УТВЕРЖДЕН

АДМГ.20134-01 30 01-ЛУ

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Формуляр

АДМГ.20134-01 30 01

Листов 68

2024

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Ввод в эксплуатацию Прикладного программного обеспечения (ППО) «Аврора Центр» АДМГ.20134-01 (далее – Изделие) релиз 5.1.0 проводится в соответствии с настоящим документом и другими эксплуатационными документами (ЭД) на Изделие.

1.2. К эксплуатации Изделия допускается персонал, обладающий знаниями и навыками работы с электронно-вычислительной машиной и техническими средствами вычислительных сетей.

1.3. Перед началом эксплуатации Изделия необходимо внимательно ознакомиться с ЭД, перечень которой приведен в документе «Ведомость эксплуатационных документов» АДМГ.20134-01 20 01.

1.4. Установка и ввод в эксплуатацию Изделия проводится в соответствии с требованиями и указаниями, приведенными 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;

– «Руководство пользователя. Часть 4. Подсистема управления тенантами» АДМГ.20134-01 90 01-4;

– «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений» АДМГ.20134-01 90 01-5;

– «Руководство пользователя. Часть 6. Приложение «Аврора Маркет» для операционной системы Аврора» АДМГ.20134-01 90 01-6;

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7;

– «Руководство администратора» АДМГ.20134-01 91 01;

– «Рекомендации по резервному копированию» АДМГ.20134-01 91 02;

– «Руководство разработчика. Подсистема Сервис уведомлений» АДМГ.20134-01 95 01.

1.5. Изделие может поставляться в виде физической поставки или в виде электронной поставки. Способ поставки[1] Изделия определяется условиями Лицензионного договора.

1.6. Комплектность поставки Изделия приведена в разделе 7 настоящего документа. Комплектность Изделия при поставке определяется условиями Лицензионного договора.

1.7. Настоящий документ входит в комплект поставки[2] Изделия и должен постоянно храниться в подразделении, ответственном за его эксплуатацию.

1.8. Все записи в настоящем документе должны производиться только черными чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления НЕ ДОПУСКАЮТСЯ. Неправильная запись аккуратно зачеркивается, и рядом делается новая, которая заверяется ответственным лицом. После подписи проставляются фамилия и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

[1] Общая информация о возможных способах передачи и носителях информации Изделия приведена в соответствующих приложениях настоящего документа.

[2] При электронной поставке Изделия лицо, ответственное за эксплуатацию, распечатывает копию настоящего документа.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Полное наименование: Прикладное программное обеспечение «Аврора Центр».

2.2. Сокращенное наименование: ППО «Аврора Центр».

2.3. Обозначение: АДМГ.20134-01.

2.4. Предприятие-разработчик, предприятие-изготовитель: Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»):

– юридический адрес: 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Университетская, д. 7, офис 59, ОГРН 1161690087020;

– фактический адрес: 119415, г. Москва, вн.тер.г. муниципальный округ Проспект Вернадского, пр-кт Вернадского, д. 41, 8 этаж.

2.5. Техническая поддержка предприятия-изготовителя: электронная почта support@omp.ru., тел. +7 (495) 269-09-80.

2.6. Изделие 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 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 (АСУ) 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 (КИИ) 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;

– в информационных системах (ИС) общего пользования до 2 класса включительно в соответствии с документом «Требования о защите информации, содержащейся в информационных системах общего пользования», утвержденным приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

2.7. Состав файлов загрузочного модуля Изделия с указанием контрольных сумм (КС) файлов приведен в разделе 7 настоящего документа.

2.8. Настоящий документ содержит следующие приложения:

– Приложение 1. Требования к мерам защиты информации, реализуемые в Изделии;

– Приложение 2. Меры по защите информации в ИС, которые позволят обеспечивать Изделие, путем его применения в ИС для управления устройствами;

– Приложение 3. Общие положения предприятия-изготовителя по возможным вариантам поставки Изделия;

– Приложение 4. Пример маркировки DVD с Изделием.

2.9. Изделие сертифицировано по 4 уровню доверия в Системе сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России № РОСС RU.0001.01БИ00 на соответствие требованиям следующих документов:

– «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;

– «Технические условия» АДМГ.20134-01 99 01.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. Изделие является прикладным программным обеспечением со встроенными механизмами защиты информации от несанкционированного доступа (НСД), предназначенным для:

– управления устройствами[3], функционирующими под управлением операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России;

– управления жизненным циклом приложений[4];

– отправки push-уведомлений на устройства;

– обновления ОС путем получения из доверенного хранилища пакетов с изменениями ОС (образа ОС) и их установки. При этом указанные процессы выполняются штатными средствами самой ОС, а Изделие участвует лишь в их инициализации в ОС и не гарантирует их успешного завершения;

– автоматизированной обработки следующих видов информации:

- общедоступной информации;
- информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, подлежащей защите в соответствии с требованиями действующего законодательства Российской Федерации в области информационной безопасности (ИБ).

3.2. Программно-технические средства необходимые для функционирования Изделия, а также варианты конфигураций, для которых проводилось тестирование приведены в документе «Руководство администратора» АДМГ.20134-01 91 01.

[3] Определение термина «Устройство» приведено в таблице (Таблица 14).
[4] Определение термина «Приложение» приведено в таблице (Таблица 14).

3.3. Изделие состоит из следующих подсистем[5]:

– подсистема безопасности (ПБ);

– подсистема «Маркет» (ПМ);

– подсистема Платформа управления (ПУ);

– подсистема управления тенантами (ПУТ);

– подсистема Сервис уведомлений (ПСУ);

– подсистема обновления ОС (ПООС);

– подсистема доставки контента (CDN).

Взаимодействие между подсистемами и компонентами подсистем осуществляется с использованием протокола HTTP стандарт RFC 2616, при этом обмен данными осуществляется в формате RFC 8259 (JSON).

Для получения push-уведомлений на устройства используется push-демон, входящий в состав ОС Аврора. Push-демон, в свою очередь, взаимодействует с ПСУ по защищенному протоколу TLS (RFC 5246, RFC 8446) с протоколом TCP (RFC 793) на транспортном уровне.

В качестве сервера базы данных (БД) используется сервер с установленной системой управления базами данных (СУБД) Postgres Pro или PostgreSQL, в которой хранятся данные Изделия, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

Подсистемы, входящие в состав Изделия, позволяют выполнять логирование информационных сообщений, сообщений об ошибках, предупреждений и отладочной информации в системный журнал ОС (`systemd-journald`).

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

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

[5] Состав подсистем Изделия зависит от вариантов поставки, описание которых приведено в разделе 7 настоящего документа.

– «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. Подсистема управления тенантами» АДМГ.20134-01 90 01-4;

– «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений» АДМГ.20134-01 90 01-5.

ПРИМЕЧАНИЕ. Описание разделов интерфейса Изделия приведено в документе «Описание применения» АДМГ.20134-01 31 01. Состав разделов интерфейса Изделия зависит от вариантов поставки, подробное описание которых приведено в разделе 7.

Описание работы приложений приведено в документах:

– «Руководство пользователя. Часть 6. Приложение «Аврора Маркет» для операционной системы Аврора» АДМГ.20134-01 90 01-6;

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

Архитектура Изделия приведена на рисунке (Рисунок 1).

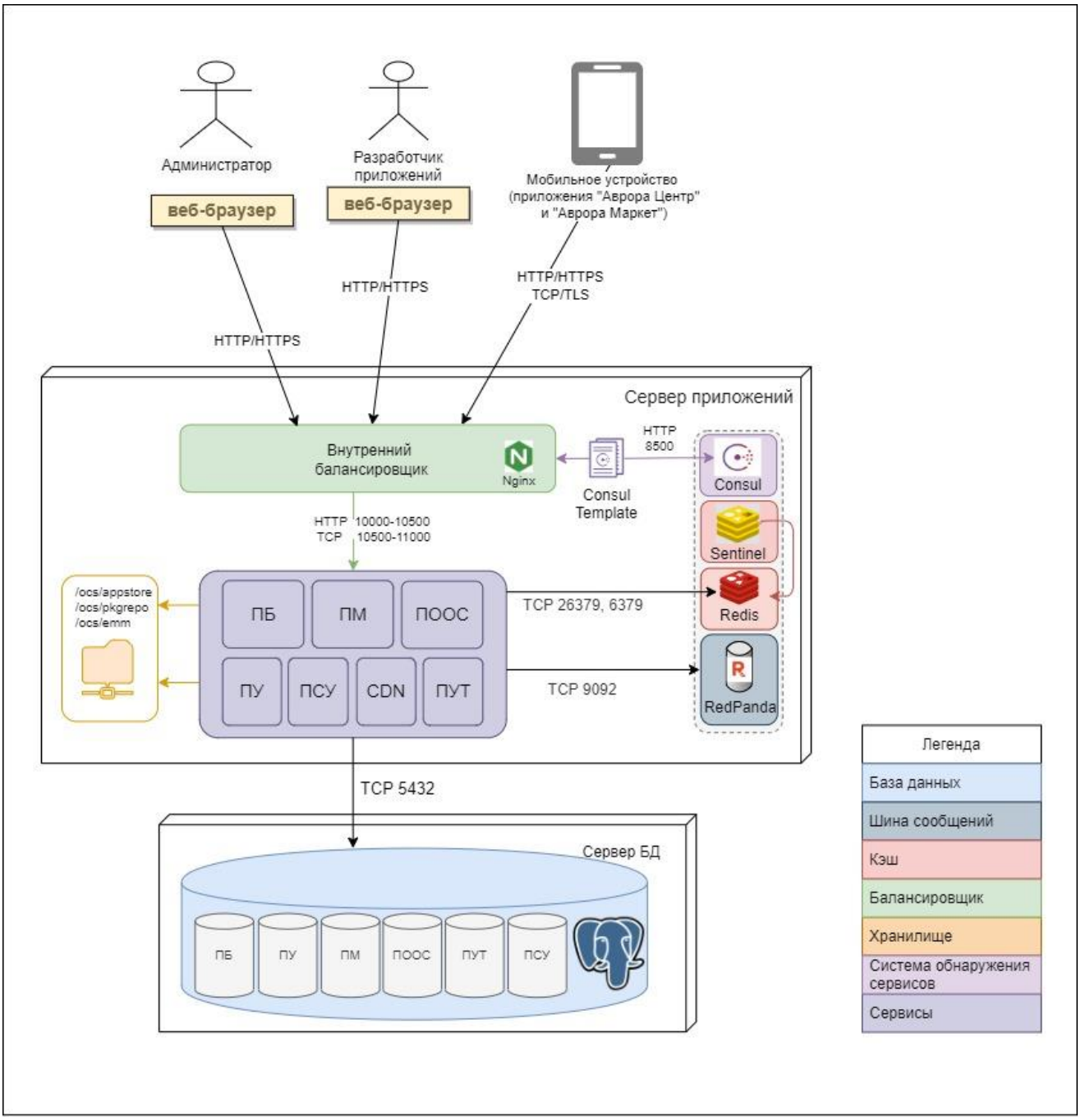

Рисунок 1

3.3.1. Подсистема безопасности

ПБ предназначена для реализации следующих функций безопасности Изделия:

- идентификации и аутентификации пользователей и устройств;
- управления идентификаторами пользователей и устройств;
- управления средствами аутентификации;
- управления учетными записями пользователей и устройств;
- управления доступом субъектов доступа к объектам доступа;

– регистрации событий безопасности;

– предоставления пользователям доступа к интерфейсу ПБ.

ПБ состоит из следующих компонентов:

– Консоль входа пользователей;

– Консоль администратора ПБ;

– Сервер приложений ПБ.

Консоль входа пользователей позволяет пользователям Изделия осуществлять ввод идентификационной и аутентификационной информации.

Консоль администратора ПБ позволяет управлять учетными записями пользователей и работать с журналом регистрации событий.

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

3.3.2. Подсистема «Маркет»

ПМ предназначена для обеспечения:

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

– управления дистрибуцией опубликованных приложений (скачивание, установка, обновление и удаление);

– предоставления пользователям доступа к интерфейсу ПМ.

ПМ состоит из следующих компонентов:

– Консоль администратора ПМ;

– Консоль разработчика ПМ;

– Приложение «Аврора Маркет»;

– Сервер приложений ПМ.

Консоль администратора ПМ позволяет осуществлять взаимодействие Администратора Аврора Маркета с ПМ в части работы с приложениями.

Консоль разработчика ПМ позволяет добавлять новые и обновлять ранее загруженные приложения, а также получать доступ к хранимой в них информации.

Приложение «Аврора Маркет» выполняется на устройстве, функционирующем под управлением ОС, и служит для отображения данных о приложениях, а также для их загрузки, установки, обновления и удаления.

Сервер приложений ПМ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять пользователям Изделия информацию о приложениях. При этом сами приложения, их значки и скриншоты хранятся в файловом хранилище.

3.3.3. Подсистема Платформа управления

ПУ предназначена для обеспечения:

– управления отдельными устройствами (оперативное управление) и группами устройств;

– управления политиками, офлайн-сценариями;

– управления записями об устройстве и пользователях устройства;

– управления приложениями на устройстве;

– контроля состояния устройства;

– контроля применения политик на устройстве;

– мониторинга событий и предоставления отчетности;

– предоставления пользователям доступа к интерфейсу ПУ.

ПУ состоит из следующих компонентов:

– Консоль администратора ПУ;

– Приложение «Аврора Центр»;

– Сервер приложений ПУ.

Консоль администратора ПУ позволяет осуществлять взаимодействие Администратора Платформы управления с ПУ.

Приложение «Аврора Центр» выполняется на устройстве, функционирующем под управлением ОС, служит для получения управляющих сообщений от ПУ и передачи их компонентам ОС, а также для передачи ПУ сведений о настройках и конфигурации ОС Аврора. В зависимости от управляющего сообщения, полученного с ПУ, приложение «Аврора Центр» посредством вызова интерфейсных функций ОС Аврора имеет возможность:

– настраивать доступ к камере, веб-браузеру, микрофону и Bluetooth®;

– управлять возможностью создания снимков экрана устройства;

– управлять настройками WLAN, в том числе точкой доступа WLAN;

– настраивать передачу файлов по протоколу MTP;

– управлять настройками авиарежима, исходящих и входящих вызовов, а также настройками даты и времени;

– сбрасывать устройство до заводских настроек, а также запрещать выполнение сброса;

– обновлять на устройстве версию ОС;

– получать системные сообщения о состоянии устройства;

– получать сообщения о событиях безопасности, произошедших на устройстве, а также настраивать фильтрацию этих сообщений;

– получать системные журналы (логи) с устройства и настраивать способ их хранения на устройстве;

– управлять приложениями (установка, обновление, удаление);

– устанавливать расписание обмена данными устройства с ПУ;

– изменять пароль учетной записи пользователя и администратора устройства, а также задавать требования к паролю;

– управлять блокировкой устройства;

– назначать офлайн-сценарии (блокировки устройства, очистки устройства, смены пароля учетной записи пользователя или администратора устройства, получения событий безопасности с устройства, запрет использования камеры и микрофона), которые сработают на устройстве при следующих условиях:

- при смене SIM-карты;
- при отсутствии у устройства связи с сервером ПУ;
- при входе в зону действия WLAN или при нахождении вне этой зоны;
- при нахождении на территории, определяемой NFC-метками;
- при нахождении на территории/вне территории, определяемых координат.

Сервер приложений ПУ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять пользователям Изделия данные о настройках и конфигурации ОС, а также формировать управляющие сообщения и офлайн-сценарии для приложения «Аврора Центр».

3.3.4. Подсистема управления тенантами

ПУТ предназначена для обеспечения:

– управления жизненным циклом тенантов (создание, редактирование и удаление);

– управления организациями;

– управления контактными лицами организаций.

ПУТ состоит из следующих компонентов:

– Консоль администратора ПУТ;

– Сервер приложений ПУТ.

Консоль администратора ПУТ позволяет осуществлять взаимодействие Администратора тенантов с ПУТ.

Сервер приложений ПУТ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять пользователям Изделия данные о тенантах, а также осуществлять управление тенантами.

3.3.5. Подсистема Сервис уведомлений

ПСУ предназначена для обеспечения:

– доставки push-уведомлений до устройств;

– управления жизненным циклом проектов (добавление, настройка и удаление);

– предоставления пользователям доступа к интерфейсу ПСУ.

ПСУ состоит из следующих компонентов:

– Консоль администратора ПСУ;

– Сервер приложений ПСУ.

Консоль администратора ПСУ позволяет осуществлять взаимодействие Администратора Сервиса уведомлений с ПСУ в части управления жизненным циклом проектов. При этом проекты содержат следующую информацию:

– настройки взаимодействия ПСУ и сервера приложений;

– информацию о приложениях, push-уведомления которых требуется передавать с сервера приложений на устройства;

– информацию о контактных лицах.

Сервер приложений ПСУ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа Изделия информацию о проектах, а также реализует функционал доставки push-уведомлений до устройств посредством tcp-сервера.

3.3.6. Подсистема обновления ОС

ПООС предназначена для обеспечения:

– предоставления информации о пакетах ОС;

– управления дистрибуцией пакетов ОС.

ПООС состоит из следующего компонента:

– Сервер приложений ПООС.

Сервер приложений ПООС представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять информацию и адреса хранения пакетов загрузочного модуля ОС.

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

3.3.7. Подсистема доставки контента

CDN является опциональной подсистемой Изделия и предназначена для оптимизации доставки контента Изделия (установочные файлы приложений, значки, скриншоты, пакеты обновления ОС) путем их размещения (кеширования) на контент-серверах таким образом, чтобы время ожидания для пользователя было минимальным.

CDN состоит из следующего компонента:

– контент-сервера (контент-серверов).

Контент-сервер представляет собой веб-приложение, позволяющее кешировать в файловом хранилище контент Изделия и предоставлять к нему доступ приложениям «Аврора Центр» и «Аврора Макет», а также ОС Аврора.

3.4. Изделие реализует ряд требований к мерам защиты информации, приведенных в документах:

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденном приказом ФСТЭК России от 11 февраля 2013 г. № 17;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденном приказом ФСТЭК России от 18 февраля 2013 г. № 21;

– «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», утвержденном приказом ФСТЭК России от 14 августа 2014 г. № 31;

– «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденном приказом ФСТЭК России от 25 декабря 2017 г. № 239.

ПРИМЕЧАНИЕ. Подробная информация о реализуемых в Изделии требованиях к мерам защиты информации приведена в приложении (Приложение 1).

Изделие позволяет обеспечивать набор мер, определенных 17-ым, 21-ым, 31-ым и 239-ым приказами ФСТЭК России по защите информации в ИС, путем его применения в ИС для управления устройствами.

ПРИМЕЧАНИЕ. Подробная информация о наборе мер, которые позволяет обеспечивать Изделие путем его применения в ИС для управления устройствами, приведена в приложении (Приложение 2).

4. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

4.1. Эксплуатация Изделия должна осуществляться в соответствии с ЭД, перечисленной в документе «Ведомость эксплуатационных документов» АДМГ.20134-01 20 01.

4.2. Изделие и его программные компоненты должны функционировать на специально выделенных серверах в составе локальной вычислительной сети и на устройствах под управлением ОС Аврора.

4.3. При эксплуатации Изделия необходимо соблюдать следующие ОГРАНИЧЕНИЯ ПО ПРИМЕНЕНИЮ:

– правом доступа к серверам с установленным Изделием должны обладать лица, обеспечивающие функционирование ИС, прошедшие соответствующую подготовку, ознакомившиеся с ЭД на Изделие и не рассматривающийся в качестве нарушителей ИБ;

– должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части технических средств, на которых установлено Изделие;

– должна обеспечиваться периодическая (не реже 1 раза в месяц) проверка целостности программных компонентов Изделия посредством сертифицированных средств контроля;

– на устройствах и серверах с установленным Изделием должны быть реализованы меры, исключающие возможность использования средств разработки и отладчиков для редактирования кода и оперативной памяти, используемой Изделием;

– должны быть обеспечены меры, исключающие возможность несанкционированной модификации программных и информационных компонентов Изделия;

– физический доступ к серверам с установленной СУБД должен предоставляться лицам, включенным эксплуатирующей организацией (оператором/потребителем) ИС в перечень лиц, которые не рассматриваются в качестве нарушителя ИБ;

– каналы связи, расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами;

– каналы связи, расположенные за пределами контролируемой зоны, должны быть защищены с использованием средств криптографической защиты информации, сертифицированных по требованиям ФСБ России;

– должны быть предприняты меры по межсетевому экранированию;

– эксплуатация ОС CentOS, ОС Ubuntu или ОС Debian должна осуществляться совместно с установленным средством защиты информации (СЗИ) «Secret Net LSP»[6] или специальным программным обеспечением СЗИ НСД «Аккорд-Х К»[7] или другим СЗИ от НСД сертифицированным по требованиям ФСТЭК России;

– ПСУ не осуществляет аутентификацию подключаемых к нему устройств под управлением ОС Аврора версии 5.0.0 и ниже, поэтому при необходимости обеспечения конфиденциальности, целостности и доступности push-уведомлений необходимо использовать компенсирующие меры защиты информации, например, криптографическую защиту канала связи с двусторонней аутентификацией между Сервером приложений ПСУ и устройствами. Для устройств под управлением ОС Аврора версии 5.1.0 и выше в ПСУ реализована аутентификация, поэтому использование компенсирующих мер не требуется;

– при эксплуатации Изделия в ГИС (ИСПДн, АСУ, КИИ), не содержащих информации составляющей государственной тайны, в зависимости от класса защищенности, должны быть установлены значения параметров, приведенные в таблице (Таблица 1).

[6] Сертификат соответствия ФСТЭК России № 2790, действителен до 18 декабря 2028 г.
[7] Сертификат соответствия ФСТЭК России № 4447, действителен до 10 сентября 2026 г.

Таблица 1

Параметр	Мера ГИС	Значение			
		ГИС 4-го класса	ГИС 3-го класса	ГИС 2-го класса	ГИС 1-го класса
Автоматическое блокирование идентификатора (учетной записи) пользователя через период времени неиспользования	ИАФ.3 УПД.1	—	не более 90 дней	не более 90 дней	не более 45 дней
Длина пароля	ИАФ.4	не менее 6 символов	не менее 6 символов	не менее 6 символов	не менее 8 символов
Алфавит пароля	ИАФ.4	не менее 30 символов	не менее 60 символов	не менее 70 символов	не менее 70 символов
Максимальное время действия пароля	ИАФ.4	180 дней	120 дней	90 дней	60 дней
Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки	ИАФ.4	от 3 до 10	от 3 до 10	от 3 до 8	от 3 до 4
Блокировка учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	ИАФ.4	От 3 до 15 минут	От 5 до 30 минут	от 10 до 30 минут	от 15 до 60 минут
Количество одновременных сессий для привилегированных учетных записей	УПД.9	—	—	—	не более 2-х
Время бездействия (неактивности) пользователя, через которое осуществляется завершение сеанса пользователя	УПД.10	—	—	до 15 минут	до 5 минут

4.4. При эксплуатации Изделия должны применяться следующие дополнительные организационные и технические меры:

– в процессе эксплуатации Изделия должно быть обеспечено регулярное отслеживание наличия и осуществление установки обновлений безопасности программного обеспечения (ПО), входящего в среду функционирования Изделия в соответствии с 3.2 настоящего документа;

– ежемесячно должен производиться поиск актуальных уязвимостей и сведений об уязвимостях Изделия и среды функционирования, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности;

– в среде функционирования Изделия (общесистемное ПО, указанное в 3.2 настоящего документа) должны быть установлены все имеющиеся обновления безопасности и «патчи» для ликвидации известных уязвимостей;

– в случае обнаружения уязвимостей в ПО Изделия должно производиться их устранение в соответствии с методами и процедурами, установленными предприятием-разработчиком;

– оператор с периодичностью 1 раз в неделю должен получать информацию о выходе обновлений Изделия через службу технической поддержки предприятия-изготовителя.

4.5. В эксплуатирующей Изделие ИС должны быть реализованы требования к мерам по обеспечению безопасности:

– информации в ГИС для 1-го класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утвержден приказом ФСТЭК России от 11 февраля 2013 г. № 17);

– информации в ИСПДн для 1-го уровня защищенности в соответствии с требованиями документа «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21);

– информации в АСУ 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» (утвержден приказом ФСТЭК России от 14 августа 2014 г. № 31);

– информации 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» (утвержден приказом ФСТЭК России от 25 декабря 2017 г. № 239).

В состав мер должны входить:

– двухфакторная аутентификация пользователей (ИАФ.1, усиление);

– антивирусная защита.

5. ПОДДЕРЖКА БЕЗОПАСНОСТИ

5.1. Предприятие-изготовитель обеспечивает поддержку безопасности Изделия, предусматривающую:

– устранение недостатков и дефектов Изделия, в том числе устранение уязвимостей и недекларированных возможностей Изделия (далее – устранение недостатков);

– информирование потребителей об обновлении Изделия и доведение до потребителей обновлений Изделия, а также изменений в ЭД (далее – обновление Изделия);

– информирование об окончании производства и (или) поддержки безопасности Изделия.

5.2. Устранение недостатков Изделия предусматривает:

5.2.1. Поиск в общедоступных источниках информации о недостатках Изделия. В качестве общедоступных источников в первую очередь используется БД уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/, Банк данных угроз безопасности информации), а также следующие дополнительные источники: http://cve.omp.ru/, https://cve.mitre.org/, https://nvd.nist.gov/, https://www.exploit-db.com/, http://www.rapid7.com/db/, http://www.cvedetails.com/, http://www.securitylab.ru/ и другие. Поиск осуществляется периодически и не реже 1 раза в месяц.

5.2.2. Получение сведений о недостатках Изделия от потребителей Изделия.

5.2.3. Проведение испытаний Изделия по выявлению недостатков в Изделии, в том числе по выявлению уязвимостей и недекларированных возможностей Изделия.

5.2.4. Разработку компенсирующих мер по защите информации или ограничений по применению Изделия, снижающих возможность эксплуатации недостатков (уязвимостей).

5.2.5. Доведение информации о недостатках Изделия, а также о компенсирующих мерах по защите информации или ограничениях по применению Изделия до потребителей Изделия, ФСТЭК России и банка данных угроз безопасности информации, ведение которого осуществляет ФСТЭК России в соответствии с пунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспертному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

5.2.6. Устранение недостатков Изделия путем доработки Изделия, принятие иных мер, снижающих возможность эксплуатации уязвимостей.

5.2.7. Тестирование (испытание) доработанного Изделия или его отдельных компонентов на предмет устранения влияния обновлений Изделия на его функции безопасности, подтверждения устранения уязвимостей, невнесения новых уязвимостей в Изделие.

5.3. Разработка компенсирующих мер по защите информации или ограничений по применению Изделия, а также доведение информации о недостатках и указанных мерах и ограничениях до потребителей осуществляются в срок не более 48 часов с момента выявления недостатка путем отправки сообщений на электронные адреса потребителей.

5.4. Доработка Изделия, в том числе разработка обновлений ПО Изделия, или разработка мер по защите информации, нейтрализующих недостаток, осуществляется в срок не более 60 дней с момента выявления недостатка.

5.5. Об окончании производства и (или) поддержки безопасности Изделия предприятие-изготовитель информирует потребителей и ФСТЭК России не позднее, чем за 1 год до окончания производства и (или) поддержки безопасности Изделия.

6. ПОРЯДОК ОБНОВЛЕНИЯ

6.1. В рамках поддержки жизненного цикла Изделия предприятие-изготовитель вносит в него изменения, направленные на улучшение эксплуатационных характеристик и устранение недостатков.

6.2. Доведение информации о выпуске обновлений Изделия до каждого потребителя Изделия осуществляется посредством:

– отправки сообщений на электронные адреса потребителей;

– публикации на официальном веб-сайте предприятия-разработчика (https://www.omp.ru, https://auroraos.ru).

6.3. Предусмотрены следующие способы предоставления обновлений потребителям:

– отправка новой версии Изделия с сопроводительным письмом;

– публикация ISO-образа загрузочного модуля новой версии Изделия на официальном веб-сайте предприятия-разработчика (https://www.omp.ru, https://auroraos.ru);

6.4. Потребитель также имеет возможность получить информацию о выходе обновлений через службу технической поддержки предприятия-разработчика по тел.: +7 (495) 269-09-80 либо по электронной почте: support@omp.ru.

6.5. Обновления Изделия, при их наличии, вводятся в эксплуатацию после проведения дополнительных испытаний для поддержания Изделия в сертифицированном статусе. В случае внесения в Изделие изменений, связанных с устранением уязвимостей, предприятие-изготовитель информирует потребителей и ФСТЭК России о необходимости обновления Изделия и доводит до потребителей обновления Изделия до проведения дополнительных испытаний. Автоматическое обновление сертифицированной версии Изделия не допускается.

6.6. Для установки сертифицированных обновлений оператор должен выполнить следующие действия:

– получить от предприятия-изготовителя Изделия сертифицированные обновления Изделия, а также обновленный в соответствии с извещением об изменениях комплект ЭД на Изделие;

– произвести проверку подлинности и целостности посредством проверки электронной подписи (ЭП) Изделия. Инструкция с описанием порядка проверки ЭП, сертификат проверки ЭП, скрипт проверки ЭП и ЭП размещены на веб-сайте предприятия-изготовителя Изделия (https://auroraos.ru/documentation);

– провести расчет КС файлов сертифицированных обновлений Изделия с использованием программы «Программа фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г., окончание срока технической поддержки 26 февраля 2026 г.);

– сравнить КС файлов обновлений с указанными в соответствующем обновленном разделе настоящего документа. При расхождении КС с эталонными значениями, указанными в настоящем документе, необходимо обратиться в службу технической поддержки предприятия-изготовителя Изделия;

– в случае соответствия КС файлов сертифицированных обновлений Изделия эталонным значениям произвести установку сертифицированных обновлений Изделия в соответствии с требованиями, приведенными в документах: «Руководство администратора» АДМГ.20134-01 91 01 и «Рекомендации по резервному копированию» АДМГ.20134-01 91 02.

6.7. Если потребитель Изделия не может реализовать компенсирующие меры по защите информации или ограничения по применению Изделия рекомендуется прекратить его применение.

6.8. Если уязвимости (недекларированные возможности) Изделия не могут быть устранены с помощью компенсирующих мер по защите информации или ограничений по применению, предприятие-изготовитель Изделия незамедлительно и гарантированно, с подтверждением, сообщает об этом всем потребителям и ФСТЭК России. Потребители прекращают применение Изделия.

6.9. Обновление Изделия до требуемой версии возможно только с версий, указанных в таблице (Таблица 2).

Таблица 2

Требуемая версия	Ранее установленная версия
2.2.0	2.1.3*
2.2.1*	2.1.3*, 2.2.0
2.2.2*	2.1.3*, 2.2.0, 2.2.1*
2.3.0	2.2.2*
2.4.0	2.2.2*, 2.3.0
2.5.0	2.2.2*, 2.3.0, 2.4.0
2.5.1*	2.2.2*, 2.3.0, 2.4.0, 2.5.0
3.0.0	2.5.1*
3.0.1	2.5.1*, 3.0.0
3.1.0	2.5.1*, 3.0.1
3.1.1*	2.5.1*, 3.0.1, 3.1.0
3.1.2*	2.5.1*, 3.1.0, 3.1.1*
3.2.0	3.1.0, 3.1.2*
4.0.0*	3.1.2*, 3.2.0
4.1.0*	3.1.2*, 4.0.0*
5.0.0*	3.2.0, 4.0.0*, 4.1.0*
5.1.0*	4.1.0*, 5.0.0*

* - версии Изделия, прошедшие сертификацию в ФСТЭК России.

7. КОМПЛЕКТНОСТЬ

7.1. Комплектность поставки[8] Изделия должна соответствовать комплектности, указанной в таблице (Таблица 3), в строгой зависимости от способа передачи[9] Изделия и спецификации Изделия, предусмотренной в соответствующем Лицензионном договоре.

Таблица 3

Обозначение	Наименование	Кол. шт.	Физическая поставка	Электронная поставка
АДМГ.20134-01	Прикладное программное обеспечение «Аврора Центр»	1	DVD с загрузочным модулем Изделия[10]	В электронном виде
АДМГ.20134-01 30 01	Прикладное программное обеспечение «Аврора Центр». Формуляр	1	В печатном виде (формат А5)[11]	В электронном виде
	Прикладное программное обеспечение «Аврора Центр». Комплект эксплуатационных документов	1	В электронном виде на DVD	В электронном виде
АДМГ.20134-01 99 01[12]	Прикладное программное обеспечение «Аврора Центр». Технические условия	1	В электронном виде на DVD	В электронном виде
Заверенная копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)		1	В печатном виде (формат А5)	В электронном виде

[8] Комплектность поставки Изделия определяется условиями Лицензионного договора.

[9] Общая информация о возможных способах передачи и носителях информации Изделия приведена в соответствующих приложениях настоящего документа.

[10] DVD с загрузочным модулем Изделия, также содержит компоненты среды функционирования и комплект ЭД на Изделие.

[11] При физической поставке независимо от количества поставляемых комплектов ЭД документ «Формуляр» АДМГ.20134-01 30 01 поставляется в 1 экземпляре на бумажном носителе на каждую партию устройств.

[12] Документ может быть включен в поставку по отдельному запросу.

Комплект ЭД, входящих в поставку[13] Изделия, определен в документе «Ведомость эксплуатационных документов» АДМГ.20134-01 20 01.

7.2. Изделие может иметь несколько различных конфигураций, при этом вариант поставки определяется в соответствующем Лицензионном договоре:

– **Вариант поставки 1** (АДМГ.20134-01 12 01), состоящий из комплекта документов и следующих подсистем: ПБ, ПМ, ПУ, ПСУ, ПООС;

– **Вариант поставки 2** (АДМГ.20134-01 12 02), состоящий из комплекта документов и следующих подсистем: ПБ, ПМ, ПУ, ПСУ, ПООС, включая ПУТ и CDN;

– **Вариант поставки 3** (АДМГ.20134-01 12 03), состоящий из комплекта документов и следующих подсистем: ПБ, ПМ, ПУ, ПСУ, ПООС, включая ПУТ и CDN с «Лицензионным соглашением» для Сервис-провайдеров[14].

7.3. КС файлов Изделия рассчитаны с использованием программы «Программа фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г., окончание срока технической поддержки 26 февраля 2026 г.).

7.3.1. КС DVD с Изделием, содержащим загрузочный модуль Изделия и компоненты среды функционирования приведены в таблице (Таблица 4).

Таблица 4

Изделие	КС DVD с Изделием
Прикладное программное обеспечение «Аврора Центр». «Синглтенант» АДМГ.20134-01 12 01	592AE215
Прикладное программное обеспечение «Аврора Центр». «Мультитенант» АДМГ.20134-01 12 02	7B0C7320
Прикладное программное обеспечение «Аврора Центр». «Мультитенант» для Сервис-провайдеров АДМГ.20134-01 12 03	1B9AAD38

[13] Дополнительно в состав комплекта документов входит файл «Лицензионное соглашение.pdf», с которым необходимо ознакомиться перед началом использования Изделия.

[14] Сервис-провайдер – организация, которая использует Изделие в качестве одного из составляющих для создания своей услуги или продукта. Данная услуга или продукт предоставляется клиентам Сервис-провайдера.

ПРИМЕЧАНИЕ. Перечень файлов загрузочного модуля Изделия и их КС приведены в таблицах (Таблица 5 и Таблица 6). Также пофайловые КС DVD с Изделием приведены на DVD в файле `/checksums/distr/distr.fix.html`.

7.3.2. В таблице (Таблица 5) приведены КС размещенного на DVD с Изделием архива, содержащего файлы Изделия, устанавливаемые на сервер, а также файлы сценариев установки.

Таблица 5

Имя файла	Размер (байт)	КС (шестн.)
`/server/installer-ac.sh` (входит в АДМГ.20134-01 12 01)	890637556	1519556B
`/server/installer-ac-mt.sh` (входит в АДМГ.20134-01 12 02)	989117809	21744E14
`/server/installer-ac-mt-spr.sh` (входит в АДМГ.20134-01 12 03)	988950929	98A07BE4

7.3.3. В таблице (Таблица 6) приведены КС файлов приложения «Аврора Маркет» и приложения «Аврора Центр», входящих в состав соответствующих подсистем Изделия (подробнее в 3.3) и размещенных на DVD с Изделием.

Таблица 6

Номер	Имя файла	Размер (байт)	Контрольная сумма (шестн.)
Каталог: `client-apps-aurora/aurora_center/aurora-4.0.2`			
1	`omp-emm-client-5.1.0.6+2-aurora-4.0.2.armv7hl.rpm`	1120002	CAA9010F
2	`omp-emm-installer-5.1.0.1+2-aurora-4.0.2.armv7hl.rpm`	519238	047EEF48
3	`omp-emm-wizard-quick-activation-5.1.0.1+2-aurora-4.0.2.armv7hl.rpm`	748670	53DA01B3
4	`omp-emm-wizard-quick-activation-configuration-5.1.0.1+2-aurora-4.0.2.armv7hl.rpm`	9630	D0C0D6F0
ИТОГО:	-	2397540	4DCD3904
Каталог: `client-apps-aurora/aurora_center/aurora-5.1.0`			
5	`omp-emm-client-5.1.0.6+2-aurora-5.1.0.aarch64.rpm`	1265435	BDF0EC19
6	`omp-emm-client-5.1.0.6+2-aurora-5.1.0.armv7hl.rpm`	1219552	2BB4BBB5

Номер	Имя файла	Размер (байт)	Контрольная сумма (шестн.)
7	omp-emm-installer-5.1.0.1+2-aurora-5.1.0.aarch64.rpm	34993	2A881186
8	omp-emm-installer-5.1.0.1+2-aurora-5.1.0.armv7hl.rpm	32841	E4AB1130
9	omp-emm-wizard-quick-activation-5.1.0.1+2-aurora-5.1.0.aarch64.rpm	54870	1E87F450
10	omp-emm-wizard-quick-activation-5.1.0.1+2-aurora-5.1.0.armv7hl.rpm	51685	BAF0B2D6
11	omp-emm-wizard-quick-activation-configuration-5.1.0.1+2-aurora-5.1.0.aarch64.rpm	9535	20FC029D
12	omp-emm-wizard-quick-activation-configuration-5.1.0.1+2-aurora-5.1.0.armv7hl.rpm	9626	50E5EBF3
ИТОГО:	-	2678537	8C09F8F2
Каталог: client-apps-aurora/aurora_center/aurora-5.1.1			
13	omp-emm-client-5.1.0.6+2-aurora-5.1.1.aarch64.rpm	1265030	BE5D6103
14	omp-emm-client-5.1.0.6+2-aurora-5.1.1.armv7hl.rpm	1219026	CF1ED0CD
15	omp-emm-installer-5.1.0.1+2-aurora-5.1.1.aarch64.rpm	35008	8D470C56
16	omp-emm-installer-5.1.0.1+2-aurora-5.1.1.armv7hl.rpm	32840	549E27C2
17	omp-emm-wizard-quick-activation-5.1.0.1+2-aurora-5.1.1.aarch64.rpm	54867	1D56DF10
18	omp-emm-wizard-quick-activation-5.1.0.1+2-aurora-5.1.1.armv7hl.rpm	51684	2709C9AB
19	omp-emm-wizard-quick-activation-configuration-5.1.0.1+2-aurora-5.1.1.aarch64.rpm	9534	7084E14C
20	omp-emm-wizard-quick-activation-configuration-5.1.0.1+2-aurora-5.1.1.armv7hl.rpm	9626	8FDD81E1
ИТОГО:	-	2677615	6D9CEC4C
Каталог: client-apps-aurora/aurora_market/aurora-4.0.2			
21	feature-appstore-5.1.0.1+2-aurora-4.0.2.armv7hl.rpm	8923	6A2D004A
22	omp-appmanager-5.1.0.1+1-aurora-4.0.2.armv7hl.rpm	98278	F40803F6
23	omp-appstore-client-5.1.0.1+2-aurora-4.0.2.armv7hl.rpm	924712	A49FFF44
ИТОГО:	-	1031913	3ABAFCF8
Каталог: client-apps-aurora/aurora_market/aurora-5.1.0			
24	feature-appstore-5.1.0.1+2-aurora-5.1.0.aarch64.rpm	8815	3A4F32B3

Номер	Имя файла	Размер (байт)	Контрольная сумма (шестн.)
25	feature-appstore-5.1.0.1+2-aurora-5.1.0.armv7hl.rpm	8906	51F36073
26	omp-appstore-client-5.1.0.1+2-aurora-5.1.0.aarch64.rpm	792878	E7A87434
27	omp-appstore-client-5.1.0.1+2-aurora-5.1.0.armv7hl.rpm	770417	6ECFEF3C
ИТОГО:	-	1581016	E2DBC9C8
Каталог: client-apps-aurora/aurora_market/aurora-5.1.1			
28	feature-appstore-5.1.0.1+2-aurora-5.1.1.aarch64.rpm	8815	AA8D7A18
29	feature-appstore-5.1.0.1+2-aurora-5.1.1.armv7hl.rpm	8905	810F0FD4
30	omp-appstore-client-5.1.0.1+2-aurora-5.1.1.aarch64.rpm	792226	5E1680B4
31	omp-appstore-client-5.1.0.1+2-aurora-5.1.1.armv7hl.rpm	770406	AF370B7D
ИТОГО:	-	1580352	DAA3FE05

7.3.4. КС исполняемых файлов Изделия, размещенных в файлах на DVD с Изделием, приведены в таблице (Таблица 7).

Таблица 7

Имя файла	Описание
/checksums/constant-files/server-const-files.fix.html	КС исполняемых файлов Изделия, расположенных на сервере
/checksums/constant-files/mobile-apps-const-files.fix.html	КС исполняемых файлов приложения «Аврора Маркет» и приложения «Аврора Центр». Информация в файле приведена по каждому RPM-пакету в отдельности. Перечень устанавливаемых RPM-пакетов зависит от приложения и версии ОС, и приведен в таблице (Таблица 6)

8. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

8.1. Контроль Изделия проводится при его первичной установке и закреплении за ответственным лицом и в дальнейшем – в соответствии с порядком проведения регламентных работ комплекса средств автоматизации объекта, но не реже 1 раза в год.

8.2. Контроль Изделия предусматривает проверку DVD с Изделием, которая производится путем их визуального осмотра с целью удостовериться в том, что они не имеют деформаций, механических или иных повреждений. Кроме того, для определения качества записи файлов загрузочных модулей на DVD производят подсчет КС файлов загрузочных модулей Изделия с последующим их сравнением со значениями КС файлов, указанных в 7.3 настоящего документа.

8.3. Ответственное лицо должно не реже 1 раза в месяц производить подсчет КС исполняемых файлов Изделия с последующим их сравнением со значениями, приведенными в 7.3 настоящего документа.

8.4. Подсчет КС файлов загрузочных модулей Изделия, размещенных на DVD, должен проводиться с использованием одной из следующих программ:

– «Программа фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г., окончание срока технической поддержки 26 февраля 2026 г.);

– «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.), «Уровень-3», константа по умолчанию.

8.5. Результаты контроля основных характеристик при эксплуатации и хранении фиксируются в таблице (Таблица 8).

Таблица 8

Наименование	Примечание	Дата проведения проверки					
		20__ г.		20__ г.		20__ г.	
		Фактическая величина	Должность, подпись	Фактическая величина	Должность, подпись	Фактическая величина	Должность, подпись
Прикладное программное обеспечение «Аврора Центр» *DVD с загрузочным модулем Изделия*	При проверке значение должно совпадать со значением, указанным в разделе 7 (∑=)	∑=		∑=		∑=	

9. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Прикладное программное обеспечение «Аврора Центр»	АДМГ.20134-01	Зав. №
наименование программного изделия	обозначение	

соответствует требованиям документа «Технические условия» АДМГ.20134-01 99 01 признано годным для эксплуатации.

Дата выпуска _____

Руководитель предприятия[15]

подпись	расшифровка подписи	дата

М. П.

Ответственный исполнитель[16]

подпись	расшифровка подписи	дата

[15] При электронной поставке маркирование Изделия осуществляется с применением ЭП, которая проставляется на титульном листе настоящего документа.

[16] При электронной поставке маркирование Изделия осуществляется с применением ЭП, которая проставляется на титульном листе настоящего документа.

10. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Прикладное программное обеспечение «Аврора Центр»	АДМГ.20134-01	Зав. №
наименование программного изделия	обозначение	

скомплектовано, маркировано и упаковано ООО «Открытая мобильная платформа» согласно требованиям, предусмотренным документом «Технические условия» АДМГ.20134-01 99 01.

Контролер ОТК[17]

подпись	расшифровка подписи	дата

[17] При электронной поставке маркирование Изделия осуществляется с применением ЭП, которая проставляется на титульном листе настоящего документа.

11. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

11.1. Предприятие-изготовитель гарантирует работоспособность Изделия в соответствии с заявленными характеристиками, предусмотренными настоящим документом, при соблюдении потребителем требований ЭД.

11.2. Предприятие-изготовитель проводит мониторинг общедоступных источников информации, публикующих сведения об уязвимостях, на предмет появления в них сведений об уязвимостях в компонентах Изделия, и принимает меры, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителями выявленных уязвимостей.

11.3. Предприятие-изготовитель обеспечивает устранение уязвимостей посредством предоставления потребителям описания необходимых организационно-технических процедур, направленных на устранение выявленной уязвимости. Также предприятие-изготовитель, в рамках проведения работ по устранению выявленных уязвимостей, разрабатывает обновления ПО.

11.4. Предприятие-изготовитель не предоставляет гарантий или условий (явных или подразумеваемых законодательством Российской Федерации) относительно гарантий товарной пригодности, интегрируемости, годности к использованию для выполнения конкретных задач потребителя, отсутствия ошибок, возможности функционирования при использовании совместно с любым программным или аппаратным обеспечением.

11.5. В случае выявления в Изделии ошибок и дефектов, свидетельствующих о несоответствии Изделия ЭД, и не являющихся уязвимостями Изделия, предприятие-изготовитель по факту получения рекламации потребителя обязуется устранить ошибки и/или дефекты при выпуске обновленных версий Изделия и уведомить об этом потребителей Изделия.

11.6. Рекламации потребителя принимаются при условии, что дефект в Изделии не вызван допущенными со стороны потребителя нарушениями в эксплуатации, хранении и транспортировке Изделия.

11.7. Рекламации предприятию-изготовителю направляются одним из следующих способов:

– по адресу: 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Университетская, д. 7, офис 59;

– по электронной почте: support@omp.ru.

12. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

12.1. Потребитель может предъявить рекламацию предприятию-изготовителю в период гарантийного срока эксплуатации Изделия при обнаружении дефектов функционирования, а также при несоответствии комплектности, упаковки и маркировки поставленного Изделия требованиям, приведенным в ЭД.

12.2. Рекламации предъявляются предприятию-изготовителю в письменном виде с указанием даты обнаружения неисправности (несоответствия), характера ее проявления и условий возникновения.

12.3. Рекламация подписывается руководителем подразделения, принимающего или эксплуатирующего Изделие.

12.4. Сведения о рекламациях и мерах, принятых по рекламациям, регистрируются в таблице (Таблица 9).

Таблица 9

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

13. СВЕДЕНИЯ О ХРАНЕНИИ

13.1. DVD с Изделием и ЭД должны храниться в вертикальном положении на предназначенном для этой цели стеллаже в упаковке, поставленной предприятием-изготовителем, при температуре окружающего воздуха от +10°С до +20°С и относительной влажности воздуха от 20% до 65%.

13.2. В помещении для хранения не должно быть агрессивных примесей, вызывающих разрушение лакокрасочных покрытий и пластмасс.

13.3. При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°С/ч) и воздействия внешних магнитных полей напряженностью более 4000 А/м.

13.4. Сроки и условия хранения Изделия заносят в таблицу (Таблица 10).

Таблица 10

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

14. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

14.1. Изменения в Изделие разрешается вносить представителям предприятия-изготовителя в присутствии службы эксплуатации на основании бюллетеней об изменении.

14.2. Сведения об изменениях в Изделии заносятся в таблицу (Таблица 11).

Таблица 11

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись ответственного за проведение изменения	Подпись ответственного за эксплуатацию Изделия

15. СВЕДЕНИЯ ОБ УСТАНОВКЕ

15.1. Сведения об установке Изделия заносятся в таблицу (Таблица 12).

Таблица 12

Наименование и зав. номер устройства	Фамилия ответственного лица	Номер документа об установке	Подпись ответственного лица и дата

16. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРИ ЭКСПЛУАТАЦИИ

16.1. Сведения о закреплении Изделия заносятся в таблицу (Таблица 13). При первичном закреплении необходимо провести контроль основных характеристик в соответствии с положениями раздела 8 настоящего документа.

Таблица 13

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

17. ОСОБЫЕ ОТМЕТКИ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

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

Таблица 14

Термин/ Сокращение	Расшифровка
АНЗ	Контроль (анализ) защищенности информации
АСУ	Автоматизированная система управления
АУД	Аудит безопасности
БД	База данных
Витрина	Группа приложений, объединенных по определенному признаку
ГИС	Государственная информационная система
ЗНИ	Защита машинных носителей информации
ИАФ	Идентификация и аутентификация
ИБ	Информационная безопасность
Изделие	Прикладное программное обеспечение «Аврора Центр»
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КИИ	Критическая информационная инфраструктура
КС	Контрольная сумма
Мультитенантность	Свойство архитектуры Изделия, позволяющее использовать 1 экземпляр инсталляции Изделия многим организациям (юридическим лицам) совместно, при этом каждая организация работает со своим набором данных
НСД	Несанкционированный доступ
Оператор/ Потребитель	Организация, эксплуатирующая Изделие
ОПС	Ограничение программной среды
ОС	Операционная система
ОТК	Отдел технического контроля
ОЦЛ	Обеспечение целостности ИС и информации
ПБ	Подсистема безопасности
ПМ	Подсистема «Маркет»
ПО	Программное обеспечение
ПООС	Подсистема обновления ОС
ППО	Прикладное программное обеспечение

Термин/ Сокращение	Расшифровка
Предприятие-разработчик, предприятие-изготовитель	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
Приложение	Приложением является мобильное приложение, функционирующее под управлением ОС Аврора
ПУ	Подсистема Платформа управления
ПУТ	Подсистема управления тенантами
ПСУ	Подсистема Сервис уведомлений
РСБ	Регистрация событий безопасности
Сервис-провайдер	Организация, которая использует Изделие в качестве одного из составляющих для создания своей услуги или продукта. Данная услуга или продукт предоставляется клиентам Сервис-провайдера
СЗИ	Средство защиты информации
СУБД	Система управления базами данных
УПД	Управление доступом
Устройство	Под устройством подразумевается мобильное устройство, на котором функционируют соответствующие компоненты Изделия
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭД	Эксплуатационные документы
ЭП	Электронная подпись
Bluetooth®	Стандарт беспроводной связи, обеспечивающий обмен данными между устройствами на основе ультракоротких радиоволн
CDN	Content Delivery Network
DVD	Digital Video Disc – оптический носитель информации, выполненный в форме диска, для хранения различной информации в цифровом виде
Endpoint	Конечная точка – само обращение к маршруту отдельным HTTP методом. Эндпоинт выполняют конкретную задачу, принимают параметры и возвращают данные Клиенту

Термин/ Сокращение	Расшифровка
HTTP	HyperText Transfer Protocol – протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», т.е. предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают сообщение с результатом
IMEI	International Mobile Equipment Identity – уникальный номер устройства, состоящий из 15 цифр
ISO-образ	Образ оптического диска, содержащий файловую систему стандарта ISO 9660
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
LDAP	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов
MAC	Media Access Control – уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей
MTP	Media Transfer Protocol – аппаратно-независимый протокол, основанный на PTP
QR-код	Quick Response Code – код быстрого реагирования, предоставляющий информацию для быстрого ее распознавания с помощью камеры на устройстве
RFC	Request For Comments – запрос комментариев
RPM-пакет	Файл формата .rpm, позволяющий устанавливать, удалять и обновлять приложение на устройстве
SIM	Subscriber Identification Module – Модуль идентификации абонента
TCP	Transmission Control Protocol – протокол транспортного уровня, гарантирующий целостность передаваемых данных и уведомление отправителя о результатах передачи
TLS	Transport Layer Security – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет

Термин/ Сокращение	Расшифровка
USB	Universal Serial Bus – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
WLAN	Wireless Local Area Network – локальная сеть, построенная на основе беспроводных технологий

ПРИЛОЖЕНИЕ 1

Требования к мерам защиты информации, реализуемые в Изделии

Реализуемые в Изделии требования к мерам защиты информации приведены в таблице (Таблица 1.1).

Таблица 1.1

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 1, 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
РСБ.8				Обеспечение возможности просмотра информации о действиях отдельных пользователей

ПРИМЕЧАНИЕ. Далее по тексту будет использоваться идентификация мер в нотации приказа ФСТЭК России от 11 февраля 2013 г. № 17.

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

Идентификация и аутентификация пользователей Изделия, являющихся работниками оператора (ИАФ.1) в части:

– идентификации пользователей Изделия;

– аутентификации пользователей Изделия с использованием паролей;

– аутентификации пользователей Изделия с ролью Сервер приложений с использованием ЭП.

Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2) в части:

– идентификации устройств по логическим именам. Аутентификация устройств в Изделии должна осуществляться по протоколу OpenID Connect 1.0 и с использованием пароля, формируемого ПБ.

Идентификация и аутентификация устройств должна осуществляться с помощью приложения «Аврора Центр».

Управление идентификаторами (ИАФ.3) в части:

– создания идентификатора пользователя и(или) устройства;

– исключения повторного использование идентификатора пользователя в течение – не менее 3 лет (для реализации усиления 1б);

– блокирования идентификатора пользователя через заданный в настройках Изделия период времени неиспользования.

Управление средствами аутентификации (ИАФ.4) в части:

– изменения аутентификационной информации;

– генерация и выдача начальной аутентификационной информации;

– установление характеристик пароля.

Установление следующих характеристик 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, а также ключа ЭП;

– 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.

Защита обратной связи при вводе аутентификационной информации (ИАФ.5) в части:

– сокрытия от пользователя действительного значения аутентификационной информации в процессе аутентификации. Вводимые символы пароля должны отображаться условными знаками «*» или «•».

Управление доступом субъектов доступа к объектам доступа (УПД)

Управление (заведение, активация, блокирование) учетными записями пользователей (УПД.1) в части:

– управления учетными записями пользователей Изделия;

– заведения, активации, блокирования и удаления учетных записей;

– модификации учетных записей пользователей Изделия;

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

Реализация дискреционного и ролевого методов управления доступом (УПД.2) в части:

– реализации дискреционного и ролевого управления доступом для субъектов Изделия к объектам Изделия;

– правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в Изделие (для реализации усиления 1);

– правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым Изделием (для реализации усиления 4).

ПРИМЕЧАНИЕ. Дискреционный метод управления доступом реализован в отношении доступа тенантов (платформ управления) к витринам приложений. Администратор ПМ может настраивать (запрещать или разрешать) доступ отдельных тенантов (платформ управления) к витринам приложений. Во всех остальных случаях используется ролевая модель разграничения доступа. Перечень объектов и субъектов

доступа, на которые распространяется ролевая модель, приведен в документе «Описание применения» АДМГ.20134-01 31 01.

Субъектами доступа являются пользователи Изделия и процессы без участия пользователей, при этом субъектам доступа может быть назначена одна или несколько ролей, позволяющих выполнять следующие действия:

– Администратор учетных записей – управлять учетными записями пользователей (наличие роли обязательно);

– Оператор аудита – работать с журналом регистрации событий;

– Администратор Аврора Маркета – управлять ПМ через интерфейс Изделия;

– Разработчик – добавлять новые, обновлять ранее загруженные приложения и получать информацию о них;

– Редактор приложений – обновлять и получать информацию о ранее загруженных приложениях;

– Пользователь Аврора Маркета – загружать приложения и получать информацию о них;

– Администратор Платформы управления – управлять ПУ через интерфейс Изделия;

– Приложение «Аврора Центр» (процесс без участия пользователей) – назначается учетным записям приложения «Аврора Центр»;

– Администратор тенантов – управлять ПУТ через интерфейс Изделия;

– Администратор Сервиса уведомлений – управлять жизненным циклом проектов;

– Мобильное приложение (процесс без участия пользователей) – получать push-уведомления;

– Сервер приложений – назначается серверам приложений для передачи push-уведомлений на Сервер приложений ПСУ.

Доступ к объектам доступа Изделия 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 приложении документа «Описание применения» АДМГ.20134-01 31 01.

Ограничение неуспешных попыток входа в Изделие (УПД.6) в части:

– автоматическое блокирование 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) (для реализации усиления 1).

Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя Изделия (УПД.9) в части:

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

– не более 2 одновременных сессий для привилегированных учетных записей (для реализации усиления 1а);

– отображения администратору числа активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей (для реализации усиления 3).

Блокирование сеанса доступа в Изделие после установленного времени бездействия (неактивности) пользователя (УПД.10), в части:

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

Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11), в части:

– запрета действий пользователей до прохождения ими процедур идентификации и аутентификации.

Регистрация событий безопасности (РСБ)

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3) в части:

– сбора и записи информации о событиях безопасности, а именно:

- регистрации фактов применения механизма идентификации и аутентификации (вход/выход пользователей Изделия);
- регистрации фактов доступа к защищаемым объектам доступа;
- регистрации фактов изменения полномочий субъектов доступа.

Для каждого события должны регистрироваться:

– идентификатор субъекта доступа;

– идентификатор объекта доступа, когда это применимо;

– время и дата запроса;

– результат запроса.

Запись информации о событиях безопасности должна осуществляться в регистрационный журнал Изделия.

Защита информации о событиях безопасности в части (РСБ.7):

– предоставления доступа к записям регистрации (аудита) только уполномоченным пользователям.

Обеспечение возможности просмотра информации о действиях отдельных пользователей (РСБ.8 в нотации 17-го приказа ФСТЭК России).

ПРИЛОЖЕНИЕ 2

Меры по защите информации в ИС, которые позволяет обеспечивать Изделие путем его применения в ИС для управления устройствами

Набор мер, которые позволяет обеспечивать Изделие путем его применения в ИС для управления устройствами, приведен в таблице (Таблица 2.1).

Таблица 2.1

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.4	ИАФ.4	ИАФ.4	ИАФ.4	Управление средствами аутентификации
Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.14	УПД.14	УПД.14	УПД.14	Контроль использования в ИС технологий беспроводного доступа
Ограничение программной среды (ОПС)				
ОПС.2	ОПС.2	ОПС.2	ОПС.2	Управление установкой (инсталляцией) компонентов ПО, а также контроль за установкой компонентов ПО
ОПС.3	ОПС.3	УКФ.3	УКФ.3	Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов
Защита машинных носителей информации (ЗНИ)				
ЗНИ.1	ЗНИ.1	ЗНИ.1	ЗНИ.1	Учет машинных носителей информации
ЗНИ.5	ЗНИ.5	ЗНИ.5	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	ЗНИ.8	ЗНИ.8	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях

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)	
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
Контроль (анализ) защищенности информации (АНЗ)				
АНЗ.2	АНЗ.2	ОПО.4	ОПО.4	Контроль установки обновлений ПО
АНЗ.4	АНЗ.4	-	-	Контроль состава технических средств и ПО
Обеспечение целостности ИС и информации (ОЦЛ)				
ОЦЛ.1	ОЦЛ.1	ОЦЛ.1	ОЦЛ.1	Контроль целостности ПО
ОЦЛ.3	ОЦЛ.3	ОДТ.6	ОДТ.6	Восстановление ПО, включая ПО СЗИ, при возникновении нештатных ситуаций
Выявление инцидентов и реагирование на них (ИНЦ)				
	ИНЦ.2	ИНЦ.1	ИНЦ.1	Выявление инцидентов и реагирование на них
Управление конфигурацией (УКФ)				
	УКФ.2	УКФ.2	УКФ.2	Управление изменениями конфигурации ИС
		УКФ.3	УКФ.3	Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов

ПРИМЕЧАНИЕ. Далее по тексту будет использоваться идентификация мер в нотации приказа ФСТЭК России от 11 февраля 2013 г. № 17.

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

Управление средствами аутентификации (ИАФ.4) в части:

– изменения аутентификационной информации пользователей устройств;

– установления характеристик пароля пользователя устройства.

Установление следующих характеристик пароля:

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

– максимальное время действия пароля, а также ключа ЭП.

Управление доступом субъектов доступа к объектам доступа (УПД)

Контроль использования в ИС технологий беспроводного доступа (УПД.14) в части управления на устройствах следующими технологиями беспроводного доступа:

– WLAN;

– точка доступа WLAN;

– Bluetooth®.

Ограничение программной среды (ОПС)

Управление установкой (инсталляцией) компонентов ПО, а также контроль за установкой компонентов ПО (ОПС.2) в части:

– установки, обновления, удаления ПО на устройствах;

– предоставления сведений Администратору Платформы управления об установленном с помощью ПУ на устройствах ПО.

Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов (ОПС.3) в части:

– централизованного управления перечнем установленного на устройствах ПО;

– централизованного управления перечнем ПО, доступного пользователям для установки на устройствах («белый список»);

– контроля ПО, установленного (инсталлированного) с помощью ПУ на устройствах, на предмет соответствия его перечню ПО, разрешенного к установке на устройствах в соответствии с АН3.4, а также на предмет отсутствия ПО, запрещенного оператором к установке.

Защита машинных носителей информации (ЗНИ)

Учет машинных носителей информации (ЗНИ.1) в части:

– учета устройств.

В качестве регистрационных номеров используются идентификаторы устройств (IMEI или MAC WLAN).

Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации (ЗНИ.5) в части:

– управления передачей данных по MTP (передача данных по USB устройств).

Уничтожение (стирание) информации на машинных носителях (ЗНИ.8) в части:

– передачи управляющего сообщения на очистку устройства до заводского состояния.

Регистрация событий безопасности (РСБ)

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3) в части:

– записи и хранения информации о событиях безопасности, полученных с устройств.

Перечень событий безопасности, подлежащих регистрации, определяется ОС устройства.

Защита информации о событиях безопасности (РСБ.7) в части:

– предоставления доступа к записям регистрации (аудита) только уполномоченным пользователям.

Контроль (анализ) защищенности информации (АНЗ)

Контроль установки обновлений ПО (АНЗ.2) в части:

– установки и контроля обновления ОС устройств;

– установки и контроля обновления ПО устройств.

Контроль состава технических средств и ПО (АН3.4) в части:

– учета устройств;

– централизованного управления перечнем установленного на устройствах ПО;

– централизованного управления перечнем ПО, доступного пользователям для установки на устройствах («белый список»);

– контроля ПО, установленного (инсталлированного) с помощью ПУ на устройствах, на предмет соответствия его перечню ПО, разрешенному к установке на устройствах в соответствии с АН3.4, а также на предмет отсутствия ПО, запрещенного оператором к установке.

Обеспечение целостности ИС и информации (ОЦЛ)

Контроль целостности ПО (ОЦЛ.1) в части:

– контроля целостности компонентов ПО (за исключением СЗИ) по наличию имен (идентификаторов) компонентов ПО.

Восстановление ПО, включая ПО СЗИ, при возникновении нештатных ситуаций (ОЦЛ.3) в части:

– возврата устройства в начальное состояние (передачи управляющего сообщения на сброс устройства до заводского состояния), обеспечивающее его штатное функционирование.

Выявление инцидентов и реагирование на них (ИНЦ)

Обнаружение инцидентов и реагирование на инциденты (ИНЦ.2 в нотации 21-го приказа ФСТЭК России) в части:

– задания на устройствах офлайн-сценариев, которые выполняются при наступлении заданных событий (инцидентов).

Управление конфигурацией информационной системы (УКФ)

Управление изменениями конфигурации информационной системы (УКФ.2) в части:

– установки, обновления, удаления ПО на устройствах;

– установки обновления ОС устройств;

– управления настройками устройств, согласно п. 3.3.3;

– контроля за состоянием устройств и их настройками.

Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов (УКФ.3 в нотации 31-го и 239-го приказов ФСТЭК России) в части:

– централизованного управления перечнем установленного на устройствах ПО;

– централизованного управления перечнем ПО, доступного пользователям для установки на устройствах («белый список»);

– контроля ПО, установленного (инсталлированного) с помощью ПУ на устройствах, на предмет соответствия его перечню ПО, разрешенного к установке на устройствах в соответствии с АН3.4, а также на предмет отсутствия ПО, запрещенного оператором к установке.

ПРИЛОЖЕНИЕ 3

Общие положения предприятия-изготовителя по возможным вариантам поставки Изделия

Основные положения по получению Изделия потребителем:

1) Изделие поставляется в строгом соответствии с Лицензионным договором;

2) Комплектность Изделия соответствует положениям раздела 7 настоящего документа и условиям Лицензионного договора;

3) Варианты носителей информации Изделия могут быть следующими:

– поставка на электронном носителе: DVD – оптический носитель информации, при этом DVD изготавливается предприятием-изготовителем Изделия и передается потребителю в подготовленном виде, в соответствии с технологическими процессами предприятия-разработчика;

– поставка по электронным каналам связи: информационный ресурс предприятия-изготовителя, информация по доступу, а также правила работы с ним доводятся до потребителя при заключении Лицензионного договора. Подлинность и целостность Изделия обеспечивается применением ЭП.

Способ передачи Изделия по электронным каналам связи предусматривает следующее обязательное условие: подготовка DVD, входящих в комплект поставки Изделия, производится на стороне потребителя.

Пример маркировки с указанием обязательных полей подготовленного потребителем DVD приведен в приложении (Приложение 4).

При передаче Изделия по электронным каналам связи потребитель должен выполнить следующие действия:

– после загрузки загрузочного модуля Изделия и комплекта ЭД необходимо произвести проверку подлинности и целостности путем проверки ЭП[18];

– провести расчет КС DVD Изделия с использованием программы «Программа фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г., окончание срока технической поддержки 26 февраля 2026 г.);

– сравнить КС с указанными в соответствующем обновленном разделе настоящего документа. При расхождении КС с эталонными значениями, указанными в настоящем документе, необходимо обратиться в службу технической поддержки предприятия-изготовителя Изделия.

[18] Инструкция с описанием порядка проверки ЭП, сертификат проверки ЭП, скрипт проверки ЭП и ЭП размещены на веб-сайте предприятия-изготовителя Изделия (https://auroraos.ru/documentation).

ПРИЛОЖЕНИЕ 4

Пример маркировки DVD с Изделием

Расположение полей при маркировке DVD, входящего в комплект поставки Изделия, приведено на рисунке (Рисунок 4.1), а их описание – в таблице (Таблица 4.1).

Рисунок 4.1

Таблица 4.1

Поле	Информация по заполнению	Примечания
Наименование Изделия	Соответствует положениям раздела 7 настоящего документа и условиям Лицензионного договора	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия

Поле	Информация по заполнению	Примечания
Обозначение Изделия (децимальный номер)	АДМГ.20134-01	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия
Дата изготовления	Проставляется в соответствии с актом приема-передачи Изделия. Также может быть проставлена дата фактического изготовления DVD	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия
Контрольная сумма	Соответствует положениям раздела 7 (Таблица 4) настоящего документа и условиям Лицензионного договора	Поле является обязательным к заполнению ТОЛЬКО для DVD, содержащего загрузочный модуль Изделия. Заполняется при любом из возможных вариантов и способов поставки Изделия
ОТК	Соответствует положениям раздела 10 настоящего документа	Поле является обязательным к заполнению ТОЛЬКО для DVD, содержащего загрузочный модуль Изделия
Зав. №	Соответствует положениям раздела 9 настоящего документа. ПРИМЕЧАНИЕ. Идентификатор присваивается в соответствии с положениями, зафиксированными в документе «Положение о системе сертификации средств защиты информации», утвержденном приказом ФСТЭК России от 03 апреля 2018 г.№55	Поле является обязательным к заполнению ТОЛЬКО для DVD, содержащего загрузочный модуль Изделия. Заполняется при любом из возможных вариантов и способов поставки Изделия

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-рованных					