-api-gw/ocs-pkgrepo-device-api-gw.json.

Пример правила маршрутизации запроса "/api/applications/{application_id}":

```
"endpoint": "/api/applications/{application_id}",
  "headers_to_pass": [
  "*"
  ],
  "backend": [
  {
   "url_pattern": "/v1/applications/{application_id}",
   "host": [
   "ocs-appstore-application-api.local"
   ],
```

Пример правила разграничения для пользователя с ролью Администратор Аврора Маркет (APS_DEVELOPER):

```
[
 {
 "ruleDescription": "Developer can read category",
 "subject": "APS_DEVELOPER",
 "resourceType": "category",
 "action": "read",
 "conditions": [
 ]
 },
 {
 "ruleDescription": "Developer can create application",
 "subject": "APS_DEVELOPER",
 "resourceType": "application",
 "action": "(create)",
 "conditions": [
 ]
 },
 {
 "ruleDescription": "Developer can read and sendToReview his application",
 "subject": "APS_DEVELOPER",
 "resourceType": "application",
 "action": "(read)|(review)",
 "conditions": [
  {
  "type": "equals",
  "fields": [
   "resource.ownerId",
   "subject.id"
  ]
  }
 ]
 }
]
```

Порядок задания правил разграничения доступа приведен в документе «Руководство администратора» АДМГ.20134-01 91 01.

ППО позволяет управлять учетные записи пользователей в части пользователей:

– управления учетными записями пользователей ППО (УПД.1);

– заведения, активации, блокирования и удаления учетных записей (УПД.1);

– модификация учетных записей пользователей (УПД.1);

– автоматического блокирования неактивных (неиспользуемых) учетных записей пользователей ППО после периода времени неиспользования заданного в настройках ППО;

– автоматического блокирования учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в Изделие за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль) (УПД.6);

– возможности задавать ограничение на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей Изделия (УПД.9);

– отображения администратору числа активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей (усиление УПД.9 3);

– завершения сеанса пользователя после превышения установленного в настройках Изделия времени бездействия (неактивности) пользователя (для реализации усиления 3);

– запрета действий пользователей до прохождения ими процедур идентификации и аутентификации (УПД.11).

Параметры механизма управления доступом приведены в документе АДМГ.20134-01 91 01.

6.2.2. Формальная спецификация ролевой модели разграничения доступа

Основная идея ролевого метода разграничения доступа основана на максимальном приближении логики работы системы к реальному разделению функций персонала в организации.

Ролевой метод разграничения доступа контролирует доступ пользователей к информации на основе типов их активностей в системе. Применение данного метода подразумевает определение ролей в системе. Понятие роль можно определить как совокупность действий и обязанностей, связанных с определенным видом деятельности. Таким образом, вместо того, чтобы указывать все типы доступа для каждого пользователя к каждому объекту, достаточно указать тип доступа к объектам для роли. А пользователям, в свою очередь, указать их роли. Пользователь, «выполняющий» роль, имеет доступ, определенный для роли.

1) ППО представляется совокупностью следующих множеств:

– конечное множество пользователей (субъектов доступа) U (Users);

– конечное множество ролей R (Roles);

– конечное множество полномочий P (Permissions);

– конечное множество сеансов C работы пользователей с ППО;

Множество полномочий P задается в конфигурационных файлах ППО, объединяющих операции доступа и объекты доступа.

2) Ролевые отношения устанавливаются следующими отображениями множеств сущностей системы:

$F_{PR}: P \times R$ – отображение множества полномочий на множество ролей;

$F_{UR}: U \times R$ – отображение множества пользователей на множество ролей.

Отображения F_{PR} и F_{UR} обеспечивают первый и второй этапы процессов организации системы ролевого доступа. При этом отображение F_{UR} реализуется матрицей «Пользователи-Роли».

3) Управление доступом в системе осуществляется на основе введения следующих функций:

$f_{user}: \mathrm{C} \to U$ – значением функции $u = f_{user}(c)$ является пользователь $u \in U$, осуществляющий данный сеанс с работы с ППО;

$f_{roles}: \mathrm{C} \to R$ – значением функции $\Re = f_{roles}(c)$ является набор ролей $\Re \subseteq R$ из доступных пользователю, по которым пользователь работает (осуществляет доступ) в данном сеансе $c \in C$;

$f_{permissions}: \mathrm{C} \to P$ – значение функции $\wp = f_{permissions}(c)$ является набор полномочий $\wp \subseteq P$, доступных всем ролям, задействованным пользователем в данном сеансе $c \in C$.

4) Основное правило (критерий безопасности) ролевого доступа определяется следующим образом: система функционирует безопасно, если и только если любой пользователь $u \in U$, работающий в сеансе $c \in C$, может осуществлять действия (операции, процедуры) в рамках полномочия $p \in P$, при условии:

$\mathrm{p} \in \wp$, где $\wp = f_{permissions}(c)$.

Основной акцент в процессах организации и управления доступом при ролевой политике заключается в особенностях отображения множества пользователей на множество ролей F_{UR} и ограничений, накладываемых на функцию авторизации $f_{roles}(c)$ пользователя в данном сеансе с разрешенными ему отношением F_{UR} ролями.

Любой пользователь (субъект доступа), работающий с ППО, может осуществлять действия в рамках полномочий, доступных всем ролям, назначенным пользователю Администратором учетных записей, следовательно, условие для достижения критерия безопасности может быть выполнено.

Выполнение условия для достижения критерия безопасности может быть представлено в виде алгоритма, представленного на рисунке (Рисунок 2).

Рисунок 2

6.3. Регистрация событий безопасности

ППО осуществляет РСБ. Полученная информация индексируется и хранится в БД. В таблице (Таблица 12) приведен перечень информации, регистрируемой по каждому событию (атрибутов события).

Таблица 12

Атрибут	Описание
`event_id`	Идентификатор события
`time`	Время и дата запроса (события)
`subject_login`	Логин субъекта доступа
`subject_id`	Идентификатор субъекта доступа
`subject_label`	Имя субъекта доступа (ФИО или IMEI)
`subject_type`	Тип субъекта доступа: МУ или пользователь
`object_id`	Идентификатор объекта доступа
`object_label`	Название объекта доступа
`object_type`	Тип объекта доступа: политика
`action`	Действие над объектом: чтение, создание, изменение, удаление
`result`	Результат запроса
`endpoint`	URL-адрес запроса
`method`	HTTP-метод: GET, POST, DELETE
`gateway_id`	Название шлюза

В таблице (Таблица 13) приведен перечень информации, отображаемой в Консоли администратора ПБ.

Таблица 13

Название поля	**Описание**
Идентификатор события	Идентификатор события
Время	Время и дата запроса (события)
Субъект	Информация о субъекте доступа (идентификатор, логин, имя)
Объект	Информация об объекте доступа (идентификатор, тип, имя)
Событие (запрос)	Наименование (описание) события
Результат запроса	В данном поле отображается результат выполнения запроса: успех/неуспех, описание ошибки

В ППО регистрируются следующие типы событий:

- вход (аутентификация) субъекта доступа;
- выход субъекта доступа;
- события (функции), приведенные в таблице (Таблица 11).

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 14).

Таблица 14

Термин/ Сокращение	Расшифровка
АВЗ	Антивирусная защита
АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
АУД	Аудит безопасности
БД	База данных
Витрина	Группа приложений, объединенных по определенному признаку: продавец, разработчик, категория приложения и пр.
ГИС	Государственная информационная система
ИАФ	Идентификация и аутентификация
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
МП	Мобильное приложение
МУ	Мобильное устройство
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПБ	Подсистема безопасности
ПО	Программное обеспечение
ПООС	Подсистема обновления ОС
ПМ	Подсистема «Маркет»
ППО	Прикладное программное обеспечение «Аврора Центр»
ПУ	Подсистема Платформа управления
РСБ	Регистрация событий безопасности
СЗИ	Средств защиты информации

Термин/ Сокращение	Расшифровка
СЗИ НСД	Средств защиты информации от несанкционированного доступа
СПО	Специальное программное обеспечение
СКЗИ	Средства криптографической защиты информации
СУБД	Система управления базами данных
Субъекты 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, 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 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; – Редактор приложений - роль позволяет осуществлять обновление любых ранее загруженных приложений в ПМ, а также получать о них информацию; – Пользователь Аврора Маркет - роль позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях; – Администратор Платформы Управления - роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО
УПД	Управление доступом
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
IMEI	Уникальный номер мобильного устройства, состоящий из 15 цифр
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
WLAN	Wireless Local Area Network – локальная сеть, построенная на основе беспроводных технологий

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рован-ных					