

УТВЕРЖДЕН
АДМГ.20134-01 90 01-1-ЛУ

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство пользователя

Часть 3

Подсистема Платформа управления

АДМГ.20134-01 90 01-3

Листов 322

АННОТАЦИЯ

Настоящий документ является третьей частью руководства пользователя Прикладного программного обеспечения «Аврора Центр» АДМГ.20134-01 (далее – ППО) релиз 5.3.0 и содержит описание функционирования подсистемы Платформа управления (ПУ), входящей в состав ППО.

ППО является прикладным программным обеспечением со встроенными механизмами защиты информации от несанкционированного доступа, предназначенным для:

- управления устройствами¹, функционирующими под управлением операционной системы (ОС) Аврора, ОС Android и ОС семейства Linux;
- управления жизненным циклом приложений²;
- 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 ППО 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.

ППО может быть использовано, но не ограничиваться, в системах и объектах, описание которых приведено в документе «Руководство администратора» АДМГ.20134-01 91 01.

ПРИМЕЧАНИЯ:

✓ Подробная информация о составе и назначении ППО, а также требования к условиям выполнения приведены в документе «Руководство администратора» АДМГ.20134-01 91 01;

✓ Подробная информация об особенностях резервного копирования приведена в документе «Рекомендации по резервному копированию» АДМГ.20134-01 91 02.

¹ Определение термина «Устройство» приведено в таблице (Таблица 61).

² Определение термина «Приложение» приведено в таблице (Таблица 61).

АДМГ.20134-01 90 01-3

Описание интерфейсов подсистем, входящих в состав ППО, 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;

– «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 ППО приведено в документе «Описание применения» АДМГ.20134-01 31 01. Состав разделов интерфейса ППО зависит от вариантов поставки, подробное описание которых приведено в документе «Формуляр» АДМГ.20134-01 30 01.

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.

ВНИМАНИЕ! Подробная информация о работе с приложениями, входящими в состав Изделия и функционирующими на соответствующих ОС, приведена на официальном веб-сайте предприятия-разработчика: <https://auroraos.ru/documentation#!/tab/565511138-2>. При необходимости для получения дополнительной информации можно направить запрос на электронную почту: info@omp.ru.

СОДЕРЖАНИЕ

1. Подготовка к работе	7
1.1. Описание принципов безопасной работы средства	7
1.1.1. Общая информация	7
1.1.2. Компрометация паролей	7
1.1.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения	8
1.2. Лицензионное соглашение	8
1.3. Начало сеанса работы	8
1.4. Описание интерфейса	11
1.4.1. Верхняя панель	11
1.4.2. Рабочая область	12
1.5. Работа с фильтрами	15
2. Работа в разделе «Управление» Консоли администратора ПУ	23
2.1. Общее описание карточек элементов управления	23
2.1.1. Работа с карточкой устройства	23
2.1.2. Работа с карточкой группы устройств	58
2.1.3. Работа с карточкой пользователя	62
2.1.4. Работа с карточкой группы пользователей	66
2.1.5. Работа с карточкой политики	70
2.1.6. Работа с карточкой офлайн-сценария	73
2.1.7. Работа с карточкой файла	75
2.2. Подраздел «Устройства»	76
2.2.1. Добавление устройства в ПУ	78
2.2.2. Добавление группы устройств вручную	81
2.2.3. Добавление устройств или группы устройств с помощью CSV-файла	86
2.2.4. Добавление приглашения на самостоятельную регистрацию устройства	94
2.2.5. Заявки на активацию	100
2.2.6. Экспорт списка устройств в CSV-файл	103
2.2.7. Привязка устройства к пользователю	104
2.2.8. Привязка устройств к группе устройств	106
2.2.9. Активация устройств	108
2.2.10. Применение оперативных команд	123
2.2.11. Отвязка (исключение) устройств из группы устройств	129
2.2.12. Архивирование устройства	131
2.2.13. Восстановление устройств из архива	134
2.2.14. Удаление группы устройств	136
2.2.15. Очистка устройств до заводских настроек	136
2.2.16. Вывод устройства из эксплуатации	137
2.3. Подраздел «Пользователи»	139

2.3.1. Добавление пользователя устройства вручную.....	140
2.3.2. Добавление группы пользователей вручную.....	141
2.3.3. Добавление пользователей или группы пользователей с помощью CSV-файла	144
2.3.4. Привязка пользователей к группе пользователей.....	153
2.3.5. Привязка пользователей к устройствам	157
2.3.6. Отвязать (исключить) пользователей из группы пользователей.....	159
2.3.7. Архивирование пользователя.....	161
2.3.8. Удаление группы пользователей.....	163
2.4. Подраздел «Политики»	164
2.4.1. Общее описание правил политик.....	172
2.4.2. Добавление политики вручную	216
2.4.3. Добавление политики на основе корпоративного шаблона	217
2.4.4. Назначение политики на группы устройств или группы пользователей ..	220
2.4.5. Добавление политики на основе существующей	223
2.4.6. Редактирование правила политики	224
2.4.7. Отвязка политики от группы устройств или группы пользователей.....	227
2.4.8. Удаление политики.....	230
2.5. Подраздел «Сценарии».....	230
2.5.1. Добавление офлайн-сценария	234
2.5.2. Назначение офлайн-сценария на группы устройств или группы пользователей	238
2.5.3. Отвязка офлайн-сценарий от группы устройств/группы пользователей...	241
2.5.4. Удаление офлайн-сценария.....	243
2.6. Подраздел «Файлы»	244
2.6.1. Добавление файла (скрипта)	245
2.6.2. Добавление, скачивание, согласование и удаление версии файла (скрипта)	247
2.6.3. Доставка файла и выполнение скрипта на устройстве с помощью ПУ	249
2.6.4. Удаление файла (скрипта) со всеми его версиями	250
3. Работа в разделе «Мониторинг» Консоли администратора ПУ в Подразделе «Индикаторы»	251
4. Работа в разделе «Администрирование» Консоли администратора ПУ	254
4.1. Подраздел «Настройки».....	254
4.1.1. Доверенные сертификаты.....	255
4.1.2. Категории пользовательских сертификатов	257
4.1.3. Платформа	260
4.1.4. Интеграция (информация о серверах)	263
4.1.5. Территории.....	286
4.1.6. Настройки правил политик	288
4.1.7. Доверенные сети	289

4.1.8. Переменные к подстановке для скриптов.....	291
4.2. Подраздел «Орг.структура»	294
5. Сообщения об ошибках и ограничения	296
5.1. Сообщения об ошибках.....	296
5.2. Ошибки импорта	303
5.2.1. Ошибки импорта устройств	303
5.2.2. Ошибки импорта пользователей.....	305
5.3. Ограничения	307
Перечень терминов и сокращений.....	308
Приложение 1.....	310
Приложение 2.....	312
Приложение 3.....	315
Приложение 4.....	316
Приложение 5.....	321

1. ПОДГОТОВКА К РАБОТЕ

ПРИМЕЧАНИЕ. Для работы пользователей с интерфейсом ППО необходимо выполнение следующих условий:

- веб-браузер должен поддерживать следующие технологии: TLS, CSS3, HTML5, ECMAScript 5 и Cookie. Рекомендуется использовать веб-браузер Chrome версии 90 или выше;

- веб-браузер в информационных системах, обрабатывающих информацию ограниченного доступа, требующую защиты в соответствии с законодательством РФ необходимо использовать из состава ОС, имеющей сертификат соответствия ФСТЭК России. Рекомендуется использовать веб-браузеры: Firefox ESR версии 91.4 или выше, Chromium версии 87 или выше;

- разрешение экрана монитора должно быть не менее 1280x960 px.

1.1. Описание принципов безопасной работы средства

1.1.1. Общая информация

ППО реализует следующие функции безопасности:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности.

При использовании ППО необходимо выполнение следующих мер по защите информации от несанкционированного доступа:

- соблюдение парольной политики;
- соблюдение требования, согласно которому пароль не должен включать в себя легко вычисляемые сочетания символов;
- отсутствие у пользователя права передачи личного пароля третьим лицам;
- обязанность пользователя при вводе пароля исключить возможность его перехвата третьими лицами и техническими средствами.

При эксплуатации ППО запрещается:

- оставлять без контроля незаблокированные программные средства и/или ППО;
- разглашать пароли, выводить их на экран, принтер или иные средства отображения информации.

1.1.2. Компрометация паролей

Под компрометацией паролей необходимо понимать следующее:

- физическую утрату носителя с парольной информацией;
- передачу идентификационной информации по открытым каналам связи;
- перехват пароля при распределении идентификаторов;
- сознательную передачу информации третьим лицам.

ПРИМЕЧАНИЕ. При компрометации пароля пользователь обязан незамедлительно оповестить Администратора учетных записей.

1.1.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения

Настройки параметров безопасности ППО доступны только пользователям с ролью Администратор учетных записей и заключаются в возможности управления ролями пользователей ППО.

Пользователям должны назначаться минимальные права и привилегии, необходимые для выполнения ими своих должностных обязанностей (функций).

1.2. Лицензионное соглашение

Перед использованием ППО пользователю необходимо ознакомиться с условиями Лицензионного соглашения с конечным пользователем (Лицензионное соглашение³), которое будет отображаться при установке системы, а также доступно к просмотру в верхнем правом углу каждого из подразделов интерфейса ППО в пункте «О платформе». Подробное описание работы в разделе «О платформе» приведено в п. 1.4.1.

ПРИМЕЧАНИЕ. Любое использование ППО означает полное и безоговорочное принятие пользователем условий Лицензионного соглашения.

1.3. Начало сеанса работы

ВНИМАНИЕ! Первоначальный вход в ППО осуществляется с помощью Консоли администратора ПБ и предустановленной учетной записи с ролью Администратор учетных записей. Подробная информация приведена в документе «Руководство администратора» АДМГ.20134-01 91 01.

Для аутентификации в Консоли администратора ПУ необходимо выполнить следующие действия:

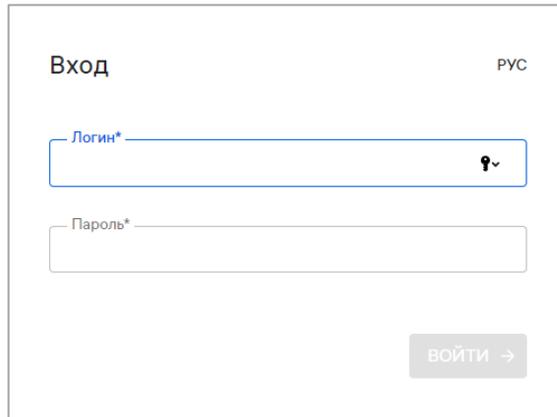
- в веб-браузере перейти по адресу Консоли администратора ПУ.

ПРИМЕЧАНИЕ. Для получения адреса Консоли администратора ПУ необходимо обратиться к системному администратору либо иному лицу, ответственному за установку и настройку системы;

- на странице аутентификации выполнить следующие действия:
 - выбрать язык интерфейса (по умолчанию интерфейс отображается на языке браузера пользователя);
 - заполнить поля «Логин» и «Пароль»;
 - нажать кнопку «Войти» (Рисунок 1).

³ Лицензионное соглашение отличается в зависимости от вариантов поставки.

ПРИМЕЧАНИЕ. Данные для заполнения полей «Логин» и «Пароль» Администратору Платформы управления предоставляет Администратор учетных записей. Процесс создания учетной записи Администратора Платформы управления приведен в документе «Руководство пользователя. Часть 1. Подсистема безопасности» АДМГ.20134-01 90 01-1.

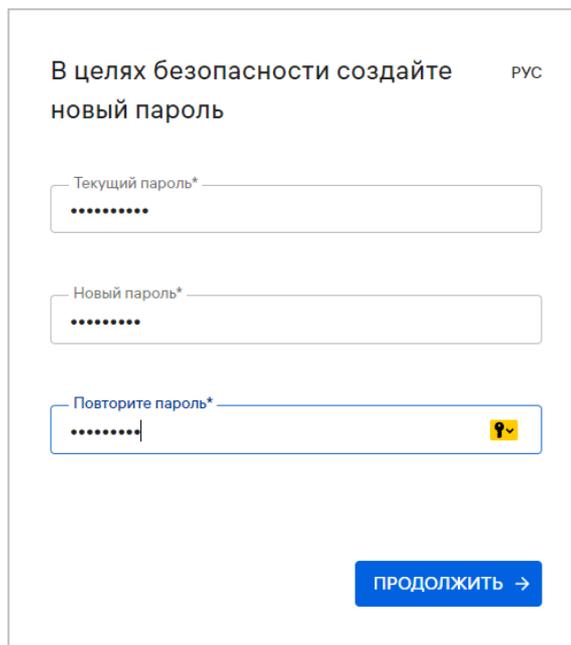


The screenshot shows a login interface with the title "Вход" and a language selector "РУС". There are two input fields: "Логин*" and "Пароль*", both with asterisks indicating they are required. The "Логин*" field has a small key icon on the right. Below the fields is a button labeled "ВОЙТИ →".

Рисунок 1

В целях безопасности при первом входе пользователю ПУ будет предложено сменить пароль. Для этого в открывшемся окне необходимо выполнить следующие действия (Рисунок 2):

- ввести текущий пароль;
- ввести новый пароль;
- повторно ввести новый пароль;
- выбрать язык интерфейса;
- нажать кнопку «Продолжить».



The screenshot shows a password change interface with the title "В целях безопасности создайте новый пароль" and a language selector "РУС". There are three input fields: "Текущий пароль*", "Новый пароль*", and "Повторите пароль*", all with asterisks indicating they are required. The "Повторите пароль*" field has a small key icon on the right. Below the fields is a blue button labeled "ПРОДОЛЖИТЬ →".

Рисунок 2

Новый пароль должен содержать:

- от 8 до 255 символов;
- заглавные буквы;
- строчные буквы;
- цифры;
- спецсимволы.

ПРИМЕЧАНИЕ. Срок действия пароля 60 дней. По истечении указанного срока пароль необходимо сменить, при этом новый пароль должен отличаться от 3 ранее вводимых.

По умолчанию для каждого пользователя возможно не более двух одновременных (параллельных) сессий доступа.

При превышении допустимого количества сессий отобразится окно с информационным сообщением «Вы превысили количество допустимых сессий. Текущие сессии будут завершены» (Рисунок 3), где необходимо выполнить одно из следующих действий:

- нажать кнопку «Подтвердить», в результате чего все текущие сессии завершатся и будет выполнен вход в Консоль администратора ПУ;
- нажать кнопку «Отмена», в результате чего все текущие сессии останутся активными и отобразится окно входа в Консоль администратора ПУ.

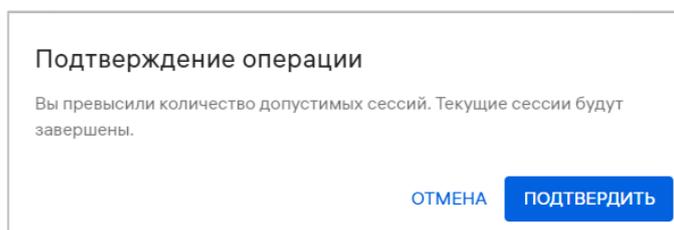


Рисунок 3

При успешной аутентификации отобразится страница Консоли администратора ПУ.

ПРИМЕЧАНИЕ. В случае изменения списка ролей необходимо пройти повторную аутентификацию.

Системным администратором могут быть установлены следующие настройки:

- автоматический выход из системы (в случае неактивности пользователя более 5 минут). Для продолжения работы необходимо повторно пройти аутентификацию;
- блокировка учетной записи пользователя (в случае неактивности пользователя в течение 45 дней). Для продолжения работы необходимо обратиться к системному администратору.

1.4. Описание интерфейса

ВНИМАНИЕ! В зависимости от конфигурации, настроек и вариантов поставки⁴ ППО состав разделов верхней панели интерфейса ППО может отличаться.

Настоящий документ содержит описание работы ПУ и относящихся к ней подразделов верхней панели интерфейса.

1.4.1. Верхняя панель

Верхняя панель позволяет выполнить следующие действия:

1) Осуществлять навигацию между подсистемами ППО (Рисунок 4 [1]).

Работа в верхней панели Консоли администратора ПУ выполняется в следующих разделах:

- «Мониторинг» (раздел 3), включающем в себя подраздел «Индикаторы» (подраздел 3);
- «Управление» (раздел 2), включающем в себя следующие подразделы:
 - «Устройства» (подраздел 2.2);
 - «Пользователи» (подраздел 2.3);
 - «Политики» (подраздел 2.4);
 - «Сценарии» (подраздел 2.5);
 - «Файлы» (подраздел 2.6);
- «Администрирование» (раздел 4), включающем в себя следующие подразделы:
 - «Настройки» (подраздел 4.1);
 - «Орг.структура» (подраздел 4.2);

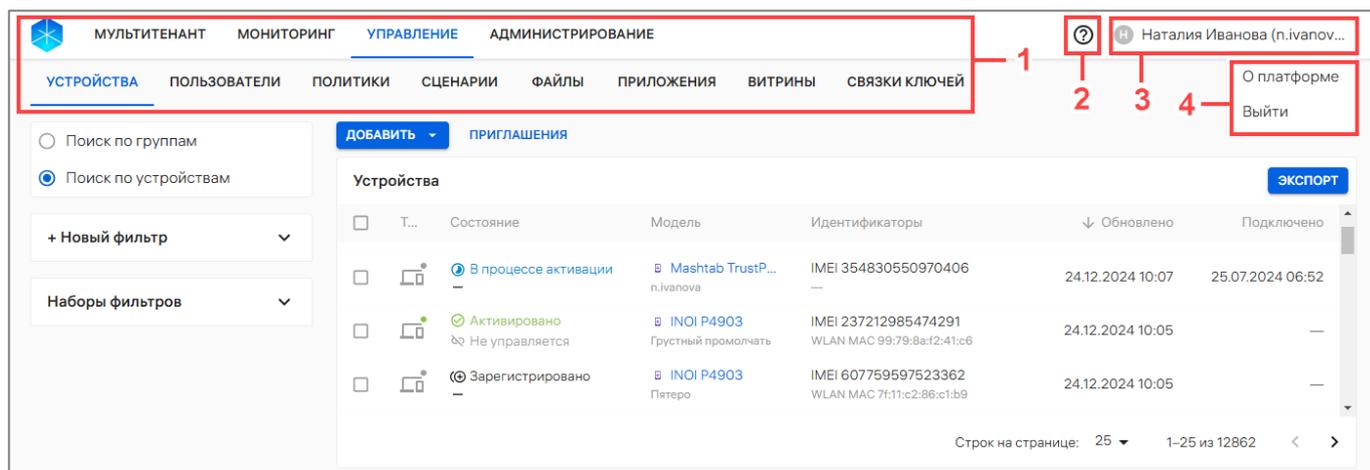


Рисунок 4

2) Получить доступ к справке с инструкцией и описанием работы в ППО нажатием значка (см. Рисунок 4 [2]);

⁴ Комплектность вариантов поставки определяется условиями Лицензионного договора.

3) Просматривать следующую информацию об учетной записи пользователя в меню текущего пользователя (см. Рисунок 4 [3]):

- имя;
- фамилия;
- Email;

4) Выбирать соответствующие пункты из раскрывающегося списка нажатием значка⁵  в меню пользователя (см. Рисунок 4 [4]):

- «О платформе», содержащий (Рисунок 5):
 - активную ссылку на Лицензионное соглашение, при нажатии на которую отобразится текст Лицензионного соглашения (Рисунок 5 [1]);
 - список версий сервисов ППО (Рисунок 5 [2]);
 - кнопку «Скопировать сервисы» для копирования информации о сервисах в буфер обмена (Рисунок 5 [4]);
 - кнопку «Закреть» (Рисунок 5 [3]) для выхода из раздела «О платформе»;

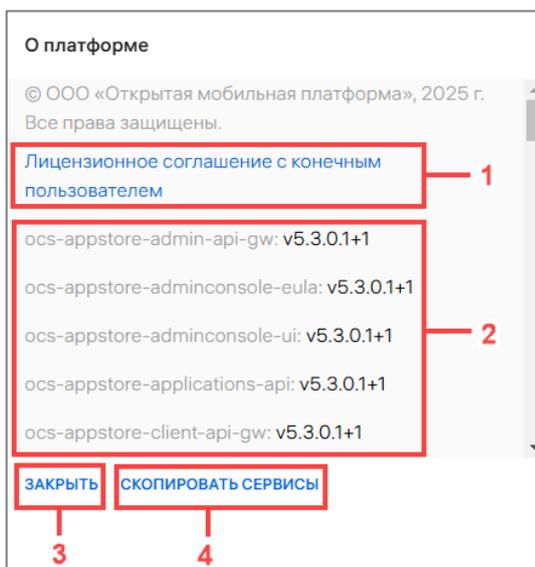


Рисунок 5

– «Выйти» – пункт для завершения сеанса работы в ППО. В результате выхода отобразится Консоль входа пользователей (см. Рисунок 1).

1.4.2. Рабочая область

В рабочей области отображаются данные выбранного подраздела Консоли администратора ПУ и осуществляется работа с элементами его интерфейса (Рисунок 6 [1]), в частности:

– добавление устройства, групп устройств, пользователей или групп пользователей (вручную, с помощью CSV-файла);

⁵ Внешний вид значка может отличаться от приведенного на рисунках в настоящем документе. На значке отображается первая буква имени пользователя.

АДМГ.20134-01 90 01-3

- добавление приглашения на самостоятельную регистрацию устройства;
- привязка устройства к пользователю и его отвязка (вручную, с помощью CSV-файла);
- блокировка и разблокировка устройства;
- очистка содержимого устройства;
- блокировка и разблокировка камеры устройства;
- получение списка системных сообщений с устройства и событий безопасности;
- назначение и отслеживание политик, назначенных на пользователей, группу пользователей, устройства или группу устройств;
- создание и назначение на группу пользователей или группу устройств офлайн-сценариев;
- просмотр информации о текущем и целевом состоянии устройств;
- просмотр информации о назначенных оперативных командах, политиках и офлайн-сценариях на устройствах, а также о том, какие из них являются действующими в момент просмотра;
- мониторинг текущего состояния устройства;
- просмотр организационной структуры компании.

ВНИМАНИЕ! В зависимости от ОС доступность управляющих действий для устройств может быть ограничена.

В Консоли администратора ПУ элементы интерфейса, выделенные цветом (Рисунок 6 [2]), представляют собой активные ссылки, при нажатии на которые можно выполнить переход на страницу/карточку, где приведена более подробная информация и имеется возможность скопировать данные в буфер обмена.

Для упрощения взаимодействия Администратора Платформы управления с интерфейсом Консоли администратора ПУ предусмотрены всплывающие подсказки (Рисунок 6 [3]), которые отображаются при наведении курсора на соответствующий элемент, а также значки (Таблица 1), доступные в списке быстрых действий и позволяющие управлять выбранными элементами.

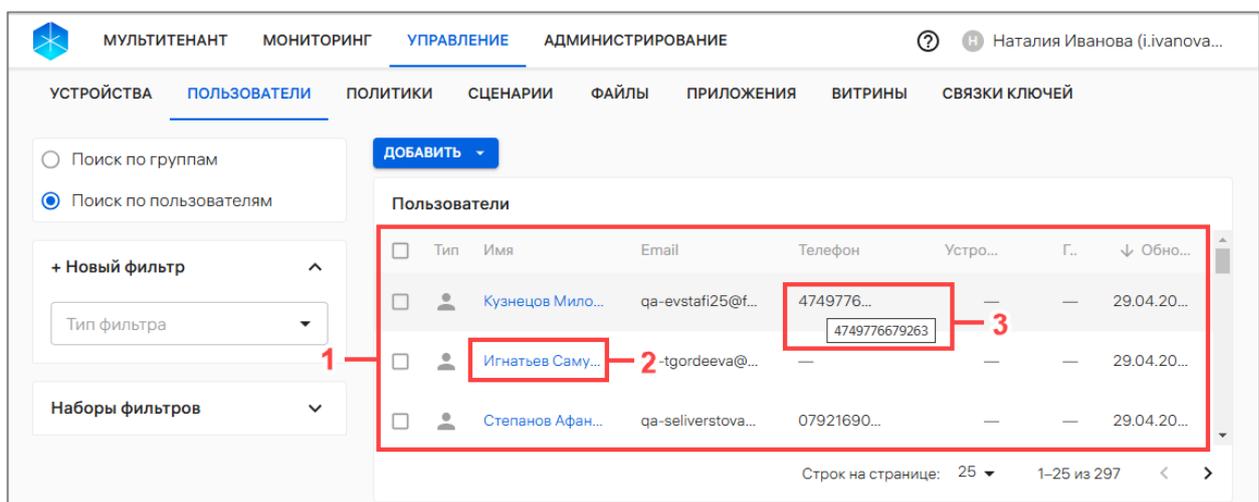


Рисунок 6

В таблице (Таблица 1) приведены возможные действия по каждому из подразделов раздела «Управление».

Таблица 1

Подраздел	Значок	Описание	Примечание
Устройства			
-		Привязать устройства к пользователям	пп. 2.2.7.1
-		Привязать устройства к группам	пп. 2.2.8.1
-		Активация устройств	пп. 2.2.9.2
-		Архивировать	пп. 2.2.12.1
Группы устройств			
ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам»		Активация устройств (активация помощью JSON-файла)	пп. 2.2.9.4
Пользователи			
-		Привязать пользователей к группам	пп. 2.3.4.1
-		Привязать устройства к пользователям	пп. 2.3.5.1
-		Архивировать пользователя	п. 2.3.7
Группы пользователей			
-		Привязать пользователей к группам	пп. 2.3.4.1
Сценарии			
-		Назначить офлайн-сценарии на группу пользователей	пп. 2.5.2.2
-		Назначить офлайн-сценарии на группу устройств	пп. 2.5.2.2
-		Удалить сценарий	п. 2.5.4
Файлы			
-		Удалить файл	п. 2.6.4

Для доступа к списку быстрых действий необходимо установить галочку в чекбоксе напротив выбранного элемента управления (Рисунок 7).

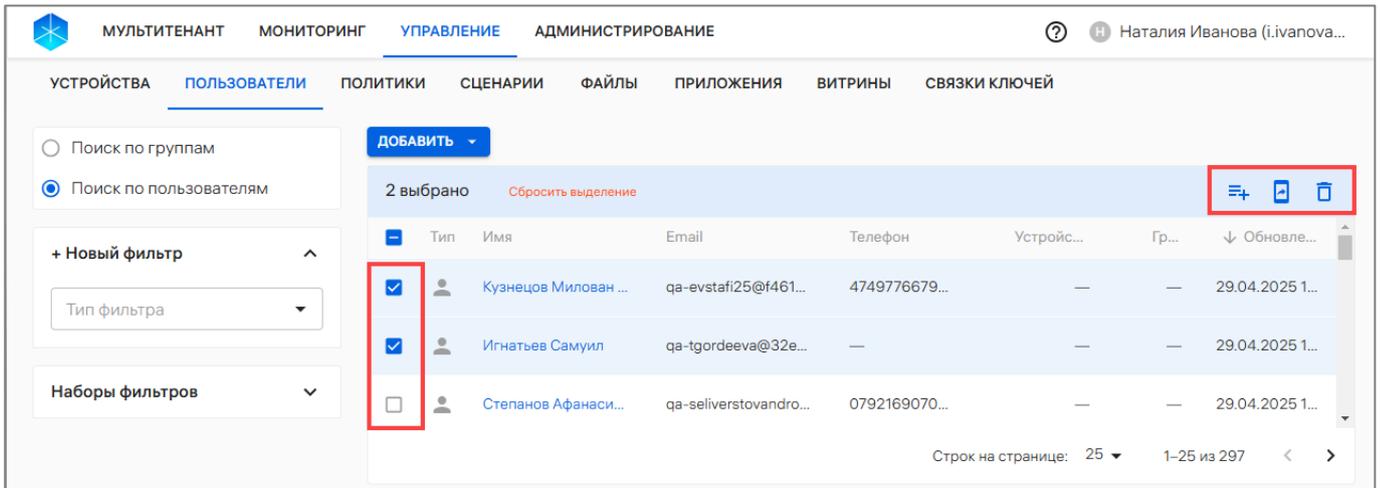


Рисунок 7

1.5. Работа с фильтрами

Область фильтров Консоли администратора ПУ позволяет выполнить поиск по критериям, доступным из раскрывающегося списка в следующих подразделах раздела «Управление»:

- «Устройства» – поиск устройств, групп устройств и событий безопасности устройств;
- «Пользователи» – поиск пользователей устройств, групп пользователей;
- «Политики» – поиск политик.

В таблице (Таблица 2) приведены фильтры для поиска информации в соответствующих разделах.

Таблица 2

Подраздел	Фильтры	Доступные значения
Поиск по устройствам		
Подраздел «Устройства» (поиск доступен также и внутри карточки группы устройств – предусмотрена возможность найти устройство, входящее в конкретную группу)	По идентификатору	Ввод значения с клавиатуры. Поиск по идентификатору устройства: – «По IMEI» – поиск по международному идентификатору устройства; – «По SN» – поиск по серийному номеру устройства; – «По Ethernet MAC» – поиск по MAC-адресу Ethernet устройства; – «По WLAN MAC» – поиск по MAC-адресу WLAN устройства. Например, «00:aa:00:00:a0:00»; – «По сетевому имени компьютера» – поиск по сетевому имени компьютера (hostname); – «По IP-адресу устройства» – поиск устройств по IP-адресу; – «Имя устройства» - поиск по имени устройства. ПРИМЕЧАНИЕ. Доступно применение нескольких идентификаторов поиска одновременно
	По UUID	Поиск по идентификатору устройства. Ввод значения с клавиатуры
	Жизненный цикл	Поиск по статусу жизненного цикла устройства. Выбор значения из списка: – «Зарегистрировано»; – «В процессе активации»; – «Активировано»; – «Не активировано»; – «Очищено»; – «Архивное»
	Клиент АЦ	Поиск устройства по статусу наличия приложения «Аврора Центр» на устройстве. Выбор значения из списка: – «Установлен»; – «Удален»; – «Неизвестно»

Подраздел	Фильтры	Доступные значения
	По соответствию политике	Поиск устройства по соответствию назначенным политикам. Выбор значения из списка: – «Соответствует»; – «Не соответствует»; – «Не управляется»
	По дате создания	Поиск по дате добавления устройства за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления устройства за выбранный период. Выбор значения из календаря
	По модели	Выбор модели устройства из списка
	По платформе	Выбор платформы: – «Аврора»; – «Android»; – «Linux»
	По группе	Поиск устройства по заданной группе. Ввод значения с клавиатуры
	По комментарию	Поиск устройства по комментарию. Ввод значения с клавиатуры
Поиск событий безопасности		
Подраздел «Устройства» → карточка устройства → вкладка «События безопасности»	По типу события	Поиск по типу события безопасности. Выбор значения из раскрывающегося списка: – «Информационное»; – «Отладочное»; – «Предупреждение»; – «Критическое»
	По имени события	Поиск по названию события безопасности. Выбор значения из списка
	По дате получения	Поиск по дате получения события безопасности за выбранный период. Выбор значения из календаря
	По дате возникновения	Поиск по дате возникновения события безопасности за выбранный период. Выбор значения из календаря
Поиск по группам устройств		
Подраздел «Устройства» →	По названию	Поиск группы устройств по названию. Ввод значения с клавиатуры

Подраздел	Фильтры	Доступные значения
«Поиск по группам»	По принципу добавления	<p>Поиск группы устройств по принципу добавления в группу.</p> <p>ПРИМЕЧАНИЕ. После применения фильтра в списке отображаются только динамические группы по выбранным критериям.</p> <p>Выбор значения из раскрывающегося списка:</p> <ul style="list-style-type: none"> – «Статус устройства» – поиск по статусу устройств. Выбор из списка: «Любое» или «Не задано»; – «Платформа устройства» – поиск по платформе устройств. Выбор из списка: «Любое» или «Не задано»; – «Объем жестких дисков» – поиск устройств по объему жестких дисков. Выбор из списка: «Любое» или «Не задано»; – «Количество процессорных ядер» – поиск устройств по количеству процессорных ядер. Выбор из списка: «Любое» или «Не задано»; – «Модель устройства» – поиск по модели устройств. Выбор из списка: «Любое» или «Не задано»; – «Тип устройства» – поиск по типу устройств. Выбор из списка: «Любое» или «Не задано»; – «Объем оперативной памяти» – поиск устройств по объему оперативной памяти. Выбор из списка: «Любое» или «Не задано»; – «Сетевое имя компьютера» – поиск устройств по сетевому имени компьютера. Выбор из списка: «Любое» или «Не задано»; – «Результат выполнения скрипта» – поиск устройств по результатам выполнения скрипта. Выбор из списка: «Любое» или «Не задано»; – «IP-адрес устройства» – поиск устройств по IP-адресу. Выбор из списка: «Любое» или «Не задано»;

АДМГ.20134-01 90 01-3

Подраздел	Фильтры	Доступные значения
		– «Производитель» – поиск устройств по названию производителя. Выбор из списка: «Любое» или «Не задано»
	По дате создания	Поиск по дате добавления группы устройств за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления группы устройств за выбранный период. Выбор значения из календаря
Поиск по пользователям		
Подраздел «Пользователи» → «Поиск по пользователям». (поиск доступен также и внутри карточки группы пользователей – предусмотрена возможность найти пользователя, входящего в конкретную группу)	По Email	Поиск по адресу рабочей почты пользователя
	По имени	Поиск по имени, фамилии, отчеству
	По фамилии	
	По отчеству	
	По дате создания	Поиск по дате добавления пользователя за выбранный период. Выбор значения из календаря
По дате обновления	Поиск по дате обновления пользователя за выбранный период. Выбор значения из календаря	
Поиск по группам пользователей		
Подраздел «Пользователи» → «Поиск по группам»	По названию	Поиск группы пользователей устройств по названию. Ввод значения с клавиатуры
	По типу группы	Поиск группы пользователей по типу группы: – «Группа пользователей»; – «Орг.подразделение»
	По принципу добавления	Поиск группы пользователей по принципу добавления в группу. Выбор значения из раскрывающегося списка: – «По дополнительным атрибутам пользователя LDAP»
	По дате создания	Поиск по дате добавления группы пользователей за выбранный период. Выбор значения из календаря

Подраздел	Фильтры	Доступные значения
	По дате обновления	Поиск по дате обновления группы пользователей за выбранный период. Выбор значения из календаря
Поиск политик		
Политики	По названию	Поиск по названию. Ввод значения с клавиатуры
	По дате создания	Поиск по дате добавления политики за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления политики за выбранный период. Выбор значения из календаря
	По правилу политики	Поиск по правилу, добавленному в политику. Выбор значения из списка (доступные значения приведены в таблице (Таблица 39))
Поиск защищенных переменных		
Подраздел «Настройки» → «Перейти на страницу переменных к подстановке для скриптов»	По названию	Поиск управляемой переменной по названию. Ввод значения с клавиатуры
	По защищенности	Поиск управляемой переменной по признаку защищенности. Выбор значения из раскрывающегося списка: – «Защищенная» - поиск защищенных переменных; – «Незащищенная» - поиск незащищенных переменных
	По блокировке	Поиск управляемой переменной по действию блокировки. Выбор значения из раскрывающегося списка: – «Действует» - поиск заблокированных переменных; – «Не действует» - поиск незаблокированных переменных

ВНИМАНИЕ! В данном пункте описаны общие принципы работы с фильтрами на примере подраздела «Пользователи».

Для поиска по заданным критериям требуется выполнить следующие действия:

- перейти в необходимый подраздел интерфейса ППО;
- выбрать из раскрывающегося списка «Тип фильтра» один из фильтров для поиска и задать параметры (Рисунок 8).

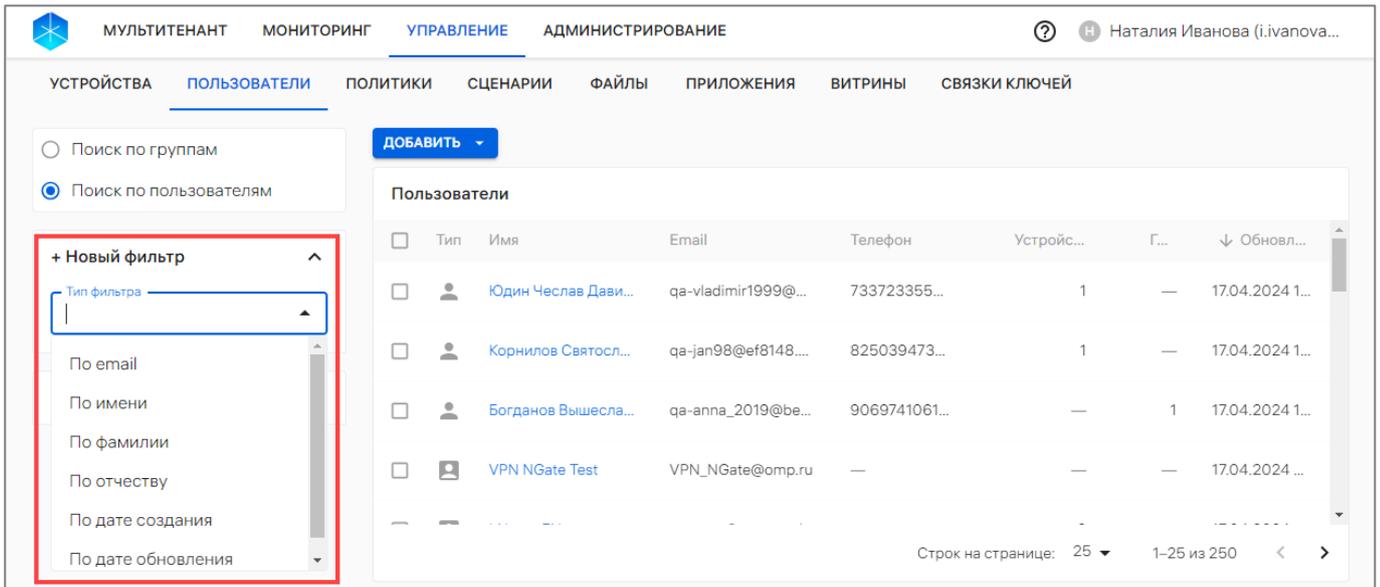


Рисунок 8

При вводе значения с клавиатуры (минимальная длина поискового запроса – 3 символа), а также выборе значения в календаре необходимо нажать соответствующую кнопку для применения фильтра, а при выборе значения из раскрывающегося списка фильтр будет применен автоматически.

Для формирования расширенного поиска по заданным критериям возможно задать несколько фильтров одновременно. В результате в рабочей области отобразится перечень элементов управления, сформированный на основании применения установленных фильтров. При необходимости для удаления фильтра следует нажать значок  (Рисунок 9 [1]). Для сброса всех выбранных фильтров необходимо нажать кнопку «Сбросить все» (Рисунок 9 [2]).

Также при необходимости примененные фильтры можно сохранить в набор фильтров, выполнив следующие действия:

- нажать кнопку «Сохранить» (Рисунок 9 [3]);

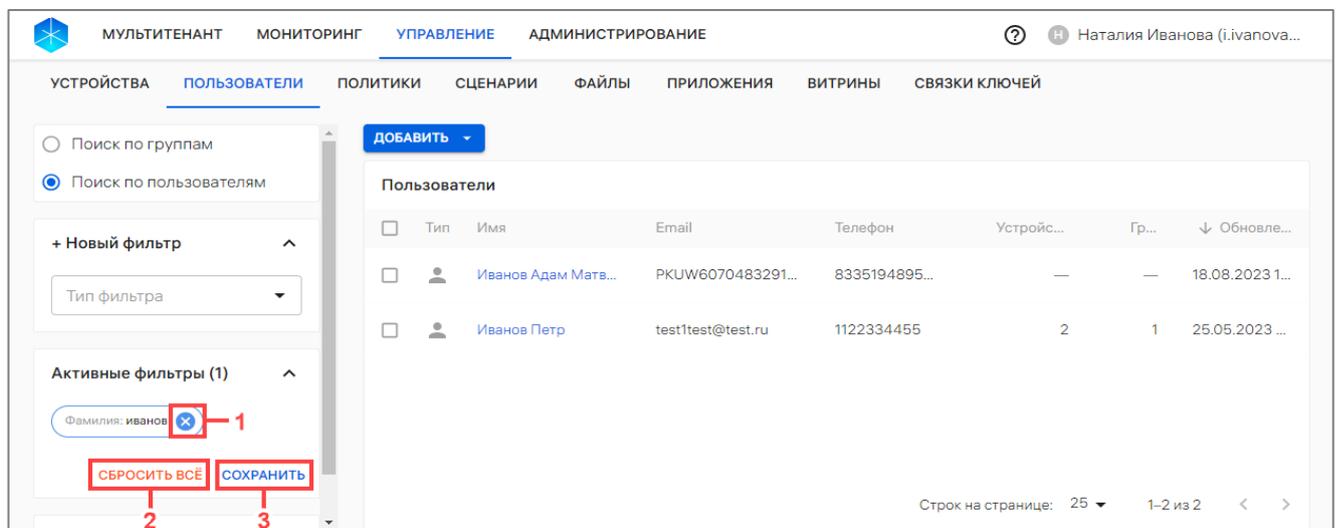


Рисунок 9

– в отобразившемся окне (Рисунок 10) ввести имя набора фильтров;

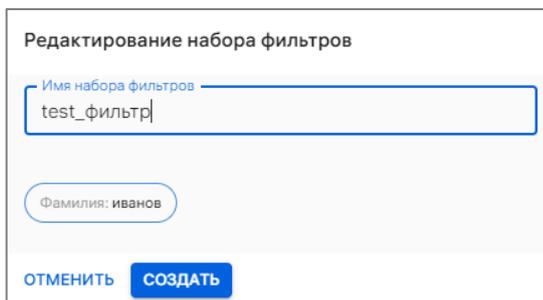
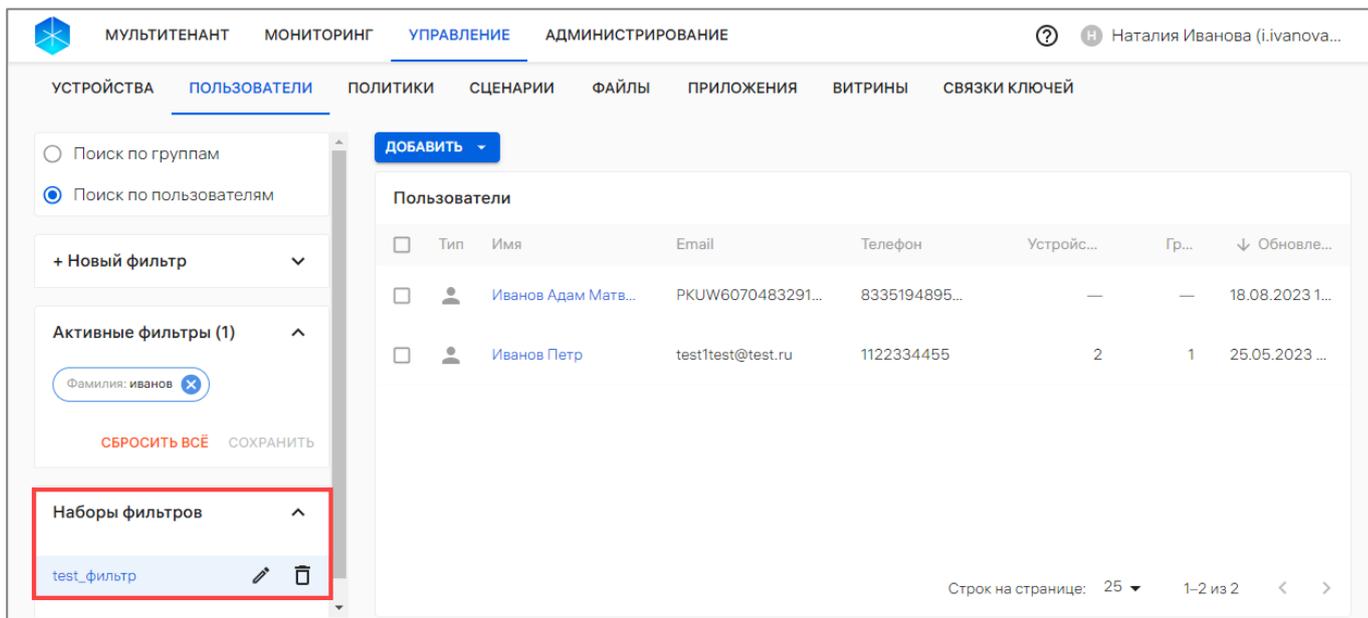


Рисунок 10

– нажать кнопку «Создать».

В результате выбранная комбинация фильтров будет сохранена в набор фильтров, который при необходимости возможно удалить нажатием значка  (Рисунок 11) или отредактировать его название нажатием значка .



<input type="checkbox"/>	Тип	Имя	Email	Телефон	Устройс...	Гр...	↓ Обновле...
<input type="checkbox"/>	Иванов Адам Матв...	PKUW6070483291...	8335194895...	—	—	18.08.2023 1...	
<input type="checkbox"/>	Иванов Петр	test1test@test.ru	1122334455	2	1	25.05.2023 ...	

Рисунок 11

ПРИМЕЧАНИЕ. При выходе из Консоли администратора ПУ и повторном входе под этой же учетной записью сохраненные фильтры будут доступны.

2. РАБОТА В РАЗДЕЛЕ «УПРАВЛЕНИЕ» КОНСОЛИ АДМИНИСТРАТОРА ПУ

2.1. Общее описание карточек элементов управления

2.1.1. Работа с карточкой устройства

С помощью карточки устройства возможно выполнить следующие действия:

- просмотр детальной информации об устройстве;
- активация устройств;
- отправка оперативной команды на устройство;
- привязка к пользователю/группе устройств;
- удаленное подключение к рабочему столу устройства;
- просмотр событий безопасности устройств;
- архивирование устройств.

Для просмотра карточки устройства необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- для отображения списка устройств в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства.

В результате откроется карточка устройства, интерфейс которой включает:

- общую информацию об устройстве (Рисунок 12 [1]), состоящую из параметров, приведенных в таблице (Таблица 3);

Таблица 3

Параметр	Описание
Модель	– название модели устройства; – тип устройства (Приложение 1)
ID	Идентификатор устройства, который можно скопировать, нажав значок 
IMEI	IMEI устройства, который можно скопировать, нажав значок 
IP-адреса	IP-адрес устройства, который можно скопировать, нажав значок 
Ethernet MAC	MAC-адрес Ethernet устройства, который можно скопировать, нажав значок 
SN	Серийный номер устройства, который можно скопировать, нажав значок 

Параметр	Описание
WLAN MAC	MAC-адрес WLAN устройства, который можно скопировать, нажав значок 
Сетевое имя	Сетевое имя компьютера, которое можно скопировать, нажав на значок 
Статус	Статус жизненного цикла устройства/соответствия политике
Клиент Аврора Центр	Версия приложения «Аврора Центр» подсистемы ППО, которое установлено на устройство. ПРИМЕЧАНИЕ. Если приложение «Аврора Центр» было удалено с устройства, то будет отображено сообщение «Клиент удален». Если устройство не активировано, то отображается «—»
Клиент Аврора Маркет	Версия приложения «Аврора Маркет» подсистемы ППО, которое установлено на устройство
Создано	Дата и время добавления устройства
Обновление	Дата и время внесения последних изменений в устройство (редактирование имени устройства, модели или комментария; привязка/отвязка к группам или пользователям; назначение/отвязка политики или офлайн-сценария на устройство)
Подключение	Дата и время последнего подключения устройства к ППО
Комментарий к устройству	Дополнительная информация об устройстве (заполняется при необходимости)

– оперативное управление (Рисунок 12 [4]), применение которого приведено в п. 2.2.10;

– вкладки карточки (Рисунок 12 [2]) с дополнительной информацией об устройстве:

- «Состояние» (пп. 2.1.1.1);
- «Управление» (пп. 2.1.1.2);
- «Пользователи» (пп. 2.1.1.3);
- «Группы» (пп. 2.1.1.4);
- «Политики» (пп. 2.1.1.5);
- «Сценарии» (пп. 2.1.1.6);
- «Удаленный доступ» (пп. 2.1.1.7);
- «События безопасности» (пп. 2.1.1.8);
- «Приложения» (пп. 2.1.1.9);
- «Карта» (пп. 2.1.1.10).

Для редактирования данных устройства необходимо нажать на значок  «Редактировать» (Рисунок 12 [3]) и внести необходимые изменения в следующие поля:

- «Имя устройства»;
- «Платформа»;
- «Модель устройства»;
- «Комментарий».

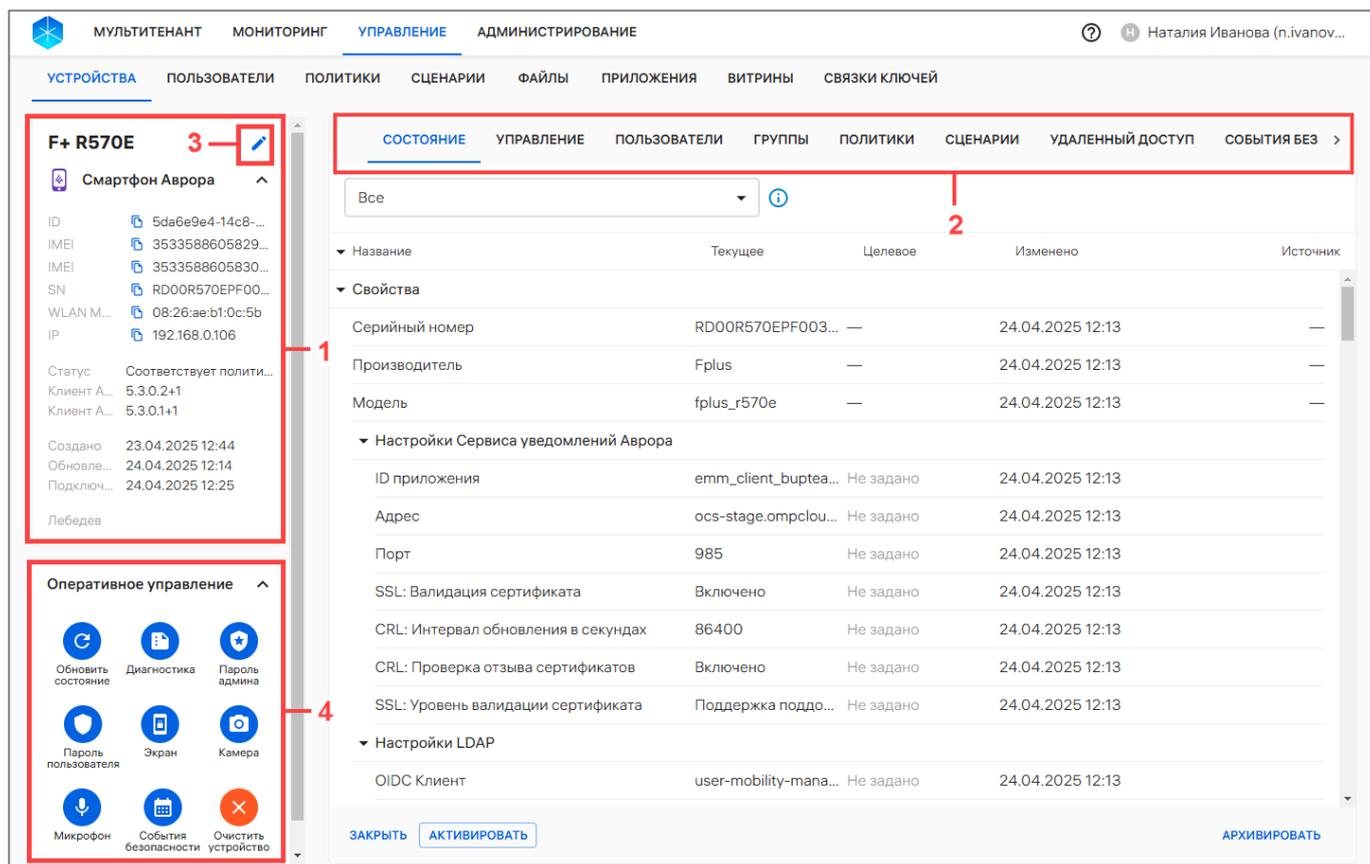


Рисунок 12

2.1.1.1. Вкладка «Состояние»

Во вкладке «Состояние» возможно выполнить следующие действия (Рисунок 13 [3]):

- активировать устройство, нажав кнопку «Активировать» (пп. 2.2.9.1);
- удалить устройство из списка устройств, нажав кнопку «Архивировать» (пп. 2.2.12.2);
- выйти из карточки устройства, нажав кнопку «Закрыть».

Также во вкладке «Состояние» предусмотрена возможность управлять отображением полей состояния по следующим параметрам (Рисунок 13 [1]):

- «Все» – отображаются все параметры;
- «Доступные для управления» – отображаются параметры, которые изменяются при назначении команд оперативного управления, политик и офлайн-сценариев (значение выставлено по умолчанию);

– «Под управлением» – отображаются параметры, измененные назначенными командами оперативного управления, политиками и офлайн-сценариями, которые находятся под управлением политики или оперативной команды.

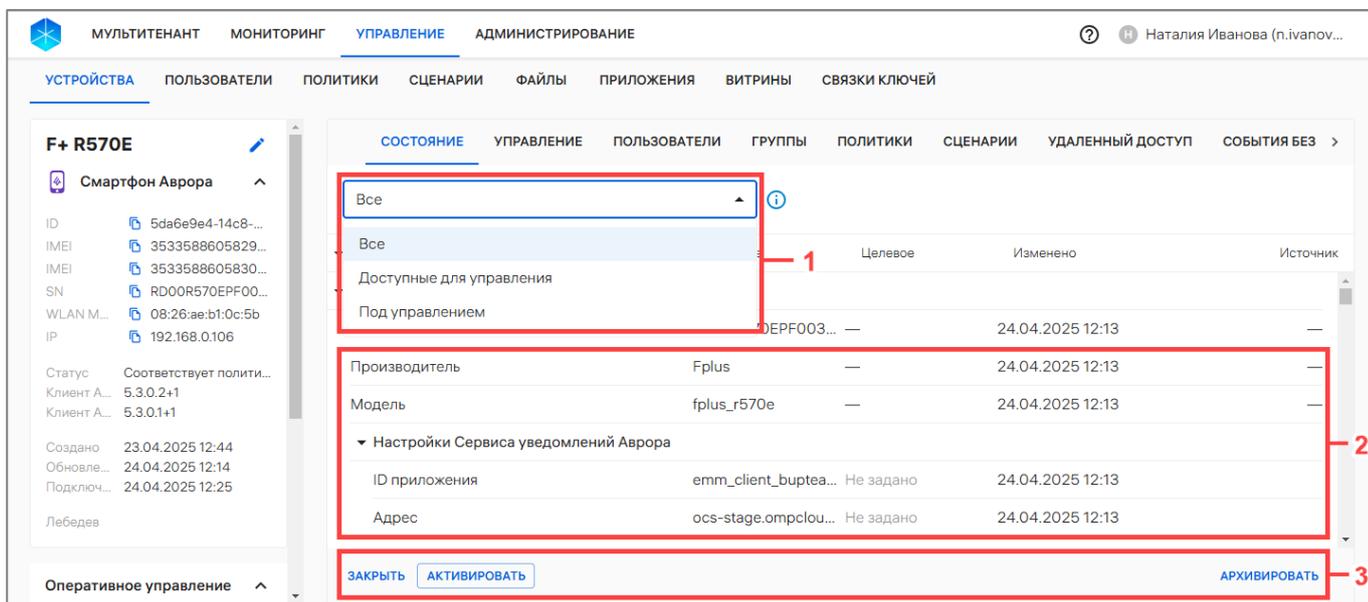


Рисунок 13

Для получения данных о состоянии активированного устройства в любом статусе необходимо создать и назначить на устройство политику отправки состояния или отправить оперативную команду «Обновить состояние». Подробное описание создания и назначения политики приведено в подразделе 2.4.

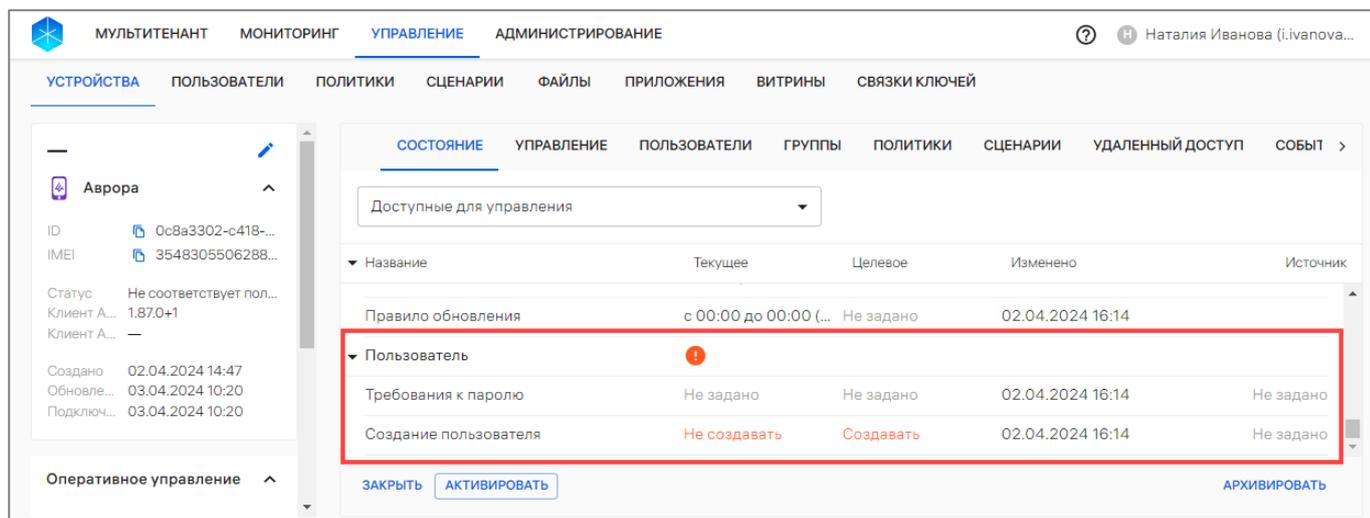
После получения данных о состоянии устройства отображается подробная информация о назначенных политиках и оперативных командах, а также параметры подключения к подсистеме Сервис уведомлений (ПСУ), входящей в состав ППО (если подключение к ПСУ зарегистрировано) в следующих столбцах (см. Рисунок 13 [2]):

- «Название» – название оперативных команд, группы политик или состояний;
- «Текущее» – последнее подтвержденное состояние устройства;
- «Целевое» – состояние, к которому устройство должно быть приведено;
- «Изменено» – дата и время изменения состояния устройства (например, после назначения (изменения) политики, офлайн-сценария или оперативной команды, перемещения устройства между группами и т.п.);
- «Источник» – источник целевого состояния (название политики, скомбинированная политика, оперативное управление).

ПРИМЕЧАНИЕ. При назначении на устройстве нескольких политик в столбце «Источник» отображаются все политики, из которых получена комбинированная политика. Например, если 3 политики назначены на устройство, при этом в 2 из них использование камеры запрещено, а в 1 – разрешено, то отобразятся политики с запретом использования камеры.

АДМГ.20134-01 90 01-3

Если политика или оперативная команда не были получены на устройство, то текущее состояние и целевое состояние устройства не будут совпадать. Несоответствия выделяются красным цветом, и отображается значок  (Рисунок 14).



The screenshot shows a management interface with a sidebar for device details and a main table for device states. The table has columns for Name, Current State, Target State, Changed, and Source. A red box highlights the 'Пользователь' row, where the current state is 'Не создавать' and the target state is 'Создавать', with a red exclamation mark icon in the current state column.

Название	Текущее	Целевое	Изменено	Источник
Правило обновления	с 00:00 до 00:00 (...)	Не задано	02.04.2024 16:14	
Пользователь	Не создавать 	Создавать	02.04.2024 16:14	
Требования к паролю	Не задано	Не задано	02.04.2024 16:14	Не задано
Создание пользователя	Не создавать	Создавать	02.04.2024 16:14	Не задано

Рисунок 14

Во вкладке «Состояние», в зависимости от версии ОС, возможно просмотреть и задать состояния на устройство, подробное описание которых приведено в таблице (Таблица 4).

ПРИМЕЧАНИЕ. Если значение целевого состояния устройства не отправлено, то в столбце «Текущее» будет отображаться «Не задано».

Таблица 4

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Свойства				
Серийный номер	Серийный номер, присвоенный устройству производителем. Может содержать от 1 до 20 символов	+	+	-
Производитель	Компания-производитель устройства	+	+	+
Модель	Модель устройства	+	+	+
Настройки Сервиса уведомлений Аврора				
ID приложения	Идентификатор приложения, с которым приложение «Аврора Центр» регистрируется в ПСУ	+	+	-
Адрес	Адрес Сервиса уведомлений Аврора для приложения «Аврора Центр»	+	+	-
Порт	Номер порта для подключения приложения «Аврора Центр»	+	+	-
SSL: Валидация сертификата	Включение или отключение валидации сертификата ПСУ. ПРИМЕЧАНИЕ. Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Включено»; – «Выключено» Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-
CRL: Интервал обновления в секундах	Временной интервал обновления списка отозванных сертификатов. ПРИМЕЧАНИЕ. Поле отображается, только если настройка была добавлена в конфигурационный файл ППО	+	+	-
CRL: Проверка отзыва сертификатов	Включение или отключение проверки наличия сертификата ПСУ среди списка отозванных сертификатов. ПРИМЕЧАНИЕ. Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Включено»; – «Выключено». Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-
SSL: Уровень валидации сертификата	Уровень валидации имени хоста, указанного в сертификате ПСУ. ПРИМЕЧАНИЕ. Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Не проверяется»; – «Поддержка поддоменов»; – «Точное совпадение». Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Настройки LDAP				
OIDC Клиент	Идентификатор клиента, необходимый для аутентификации в LDAP	+	+	-
Настройки проверки подключения к сети				
Адрес IPv4	Адрес IPv4 для проверки доступа к сети Интернет у устройства. ПРИМЕЧАНИЕ. Задается в конфигурационном файле ППО (/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml параметр networkCheckSettings.ipv4Url) и передается на устройство при его активации или подключении к серверу	+	-	-
Адрес IPv6	Адрес IPv6 для проверки доступа к сети Интернет у устройства. ПРИМЕЧАНИЕ. Задается в конфигурационном файле ППО (/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml параметр networkCheckSettings.ipv6Url) и передается на устройство при его активации или подключении к серверу	+	-	-
Настройки сервера времени				
Адреса	Список адресов серверов времени NTP. ПРИМЕЧАНИЕ. Задаются в конфигурационном файле ППО (/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml параметр timeServerSettings.hosts) и передается на устройство при его активации или подключении к серверу	+	-	-
Конфигурация				
Получение команд	Расписание на получение оперативных команд и заданных на устройствах политик и офлайн-сценариев. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	+	+
Отправка состояния	Расписание отправки состояния устройства на ПУ. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	+	+
Расписание отправки событий безопасности	Расписание отправки сообщений о событиях безопасности, произошедших на устройстве. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	-	-
Исключения событий безопасности	Уровень событий безопасности процесса, который не будут отправляться в Аврора Центр	+	-	-
Обновление координат в клиенте Аврора Центр	Частота обновления координат в приложении «Аврора Центр». Значение в формате «Каждые [чч] ч. [мм] м [сс] с»	+	+	-
Хранение логов на устройстве	Тип хранения системных сообщений на устройствах. Возможные значения: – «Временное»; – «Постоянное»	+	-	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Настройки правил политик (параметр отображается в ППО релиз 5.2.0 и выше)				
Запрет удаления приложений	Отображается одно из значений в текущем состоянии устройства в зависимости от выбранных настроек в разделе «Администрирование» → «Настройки» (п. 4.1.6). В целевом состоянии устройства отображается прочерк.	+	+	+
Запрет удаления файлов	Возможные значения: – «Действует»;	+	+	+
Запрет удаления скриптов	– «Не действует»	+	+	+
Создание точек восстановления				
Исключаемые директории	Директории, которые не попадут в точку восстановления	-	+	+
Интервал автоматического восстановления	Временной интервал. Если после применения политики, соответствующей режиму работы, связь с ППО оборвется более чем на указанный интервал, произойдет автоматический откат изменений на последнюю точку восстановления	-	+	+
Режим работы	Режим работы создания точек восстановления. Возможные значения: – «Всегда»; – «Только при применении правил, меняющих Файловую систему»	-	+	+
Статус	Статус создания точки восстановления. Например: «Создано»/«Не требуется»	-	+	+
Настройки прокси-сервера				
Хост	Хост прокси-сервера	-	-	+
Порт	Порт прокси-сервера	-	-	+
Имя пользователя	Имя пользователя для подключения через прокси-сервер	-	-	+
Хэш пароля	Хэш-сумма (sha256) пароля пользователя	-	-	+
Исключения из проксирования	Список хостов, которые будут исключены из проксирования	-	-	+
Таймаут экрана				
Таймаут	Время бездействия пользователя, после которого экран устройства блокируется	-	-	+
Корневые сертификаты (количество сертификатов)				
Название сертификата	В столбце «Текущее»/«Целевое» отображается цифровой отпечаток (Fingerprint) доверенного сертификата	+	+	-
Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат	+	+	-
Дата выпуска	Дата выпуска сертификата	+	+	-
Срок действия, до	Срок действия сертификата	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Система				
Блокировка экрана	Разблокировка или блокировка экрана устройства, а также, в случае блокировки, сообщение, которое будет отображено на экране. Возможные значения: – «Разблокировано»; – «Заблокировано»	+	+	+
Использование камеры	Разрешение или запрет на использование камеры. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Снимки экрана	Разрешение или запрет на создание снимков экрана. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Управление датой и временем	Разрешение или запрет на внесение изменений в настройки даты и времени. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Режим разработчика	Разрешение или запрет на использование режима разработчика. Возможные значения: – «Доступен»; – «Недоступен»	+	+	-
Сброс к заводским настройкам	Разрешение или запрет на сброс устройства к заводским настройкам. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Использование микрофона	Разрешение или запрет на использование микрофона. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Отправка и получение SMS	Разрешение или запрет на отправку и получение SMS. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Системные репозитории (сгруппированы по пронумерованным репозиториям)				
Параметры подключения	Информация о параметрах подключения к системному репозиторию	-	-	+
Безопасное подключение	Определяет, защищено ли подключение к системному репозиторию. Возможные значения: – «Да»; – «Нет»	-	-	+
Голосовые вызовы				
Исходящие вызовы	Разрешение или запрет выполнения исходящих звонков с устройства. Возможные значения: – «Разрешены»; – «Запрещены»	+	+	-
Входящие вызовы	Разрешение или запрет принятия входящих на устройства вызовов. Возможные значения: – «Разрешены»; – «Запрещены»	+	+	-
Параметры устройства				
Сетевое имя компьютера	Сетевое имя компьютера (hostname)	-	-	+
Тип устройства	Тип устройства – ПК/Ноутбук/Other	-	-	+
Серийный номер	Серийный номер, присвоенный устройству производителем. Может содержать от 1 до 20 символов	-	-	+
Объем жестких дисков	Общий объем жестких дисков на устройстве	-	-	+
Процессор				
Название	Название модели процессора	-	-	+
Частота	Частота процессора	-	-	+
Количество ядер	Количество ядер процессора	-	-	+
Звуковые устройства (список названий звуковых устройств ЭВМ)				
Название	Название звукового устройства ЭВМ	-	-	+
Мониторы, подключенные к устройству (сгруппированы по названиям мониторов)				
Интерфейс подключения	Информация о том, как подключен монитор к устройству	-	-	+
Размер матрицы	Размер матрицы монитора	-	-	+
Дата производства	Информация о дате производства монитора	-	-	+
Серийный номер	Серийный номер монитора	-	-	+
Память (список хранилищ устройств)				

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Диски				
Тип физического диска	Тип физического диска. Возможные значения: HDD, SSD	-	-	+
Интерфейс физического диска	Интерфейс диска. Возможные значения: SATA, NVME	-	-	+
Серийный номер диска	Серийный номер диска	-	-	+
Разделы (сгруппированы по названиям разделов). Разделы на физическом диске, доступные на устройстве				
Общий объем	Общий объем памяти раздела	+	+	+
Доступный объем	Доступный объем памяти раздела	+	+	+
Свободно	Свободный объем памяти раздела	+	+	+
Тип файловой системы	Тип файловой системы	-	-	+
Название раздела	Название партиции каталога	-	-	+
Название диска	Название диска, на котором присутствует этот каталог	-	-	+
ОЗУ (оперативная память устройства)				
Объем RAM	Объем оперативной памяти	-	-	+
Тип RAM	Тип оперативной памяти	-	-	+
Количество занятых слотов	Количество занятых слотов для оперативной памяти на устройстве	-	-	+
Количество свободных слотов	Количество свободных слотов для оперативной памяти на устройстве	-	-	+
Батарея (сгруппированы по элементам питания)				
Уровень заряда	Уровень заряда аккумулятора устройства	+	+	+
Заряжается	Заряжался ли аккумулятор устройства в момент отправки состояния. Возможные значения: – «Да»; – «Нет»	+	+	+
Износ батареи	Уровень износа элемента питания	+	+	+
Управление соединениями				
Управление авиарежимом	Разрешение или запрет на использование авиарежима. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Управление точкой доступа WLAN	Разрешение или запрет на изменение настроек мобильной точки доступа. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Использование браузера	Разрешение или запрет возможности использования браузера на устройстве. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Передача данных MTP	Разрешение или запрет возможности передачи данных по протоколу MTP. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Мобильная сеть				
Управление мобильной передачей данных	Разрешение или запрет на изменение настроек мобильной передачи данных	+	+	-
Точка доступа				
Имя	Имя точки доступа мобильной сети	+	+	-
APN	Хост точки доступа мобильной сети	+	+	-
MCC	Мобильный код страны	+	+	-
MNC	Код мобильной сети	+	+	-
Тип APN	По умолчанию значение «Интернет»	+	+	-
Тип аутентификации	По умолчанию значение «Нет»	+	+	-
Сетевые интерфейсы				
Название сетевого интерфейса				
Тип	Тип сетевого интерфейса	+	+	+
MAC	MAC-адрес сетевого интерфейса	+	+	+
IP-адрес	IP-адреса сетевого интерфейса	+	+	+
Метод получения IP	Информация о том, каким методом устройство получило IP-адрес	-	-	+
IP DHCP сервера	Информация об IP-адресе DHCP-сервера	-	-	+
DNS	Список IP-адресов, подключенных с помощью DNS	-	-	+
Шлюз	IP-адрес шлюз-сервера	-	-	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
WLAN				
Работа WLAN	Разрешение или запрет на использование сети WLAN. Возможные значения: – «Включен»; – «Выключен»	+	+	-
Управление WLAN	Разрешение или запрет изменения состояния адаптера сети WLAN. Возможные значения: – «Разрешено»; – «Запрещено»	+	+	-
Название WLAN	Название сети WLAN, к которой подключено устройство	+	+	-
MAC-адрес роутера	MAC-адрес роутера, к которому подключено устройство	+	+	-
Подключения (созданные на устройствах подключения к сети WLAN, которые группируются по названиям подключений)				
Название	Название беспроводной сети (Service Set Identifier) для подключения	+	+	-
Скрытая сеть	Определяет, транслируется ли название беспроводной сети. Возможные значения: – «Да»; – «Нет»	+	+	-
Автоподключение	Определяет, следует ли автоматически подключаться к беспроводной сети. Возможные значения: – «Да»; – «Нет»	+	+	-
Настройка IP-адреса	Способ настройки/получения IP-адреса. Возможные значения: «Автоматически»	+	+	-
Безопасность	Технология безопасности беспроводной сети. Возможные значения: – «WPA2»; – «WPA-EAP»	+	+	-
Протокол	Протокол защиты беспроводной сети. ПРИМЕЧАНИЕ. Отображается для сети с WPA-EAP. Возможные значения: «TLS»	+	+	-
Категория сертификата	Название категории, в рамках которой был выпущен пользовательский сертификат. ПРИМЕЧАНИЕ. Отображается для сети с WPA-EAP-TLS	+	+	-
Тип аутентификации	Тип аутентификации пользователя. ПРИМЕЧАНИЕ. Отображается для сети с WPA-EAP-PEAP	-	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Идентификатор	Идентификатор пользователя для подключения к беспроводной сети. ПРИМЕЧАНИЕ. Отображается для сети с WPA-EAP-TLS и WPA-EAP-PEAP с типом идентификации по шаблону	+	+	-
Логин	Логин пользователя для подключения к беспроводной сети. ПРИМЕЧАНИЕ. Отображается для сети с WPA-EAP-PEAP с типом идентификации по логину и паролю	-	+	-
Хэш пароля	Хэш-значение пароля беспроводной сети (для WPA2) или пользователя (для WPA-EAP-PEAP). ПРИМЕЧАНИЕ. Отображается для сети с WPA2 и WPA-EAP-PEAP)	-	+	-
VPN				
Подключения (подключения VPN, созданные на устройстве с помощью политики)				
Название (тип подключения)	Название подключения VPN. В скобках указывается тип подключения: – для устройств с ОС Аврора – КриптоПро NGate R2; – для устройств с ОС Android – Cisco AnyConnect/КриптоПро NGate R2	+	+	-
Адрес сервера	Адрес сервера VPN	+	+	-
Тип	Тип соединения VPN. Доступные значения: – КриптоПро NGate R2 – для ОС Аврора/ОС Android; – Cisco AnyConnect – для ОС Android	+	+	-
Протокол (доступно для типа Cisco AnyConnect)	Протокол безопасности соединения VPN. Доступен только один протокол безопасности – SSL	-	+	-
Категория сертификата (доступно для типа Cisco AnyConnect)	Название категории пользовательских сертификатов, в рамках которой выпущен сертификат для подключения VPN	-	+	-
Тип аутентификации (доступно для типа КриптоПро NGate R2)	Тип аутентификации пользователя. Доступен только 1 тип аутентификации – «По логину и паролю»	+	+	-
Логин (доступно для типа КриптоПро NGate R2)	Логин пользователя для подключения к VPN	+	+	-
Автозапуск VPN (доступно для типа КриптоПро NGate R2)	Переключатель для автоматического подключения устройства к VPN	+	+	-
Хэш серийного номера лицензии (доступно для типа КриптоПро NGate R2)	Хэш-значение серийного номера лицензии пользователя	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Bluetooth				
Управление Bluetooth	Разрешение или запрет на внесение изменений в настройки и подключение к новым устройствам Bluetooth®. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Работа Bluetooth	Разрешение или запрет возможности использования Bluetooth®. Возможные значения: – «Включен»; – «Выключен»	+	+	-
NFC				
Управление NFC	Разрешение или запрет на изменение настроек NFC	+	+	-
Геопозиция				
Режим работы	Режим работы геопозиционирования. Возможные значения: – «Не задано»; – «Выключено»; – «Пользовательские настройки»; – «Сохранение заряда аккумулятора»; – «Только спутники»; – «Высокая точность»	+	+	-
Изменение настроек	Разрешение или запрет на внесение изменений в настройки геопозиционирования. Возможные значения: – «Разрешено»; – «Запрещено»	+	+	-
Работа геопозиции (GPS модуль)	Разрешение или запрет возможности внесения изменений в настройки геопозиции. Возможные значения: – «Включена»; – «Выключена»	+	+	-
AGPS	Наличие и отсутствие AGPS-модуля на устройствах. Возможные значения: – «Доступен»; – «Недоступен»	+	+	-
Активность AGPS	Активность AGPS-модуля при его наличии на устройствах. Возможные значения: – «Включен»;	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
	– «Выключен»			
GPS-координаты	Географические координаты устройства (широта и долгота)	+	+	-
Время получения координат	Дата и время фиксации координат	+	+	-
SIM-карты				
Слот SIM1 (то же для Слот SIM2)				
IMEI	Уникальный номер SIM-карты	+	+	-
ICCID	Уникальный серийный номер SIM-карты	+	+	-
Активен	Активность SIM-карты. Возможные значения: – «Да»; – «Нет»	+	+	-
Защищена PIN-кодом	Защита SIM-карты PIN-кодом. Возможные значения: – «Да»; – «Нет»	+	+	-
Голосовые вызовы	Разрешение или запрет голосовых вызовов. Возможные значения: – «Разрешена(ны)»; – «Запрещена(ны)»	+	+	-
Мобильная передача данных	Разрешение или запрет на мобильную передачу данных. Возможные значения: – «Разрешена»; – «Запрещена»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Внешние накопители				
Использование USB-накопителей	Разрешение или запрет использования USB-накопителей. Возможные значения: – «Разрешено»; – «Запрещено»	+	-	+
Использование SD-карт	Разрешение или запрет использования SD-карт. Возможные значения: – «Разрешено»; – «Запрещено»	+	-	-
Управление приложениями				
Установка приложений	Разрешение или запрет установки приложения на устройства. Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»	+	+	-
Установленные приложения (сгруппированы по названиям приложения)				
Статус	Статус установки приложения. Возможные значения: – «Установлено»; – «Ошибка скачивания приложения»; – «Ошибка установки приложения»; – «Неправильный хэш»; – «Тип приложения не поддерживается»	+	+	+
Витрина	Название витрины приложения. В разделе текущего состояния отображается название витрины установленного приложения на устройстве. В разделе целевого состояния отображается название витрины приложения, указанного в политике, назначенной на устройствах	+	+	+
Наименование	Наименование приложения. В разделе текущего состояния отображается наименование установленного приложения на устройстве. В разделе целевого состояния отображается название приложения, указанного в политике, назначенной на устройствах	+	+	+
Версия	Версия приложения. В разделе текущего состояния отображается версия установленного приложения на устройстве. В разделе целевого состояния отображается версия приложения, указанного в политике, назначенной на устройствах	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Автозапуск	Определяет включение автозапуска приложения. Возможные значения: – «Не задано»; – «Да»; – «Нет»	+	+	+
Время установки	Время установки приложения на устройство. Возможные значения: – «Моментально»; – интервал установки приложения на устройство (пример: с 14:00 до 15:00)	+	+	+
Принудительное создание ярлыка	Статус создания ярлыка приложения (вынесение desktop-файлов устанавливаемого приложения на рабочий стол). Возможные значения: – «Не задано»; – «Создан»; – «Не создан»	+	-	-
Запрещенные приложения (сгруппированы по запрещенным пакетам)				
Название пакета	Название запрещенного пакета	+	+	+
Диапазон версий N	Диапазон запрещенных версий приложения (может быть несколько, N - номер диапазона). Если диапазон версий не был включен и задан при создании и назначении политики на группу устройств, то этот параметр не отображается	+	+	+
Статус	Статус присутствия приложения на устройстве. Возможные значения: – «Отсутствует на устройстве»; – «Присутствует на устройстве»	+	+	+
Управление файлами				
Файлы (сгруппированы по названиям файлов)				
Версия	Номер версии файла	-	+	+
Директория	Директория на устройстве, в которую должен быть помещен файл	-	+	+
Размер	Размер файла	-	+	+
Комментарий	Комментарий к файлу	-	+	+
Хэш файла (SHA-256)	Хэш содержимого файла	-	+	+
Файлы с устройства				
Загружаемые файлы с устройства (сгруппированы по пути к папке с файлами на устройстве)				
Директория	Папка на устройстве для отправки из нее файлов на сервер	-	+	+
Проверять	Интервал проверки содержимого папки на наличие новых файлов	-	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Удалять на устройстве после отправки	Определяет, удалять ли файлы из папки устройства после загрузки на сервер приложения. Возможные значения: – «Не задан»; – «Да»; – «Нет»	-	+	+
Статус	Статус отправки файлов. Возможные значения: – «Загружена»; – «Выполняется»; – «Ошибка загрузки»	-	+	+
Сообщение	Сообщение с текстом ошибки при статусе «Ошибка загрузки»	-	+	+
Дата последней проверки файлов	Дата и время последней проверки файлов в папке	-	+	+
Управление скриптами				
Скрипты (сгруппированы по пути к файлам со скриптами)				
Таймаут	Таймаут выполнения скрипта. Формат: [мм:сс]	-	+	+
Статус	Статус выполнения скрипта. Возможные значения: – «Успешно выполнено»; – «Не выполнен по таймауту»; – «Не выполнен»; – «Не запущен»; – «Выполнен: код <код из ответа>»	-	+	+
Результат выполнения скрипта	Результат выполнения скрипта. Передается если в файл скрипта была добавлена переменная скрипт OMP_SCRIPT_RESULT_FILE. Подробнее в приложении (Приложение 3)	-	+	+
Последнее успешное выполнение	Дата и время последнего успешного выполнения скрипта. Формат: [дд].[мм].[гг] [чч]:[мм]	-	+	+
Дистрибутив ОС				
ОС	Название ОС	+	+	+
Версия ОС	Номер версии ОС	+	+	+
Вариант ОС	Название варианта ОС	+	+	+
Пакеты доступные для обновления	Количество пакетов, которые можно обновить	-	-	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Версия ядра доступная для обновления	Имя нового ядра, до которого можно обновиться	-	-	+
Дата обнаружения обновлений ОС	Дата и время, когда было обнаружено, что согласно политике обновления ОС устройство имеет возможность выполнить обновления (либо обновление пакетов, либо обновление ядра, либо двух – как задано в политике)	+	+	+
Планируемая дата обновления ОС	Дата и время планового обновления, которые были рассчитаны на устройстве в момент обнаружения возможных обновлений	+	+	+
Правило обновления	Временной период установки обновлений ОС. В скобках указана версия ОС	+	+	+
Дата установки	Дата установки дистрибутива ОС	-	-	+
Статус обновления	Статус установки обновлений ОС. Возможные значения: – «Нет данных»; – «Выполнено»; – «Не выполнено»; – «Запланировано»	-	-	+
Обслуживание ОС				
Обновить пакеты	Определяет, требуется ли обновить пакеты ОС	-	-	+
Обновить ядро	Определяет, требуется ли обновить ядро ОС (и его модули)	-	-	+
Остановить обновления ядра, если хотя бы 1 модуль удаляется	Определяет, требуется ли остановить обновления ядра, если хотя бы 1 его модуль будет удален в процессе обновления	-	-	+
Удаление ранее скачанных пакетов	Определяет, требуется ли удалить ранее скачанные пакеты после успешного обновления ОС	-	-	+
Удаление неиспользуемых пакетов	Определяет, требуется ли удалить неиспользуемые пакеты после успешного обновления ОС	-	-	+
Удаление дубликатов пакетов	Определяет, требуется ли удалить дубликаты пакетов после успешного обновления ОС	-	-	+
Удаление старых ядер	Определяет, требуется ли удалить старые ядра после успешного обновления ОС	-	-	+
Перезагрузка ОС	Определяет, требуется ли выполнить перезагрузку ОС после успешного обновления	-	-	+
Последняя попытка обновления				
Дата обновления	Дата и время последней попытки обновления ОС	-	-	+
Результат обновления	Результат последней попытки обновления. Возможные значения: – «Успешно»; – «Неуспешно»	-	-	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Детали обновления	Отчет об обновлении ОС в виде списка деталей (этапов). Для каждой детали (этапа) отображается: – «Этап» - название стадии обновления (packageUpdate, kernelUpdate и т.п.); – «Сообщение» - тело сообщения (произвольный текст)	-	-	+
Тип сообщения	Важность сообщения. Возможные значения: – «Информационное»; – «Ошибка»; – «Предупреждение»	-	-	+
Пользователь				
Требования к паролю	Информация о требованиях к следующим параметрам пароля: – сложность; – длина; – срок истечения. Возможные значения: – обычный: сложность – обычная (цифры), длина – от 7 до 10 символов; – сложный: сложность – высокая (цифры, буквы, символы, знаки пунктуации), длина – от 8 до 12 символов; – срок истечения пароля: 30, 60, 90, 120, 150, 180 дней (не зависит от сложности пароля)	+	+	+
Создание пользователя	Требование создания пользователя на устройствах. Возможные значения: – «Создавать»; – «Не создавать»	+	-	+
Пользовательские сессии				
Сессии пользовательских входов на устройстве	В текущем состоянии выводится ТОП-3 по наибольшему времени сессии пользователей, авторизованных на устройстве. Отображается логин и время сессии в минутах	-	-	+
Сертификаты пользователей				
Сертификат (информация о сертификатах пользователя, которые были выпущены и доставлены на устройства)				
Категория	Название категории, в рамках которой был выпущен пользовательский сертификат	+	+	-
Шаблон	Название шаблона для выпуска пользовательских сертификатов	+	+	-
Фингерпринт	Цифровой отпечаток (Fingerprint) сертификата	+	+	-
Хэш-алгоритм запроса	Алгоритм хэширования	+	+	-
Тип шифрования и длина ключа	Алгоритм шифрования приватного ключа	+	+	-
Subject	Список субъектов для сертификата. Каждый субъект состоит из набора параметров – название параметра (key) и его значения (value)	+	+	-
Расширение	Дополнительные имена субъекта для сертификата. Отображается, если параметр «Subject Alt Name» указан в категории пользовательских сертификатов	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Режим киоска				
Включен	Определяет, включен ли режим киоска	-	+	-
Отключение панели управлений	Определяет, отключено ли отображение панели уведомлений (верхнее меню) в режиме киоска	-	+	-
Код выхода из режима киоска	Код для выхода из режима киоска на устройстве	-	+	-
Цвет шрифта	Настройка цвета шрифта. Возможные значения: – «По умолчанию»; – заданный цвет и HEX-код цвета в формате "#ffffff"	-	+	-
Фон	Настройка цвета фона. Возможные значения: – «Системное изображение»; – заданный цвет и HEX-код в формате "#ffffff"	-	+	-
Приложения				
Код приложения [№]	Названия пакетов приложений, которые будут доступны пользователю в режиме киоска	-	+	-
Ярлыки веб-страниц				
Название ярлыка	Название ярлыка веб-страницы	-	+	-
URL	Электронный адрес сайта/веб-страницы в формате URL	-	+	-
Запрещенные сайты	Электронные адреса запрещенных сайтов. Если отображается значение в виде звездочки (*), то запрещены все сайты, кроме указанных в исключениях	-	+	-
Исключения из запрещенных сайтов	Электронные адреса сайтов, которые исключены из запрещенных	-	+	-
Внешний вид				
Фон рабочего стола (информация об установленном фоне на рабочий стол устройства)				
Путь к файлу	Абсолютный путь к файлу изображения на устройстве	-	+	-
Отображение идентификаторов в клиенте Аврора Центр	Отображаются идентификаторы устройства в порядке, заданном в политике	+	+	+

2.1.1.2. Вкладка «Управление»

Во вкладке «Управление» отображается:

– перечень правил политик, офлайн-сценариев и оперативных команд, назначенных на устройство (доступные значения необходимо выбрать из раскрывающегося списка (Рисунок 15 [1]);

– информация о соответствии назначенных правил (в случае конфликта отображается действующее правило (Рисунок 15 [2])).

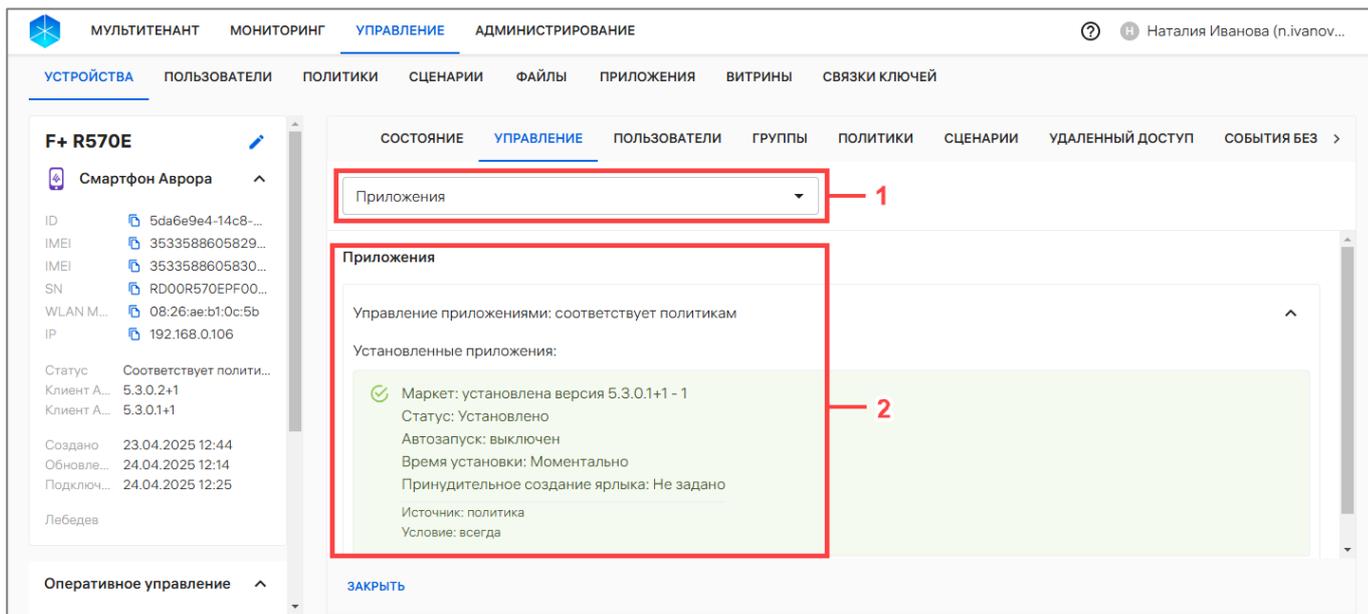


Рисунок 15

ПРИМЕЧАНИЕ. Одновременно назначенные на устройство правила имеют следующий приоритет:

- 1) Оперативная команда;
- 2) Офлайн-сценарий;
- 3) Политика.

2.1.1.3. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список привязанных к устройству пользователей (Рисунок 16 [1]), а при его отсутствии отображается сообщение «Устройство не привязано ни к одному пользователю».

Устройство можно привязать к пользователю из карточки с помощью кнопки «Привязать пользователей» (Рисунок 16 [2]), выполнив действия, приведенные в пп. 2.2.7.2.

Список пользователей сортируется по дате обновления информации о пользователях устройства.

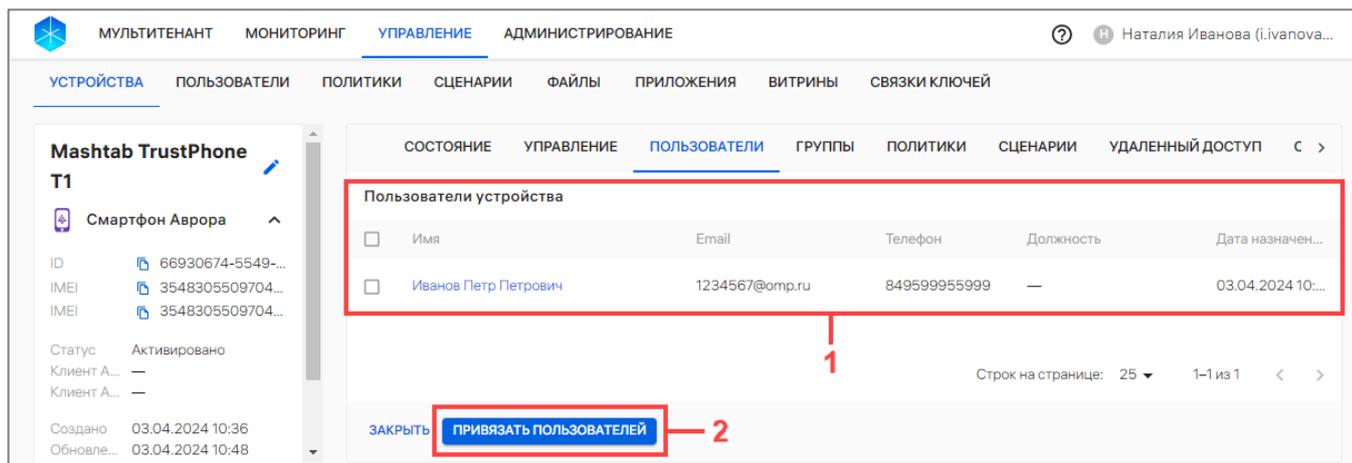


Рисунок 16

Информация о пользователях отображается в столбцах, приведенных в таблице (Таблица 5).

Таблица 5

Параметр	Описание
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке пользователя (п. 2.1.3))
Email	Рабочая почта пользователя
Телефон	Номер телефона пользователя
Должность	Должность занимаемая пользователем
Дата назначения	Дата и время привязки устройства к пользователю

2.1.1.4. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к устройству групп устройств (Рисунок 17 [1]).

Устройства можно привязать к группе устройств с помощью кнопки «Добавить в группы» (Рисунок 17 [2]), выполнив действия, приведенные в пп. 2.2.8.2.

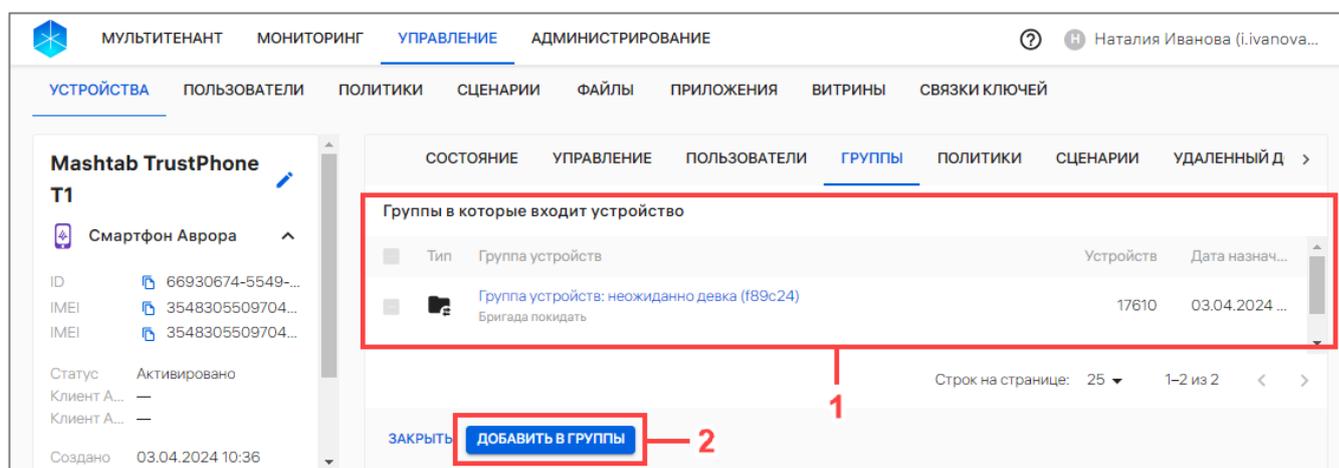


Рисунок 17

Информация о группах устройств отображается в столбцах, приведенных в таблице (Таблица 6).

Таблица 6

Параметр	Описание
Тип	Тип группы устройств (Приложение 1)
Группа устройств	– название группы устройств (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы устройств (п. 2.1.2); – комментарий – дополнительная информация (заполняется при необходимости)
Устройств	Количество устройств в данной группе устройств
Дата назначения	Дата и время добавления устройств в группу устройств

2.1.1.5. Вкладка «Политики»

Во вкладке «Политики» отображается список назначенных на устройство политик и их правил (Рисунок 18), а при отсутствии списка отображается сообщение «На устройство не назначено ни одной политики».

В случае пересечения с другими политиками отобразится полный список названий всех политик на группах устройств или группах пользователей.

Информация во вкладке «Политики» отображается в следующих столбцах:

– «Название» – название политики, назначенной на группу устройств/пользователей, в которую входит текущее устройство. Название политики выделено цветом и представляет собой активную ссылку (Рисунок 18 [1]), при нажатии на которую осуществляется переход к карточке политики;

– «Содержимое» – краткая информация о правилах, добавленных в политику;

– «Группа» – наименование группы, на которую назначена политика. Название группы представляет собой активную ссылку (Рисунок 18 [2]), при нажатии на которую осуществляется переход к карточке группы.

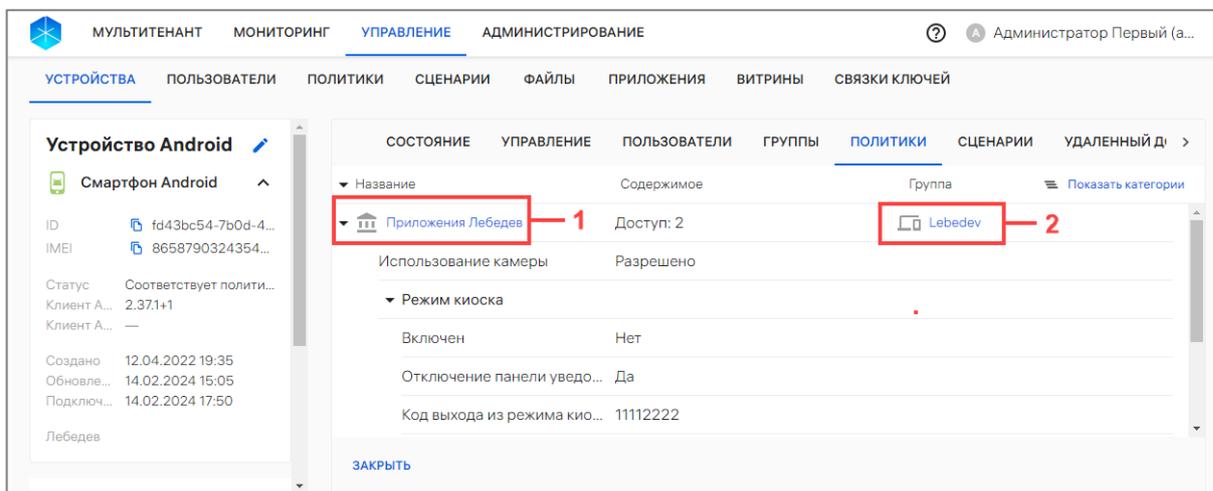


Рисунок 18

При отсутствии политик, назначенных на группу устройств/пользователей, в которую входит данное устройство, необходимо выполнить действия, приведенные в п. 2.4.4.

2.1.1.6. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается следующий список:

- офлайн-сценарии, назначенные на устройство (Рисунок 19 [1]);
- бизнес-сценарии, выполняющиеся на устройстве (Рисунок 19 [2]).

В ППО доступен бизнес-сценарий по экстренному выводу устройства из эксплуатации (например, при утере или краже), при применении которого, устройство блокируется, затем очищается вместе со всеми данными (сбрасывается до заводских настроек (п. 2.2.15) и архивируется).

При отсутствии офлайн-сценариев, назначенных на группу устройств/пользователей, в которую входит данное устройство, отображается сообщение «На устройство не назначен ни один офлайн-сценарий». Подробное описание назначения офлайн-сценариев приведено в п. 2.5.2.

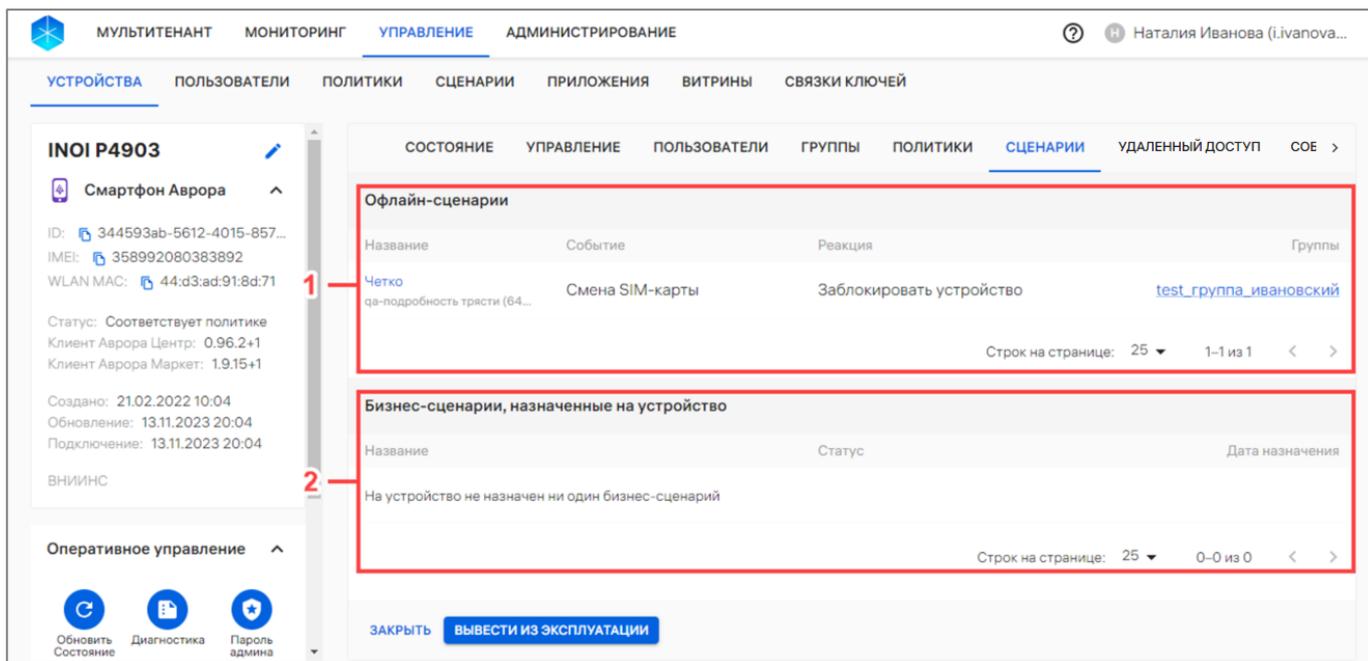


Рисунок 19

Информация об офлайн-сценариях и о бизнес-сценариях отображается в столбцах, приведенных в таблице (Таблица 7).

Таблица 7

Параметр	Описание
Офлайн-сценарии	
Название	Название офлайн-сценария, назначенного на группу устройств/пользователей, в которую входит текущее устройство. Название офлайн-сценария представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке офлайн-сценария
Событие	Событие, по которому офлайн-сценарий должен сработать
Реакция	Реакция устройства, которая должна произойти при наступлении события офлайн-сценария
Группы	Наименование группы, на которую назначен офлайн-сценарий. Название группы представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы
Бизнес-сценарии, назначенные на устройства	
Название	Название бизнес-сценария, выполняющегося на устройстве
Статус	Статус выполнения бизнес-сценария
Дата назначения	Дата и время назначения бизнес-сценария на устройства

2.1.1.7. Вкладка «Удаленный доступ»

Во вкладке «Удаленный доступ» отображаются настройки RustDesk для удаленного подключения.

ВНИМАНИЕ! Данный функционал доступен только для устройств, функционирующих на ОС Android и ОС Альт Linux.

ПРИМЕЧАНИЕ. Для успешной работы удаленного доступа через ППО необходимо, чтобы был развернут и зафиксирован в конфигурационном файле ПУ сервер RustDesk. Подробная информация приведена в документе «Руководство администратора» АДМГ.20134-01 91 01.

Для удаленного подключения к рабочему столу активированного устройства, а также для обмена файлами с помощью ПУ, необходимо выполнить следующие действия:

1) Установить desktop-клиент RustDesk на ЭВМ.

ПРИМЕЧАНИЕ. В зависимости от версии ОС дистрибутив desktop-клиента расположен в следующей папке распакованного архива с дистрибутивом ППО:

- ОС Windows версии 11: /client-apps-android/thirdparty/rustdesk-fa/windows/;
- ОС Ubuntu 20.04: /client-apps-android/thirdparty/rustdesk-fa/ubuntu-20.04/;
- ОС Ubuntu 22.04: /client-apps-android/thirdparty/rustdesk-fa/ubuntu-22.04/.

ВНИМАНИЕ! Корректная работа desktop-клиента RustDesk на других версиях ОС не гарантируется;

2) Открыть настройки desktop-клиента RustDesk. Для этого необходимо открыть настройки desktop-клиента RustDesk (Рисунок 20), перейти в раздел «Сеть» и указать адрес и ключ сервера RustDesk, которые были получены на шаге 1.

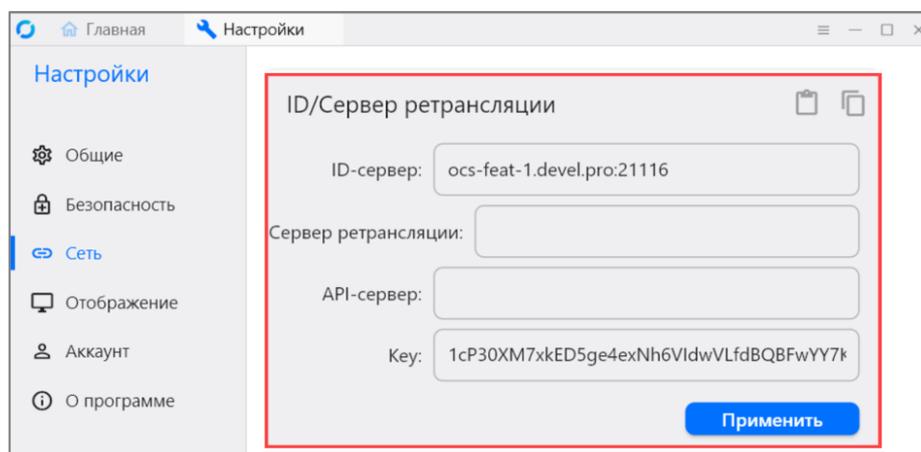


Рисунок 20

ПРИМЕЧАНИЕ. Для desktop-клиента RustDesk для ОС Windows необходимо также нажать кнопку «Установить» (Рисунок 21) на главной странице и следовать инструкциям из Wizard для установки RustDesk в системе;

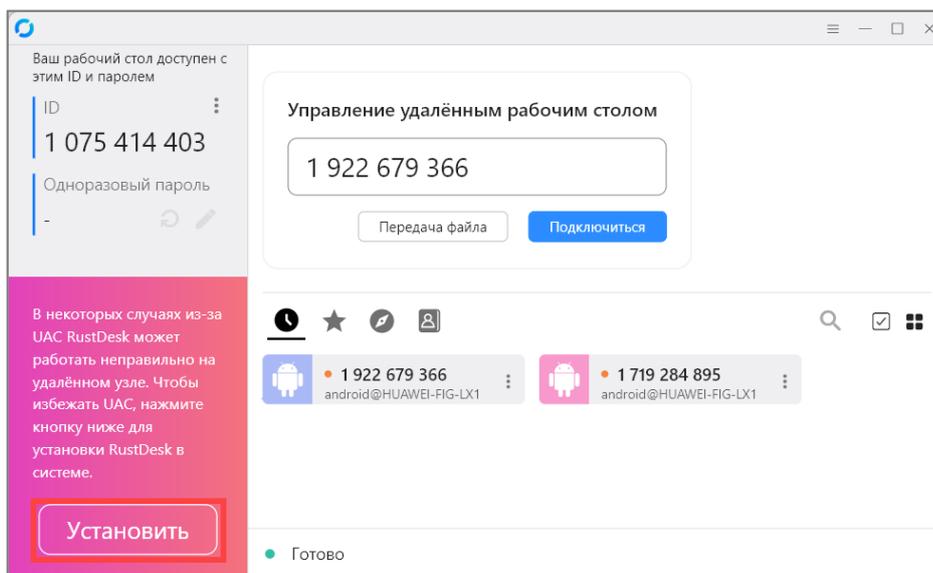


Рисунок 21

3) Установить приложение RustDesk на устройствах пользователя.

ВНИМАНИЕ! В зависимости от ОС, установленной на устройстве, дистрибутив приложения расположен в папке распакованного архива с ППО, а именно:

– **ОС Android версии 7 и выше:** /client-apps-android/thirdparty/rustdesk/android/ (подготовка устройства к удаленному подключению приведена в приложении (Приложение 4).

Может быть доступна сборка приложения RustDesk, подписанная подписью производителя. Такая сборка позволяет осуществлять удаленное подключение к рабочему столу пользователя без запроса у пользователя отдельного разрешения (далее «бесшовное» подключение), при этом для нее характерно следующее:

- сборка располагается в архиве `client-apps-android-signed-vendor.tar.gz`, который входит в комплект поставки ППО;

- суффикс в названии APK-файла определяет производитель.

Особенности, характерные для производителя Chainway:

- приложение RustDesk располагается в папке: `/client-apps-android/thirdparty/rustdesk/android/rustdesk-1.5.1+1-android.armeabi-v7a.chainway-4d.apk`;

- используемые подписи зависят от модели устройства, например:

- для устройств на Qualcomm – подпись с суффиксом `4d`;

- для устройства C72 – подпись с суффиксом `cd`.

- **ОС Альт Linux версии p10:** `/client-apps-linux/thirdparty/alt-p10`.

ВНИМАНИЕ! Рекомендуется установить приложение RustDesk, назначив политику «Приложения/Установка приложений на устройство» (пп. 2.4.1.42);

Для установки приложения RustDesk с «бесшовным» подключением необходимо создать динамическую группу устройств по производителю (пп. 2.2.2.2) и затем назначить политику с правилом «Приложения/Установка приложений на устройство», которая установит необходимое приложение в зависимости от производителя.

ПРИМЕЧАНИЕ. Если приложение RustDesk (из состава ППО релиз 5.0.0) версии 5.0.0.1+1 загружен в ПМ, то подгрузить к нему для обновления версию 1.5.1+1 и выше (ППО релиз 5.2.0) невозможно.

В этом случае необходимо создать новое приложение RustDesk под релиз 5.2.0 и затем переназначить его установку на устройства с использованием соответствующей политики;

4) Передать настройки на устройство и выполнить удаленное подключение через ПУ. Для этого в Консоли администратора ПУ в карточке устройства во вкладке «Удаленный доступ» нажать на кнопку «Конфигурировать сеанс» (Рисунок 22), предварительно убедившись, что настройки сервера RustDesk заданы в настройках сети desktop-клиента RustDesk (см. Рисунок 20).

В результате настройки удаленного подключения будут переданы и применены на устройстве (это может занять некоторое время).

ПРИМЕЧАНИЯ:

- ✓ Поставляемое в дистрибутиве ППО приложение RustDesk для администратора в целях безопасности не поддерживает подключение к нему и может быть использовано только для подключения к управляемым устройствам;

✓ Если требуется удаленно подключаться к рабочему столу устройства в режиме киоска, то приложение RustDesk не нужно включать в список разрешенных приложений. В режиме киоска оно будет по умолчанию скрыто на экране устройства, при этом будет возможность удаленно подключиться к рабочему столу, выполнив шаги, приведенные выше.

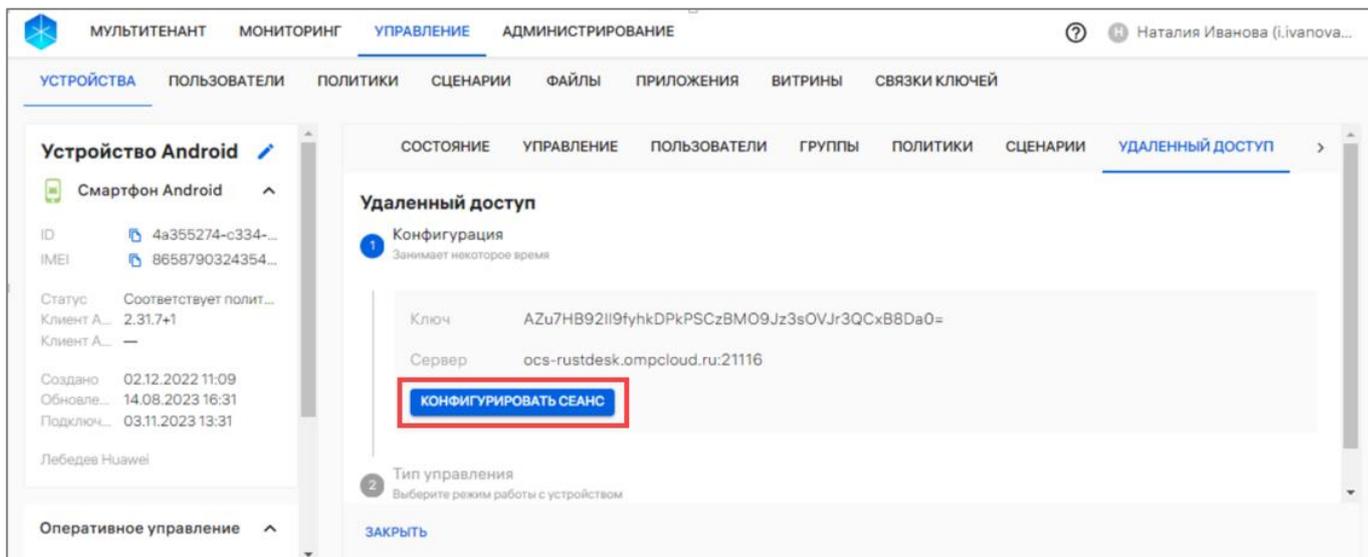


Рисунок 22

Далее отобразится «Тип управления», в котором будут отображены (Рисунок 23 [1]):

- «ID клиента» – идентификатор клиента RustDesk на устройстве пользователя;
- «Пароль» – пароль для удаленного подключения.

ПРИМЕЧАНИЕ. Для устройств, функционирующих на ОС Android, перед выполнением удаленного подключения необходимо на устройствах вручную запустить службу RustDesk и выдать требуемые разрешения (Приложение 4).

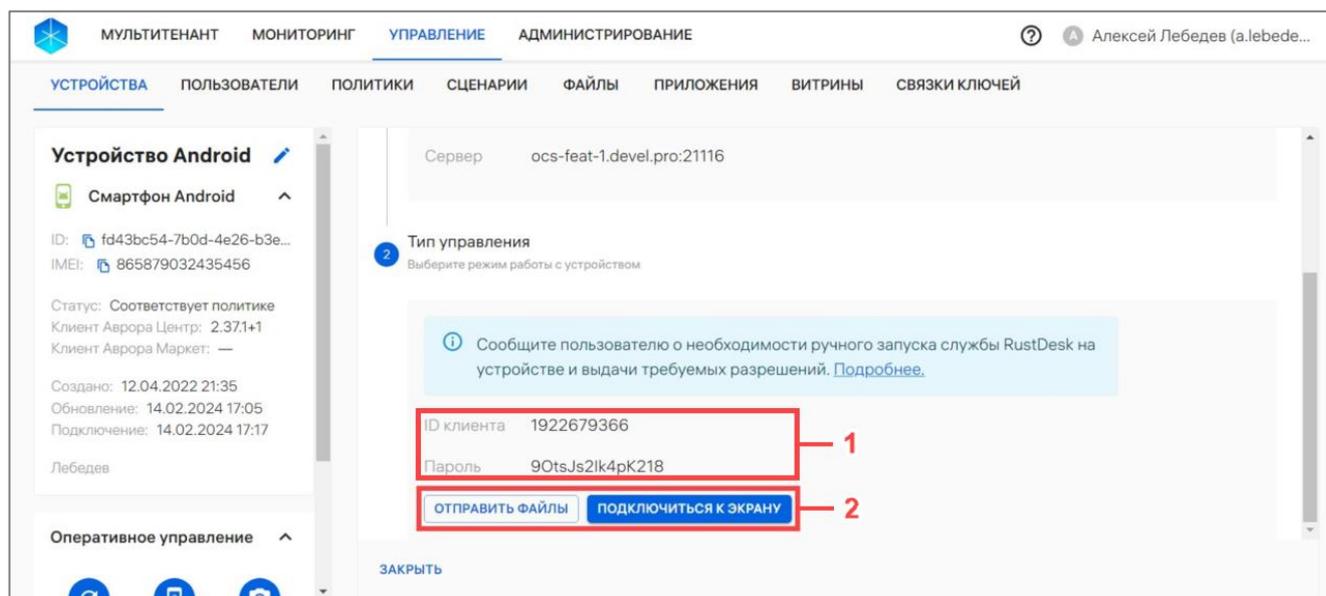


Рисунок 23

Если необходимо:

– подключиться к рабочему столу пользователя устройства, необходимо нажать кнопку «Подключиться к экрану» (см. Рисунок 23 [2]) и подтвердить подключение. Откроется окно desktop-клиента RustDesk с удаленным рабочим столом пользователя;

– передать на устройство или, наоборот, скопировать файлы с устройства, нажать «Отправить файлы» (см. Рисунок 23 [2]) и подтвердить подключение. Откроется окно desktop-клиента RustDesk для обмена файлами между ЭВМ и устройством пользователя.

В результате удаленное подключение к устройству пользователя будет настроено и выполнено.

2.1.1.8. Вкладка «События безопасности»

Во вкладке «События безопасности» отображается список произошедших на устройстве событий безопасности (Рисунок 24 [1]), который при разборе инцидентов позволяет определить, что происходило на устройстве, а при отсутствии событий на устройстве отображается сообщение «Нет данных».

Для получения события безопасности необходимо воспользоваться оперативной командой «Расписание отправки событий безопасности» (п. 2.2.10) или политикой с правилом «Конфигурация/Расписание отправки событий безопасности» (пп. 2.4.4.2).

ПРИМЕЧАНИЕ. Оперативная команда «Расписание отправки событий безопасности» доступна только для устройств, функционирующих под управлением ОС Аврора.

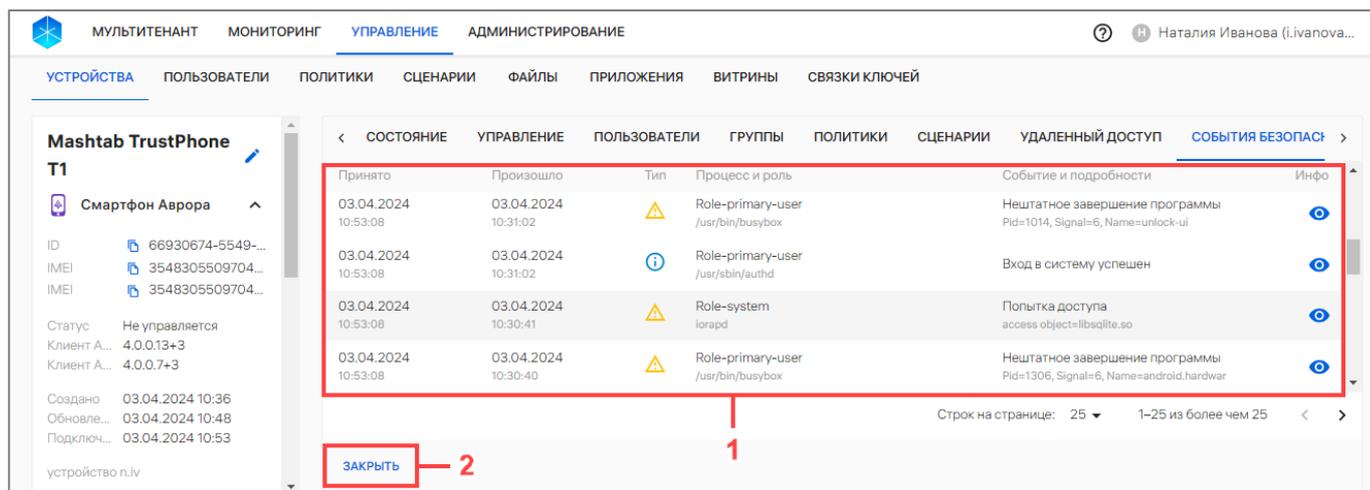


Рисунок 24

Список событий сортируется по дате произошедшего события, также возможно фильтровать по атрибутам, приведенным в таблице (см. Таблица 2).

Информация о событиях безопасности отображается в следующих столбцах, приведенных в таблице (Таблица 8).

Таблица 8

Параметр	Описание
Принято	Дата и время поступления события на устройствах
Произошло	Дата и время выполнения события на устройствах
Тип	Тип сообщения о событии в зависимости от важности (Приложение 1)
Процесс и роль	Роль отправителя события и полный путь к исполняемому файлу процесса отправителя события
Событие и подробности	Название события и дополнительная информация о нем
Инфо	Содержание сообщения. Для просмотра необходимо нажать значок  «Содержание сообщения». Для копирования текста сообщения в буфер обмена необходимо нажать кнопку «Копировать» (Рисунок 25). Для закрытия сообщения нажать кнопку «Закрыть»

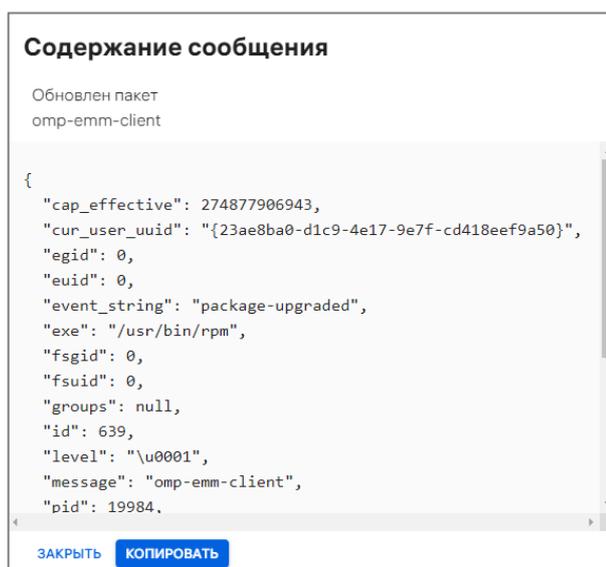


Рисунок 25

Для завершения просмотра карточки устройства и возврата к списку устройств необходимо нажать кнопку «Закрыть» (см. Рисунок 24 [2]).

2.1.1.9. Вкладка «Приложения»

Во вкладке «Приложения» отображается список приложений, установленных на устройстве.

ПРИМЕЧАНИЕ. На устройствах с ОС семейства Linux поиск установленных пакетов с типом `appimage` осуществляется в папках `/home`, `/tmp/.private/*`.

Информация о приложениях отображается в столбцах (Рисунок 26 [1]), приведенных в таблице (Таблица 9).

Таблица 9

Параметр	Описание
Приложение	Название приложения и его версия
Автозапуск	<p>Определяет включение автозапуска приложения.</p> <p>Возможные значения:</p> <ul style="list-style-type: none"> – <input type="radio"/> – Выключено; – <input checked="" type="checkbox"/> – Включено. <p>ВНИМАНИЕ! Автозапуск можно установить только для приложений с ОС Аврора.</p> <p>ПРИМЕЧАНИЕ. Если информация об автозапуске не была получена (например, автозапуск приложений отсутствует на устройстве на базе ОС Android), то ячейка не заполняется</p>
Разрешения	<p>Автоматическое применение разрешений.</p> <p>Определяет, выдано ли приложению автоматическое применение требуемых разрешений. Возможные значения:</p> <ul style="list-style-type: none"> – <input type="radio"/> – Выключено; – <input checked="" type="checkbox"/> – Включено. <p>ПРИМЕЧАНИЕ. Если информация о выданных разрешениях не была получена (например, для системных приложений в ОС Android), то ячейка не заполняется</p>
Политика	<p>Название политики, по правилу которой было установлено приложение. Название политики выделено цветом и представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5). При отсутствии политик с правилом установки приложения отображается значок «—»</p>
Пакетный менеджер	<p>Источник установки пакета приложения. Например: <code>dpkg</code>, <code>rpm</code>, <code>appimage</code>, <code>snap</code> и другие. Если информация об источнике не была получена, то отображается значение «n/a»</p>
Обновлено	Дата и время получения информации о пакете
Инфо	<p>Отображение названия пакета приложения (Рисунок 27) при нажатии значка  «Дополнительная информация» (Рисунок 26 [2])</p>

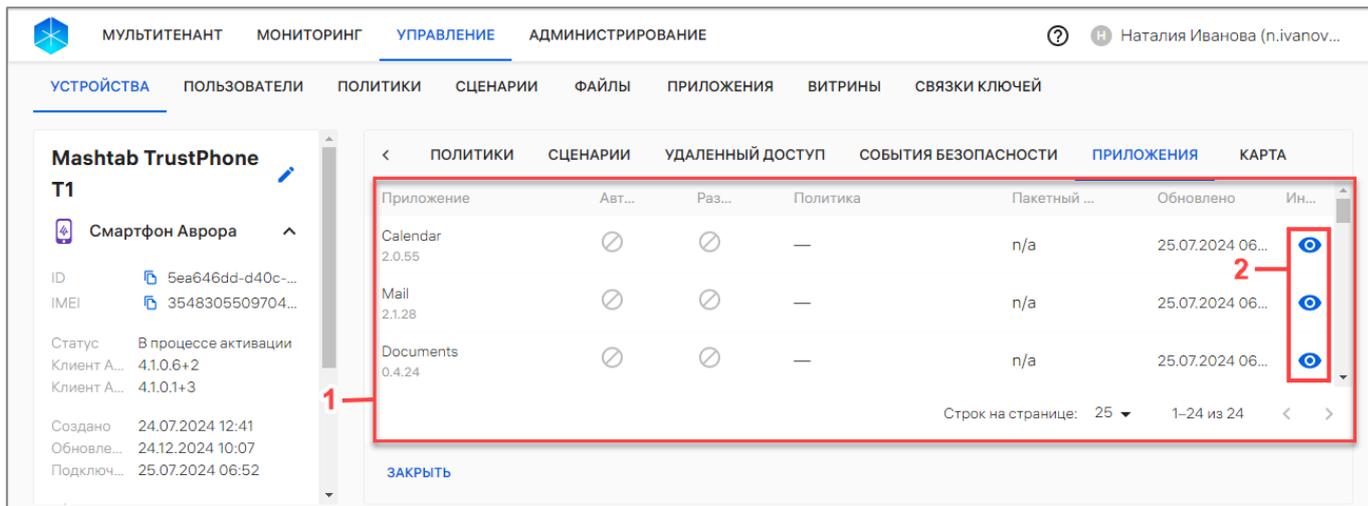


Рисунок 26

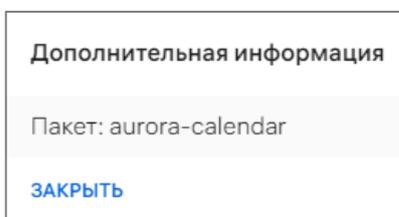


Рисунок 27

2.1.1.10. Вкладка «Карта»

Во вкладке «Карта» доступен просмотр местоположения активированного устройства на карте (Рисунок 28).

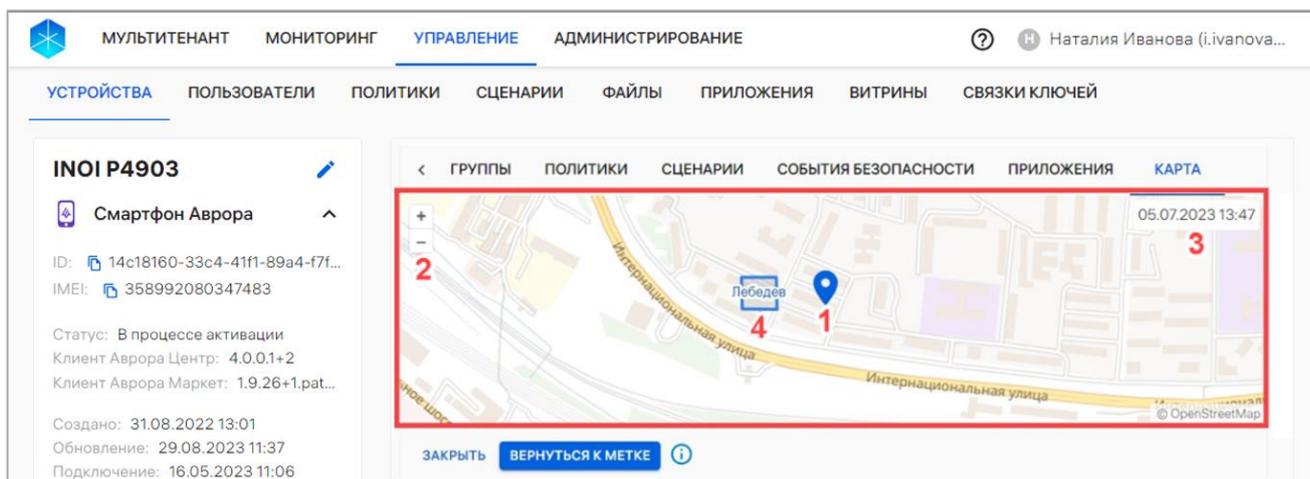


Рисунок 28

На карте отображены следующие элементы:

- метка с местоположением устройства (см. Рисунок 28 [1]);
- кнопки для увеличения или уменьшения масштаба карты (см. Рисунок 28 [2]);
- дата актуальности координат (см. Рисунок 28 [3]);
- территория (см. Рисунок 28 [4]) – если на устройство назначен офлайн-сценарий с событием «Нахождение на территориях, определяемых координатами»

или «Нахождение вне территории, определяемой координатами», то на карте также отображаются территории из офлайн-сценария.

При наведении курсора на метку устройства отображается подсказка, содержащая следующую информацию (Рисунок 29 [1]):

- координаты устройства;
- дата актуальности координат;
- режим работы геопозиционирования.

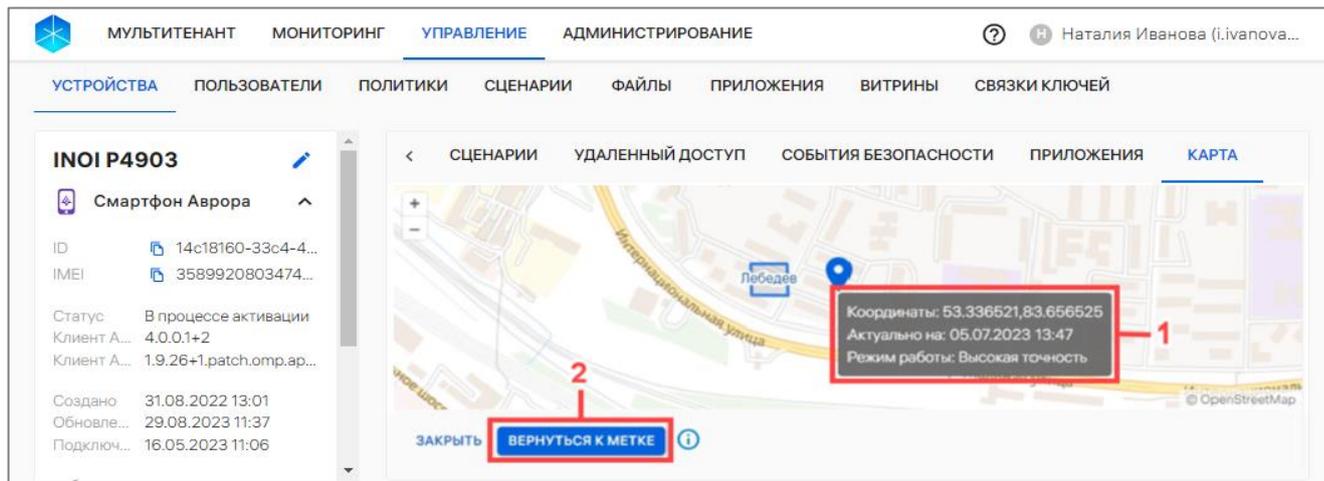


Рисунок 29

При необходимости возможно изменить масштаб и просматривать другие области карты. Чтобы вернуться к метке устройства в масштабе по умолчанию, необходимо нажать кнопку «Вернуться к метке» (см. Рисунок 29 [2]).

ПРИМЕЧАНИЯ:

- ✓ Координаты с устройства отправляются по расписанию отправки состояния;
- ✓ Актуальные координаты могут отсутствовать в состоянии, если устройство не определило их или определение отключено. Необходимо воспользоваться оперативным управлением для получения состояния устройства вне расписания;
- ✓ Точность определения координат устройства зависит от многих факторов, таких как: тип устройства, состояние сети, скорость, нахождение в здании или около высоких объектов, покрытие спутников, аппаратные и программные характеристики, уровень шума/помех и т.д.;
- ✓ Местоположение устройства с ОС семейства Linux отображается, но точность может быть только на уровне города.

2.1.2. Работа с карточкой группы устройств

С помощью карточки группы устройств можно просмотреть детальную информацию о группе устройств, выполнив следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- для отображения группы устройств в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройств.

В результате откроется карточка группы устройств, интерфейс которой включает:

- общую информацию о группе устройств (Рисунок 30 [1]), состоящую из параметров, приведенных в таблице (Таблица 10);

Таблица 10

Параметр	Описание
ID	Идентификатор группы устройств, который можно скопировать, нажав кнопку  «Копировать id группы в буфер обмена»
Создано	Дата и время добавления группы устройств
Обновление	Дата и время последнего обновления группы устройств
Комментарий	Дополнительная информация (заполняется при необходимости)

- вкладки карточки (Рисунок 30 [2]) с дополнительной информацией о группе устройств:

- «Устройства» (пп. 2.1.2.1);
- «Политики» (пп. 2.1.2.2);
- «Сценарии» (пп. 2.1.2.3).

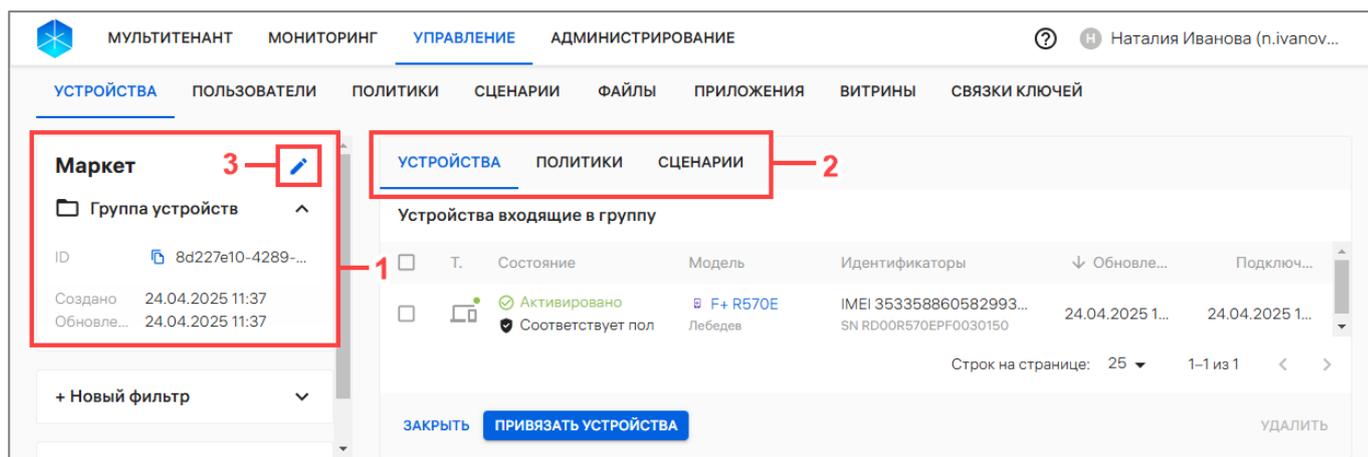


Рисунок 30

Для редактирования данных группы устройств необходимо нажать на значок  «Редактировать» (см. Рисунок 30 [3]) и внести необходимые изменения в следующие поля:

- «Имя группы»;
- «Комментарий».

2.1.2.1. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к группе устройств (Рисунок 31 [1]), а при его отсутствии отображается сообщение «Группа не содержит устройств».

При необходимости для поиска устройств возможно применение фильтров (Рисунок 31 [3]). Описание фильтров и процесса поиска приведено в подразделе 1.5.

Устройство возможно привязать к группе устройств с помощью кнопки «Привязать устройства» (Рисунок 31 [2]), выполнив действия, приведенные в пп. 2.2.8.3.

ПРИМЕЧАНИЕ. Указанный выше способ редактирования списка не применим для устройств из динамической группы. Кнопка «Привязать устройства» во вкладке «Устройства» у динамической группы устройств отсутствует.

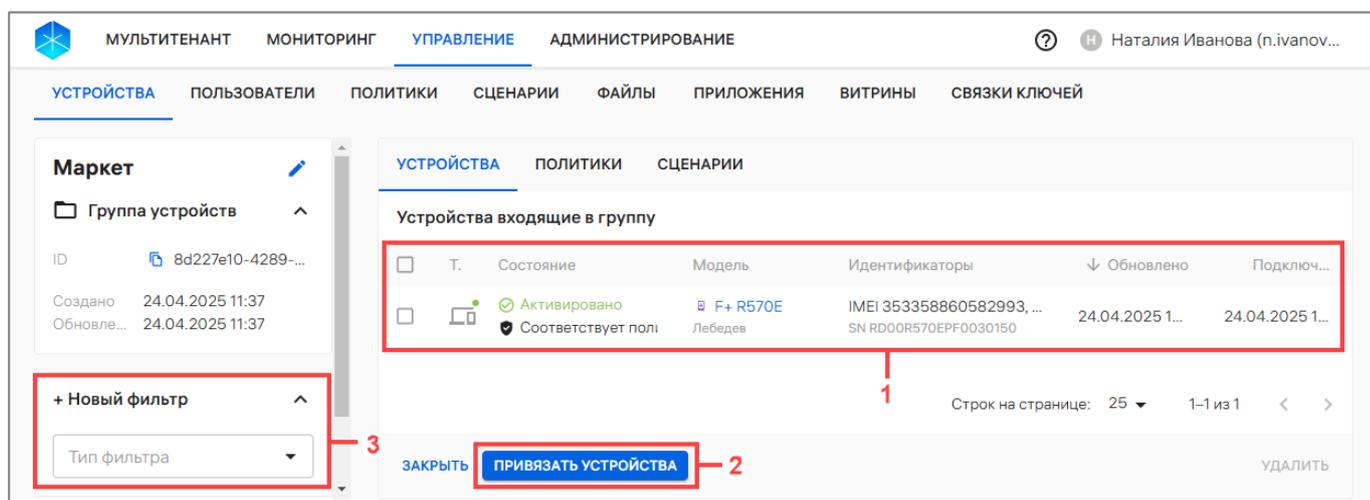


Рисунок 31

Информация по каждому устройству отображается в столбцах, приведенных в таблице (Таблица 11).

ПРИМЕЧАНИЕ. Значение некоторых столбцов может быть отсортировано: ↑ от старых к новым, ↓ от новых к старым.

Таблица 11

Параметр	Описание
Тип	<p>Значок с типом создания устройства и индикатор приложения «Аврора Центр». При наведении на значок отображается подсказка с типом создания устройства и статусом приложения «Аврора Центр».</p> <p>Возможные значения для типа создания устройства:</p> <ul style="list-style-type: none"> – «Устройство» - устройство было добавлено вручную, с помощью импорта или с использованием приглашения; – «Устройство из службы каталогов» - устройство было добавлено при синхронизации с LDAP-сервером.

Параметр	Описание
	Возможные значения для статуса приложения «Аврора Центр»: <ul style="list-style-type: none"> – «Клиент АЦ установлен» - на устройстве установлено приложение «Аврора Центр», с помощью которого выполняется управление устройством; – «Клиент АЦ удален» - на устройстве было удалено приложение «Аврора Центр»; – «Нет данных о Клиенте» - ППО не получил данные об установленном приложении «Аврора Центр» на устройстве
Состояние	Статус жизненного цикла и соответствие назначенной политике (Приложение 1)
Модель	<ul style="list-style-type: none"> – модель устройства (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку устройства (п. 2.1.1); – комментарий – дополнительная информация (заполняется при необходимости)
Идентификаторы	Идентификаторы устройства. Порядок отображения идентификаторов задается в настройках администрирования ППО (пп. 4.1.3.1)
Обновлено	Дата и время внесения последних изменений в устройство (редактирование имени устройства, модели или комментария; привязка/отвязка к группам или пользователям; назначение/отвязка политики или офлайн-сценария на устройство)
Подключено	Дата и время последнего подключения устройства к ППО

2.1.2.2. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу устройств (Рисунок 32 [1]), а при его отсутствии отображается сообщение «На группу не назначена ни одна политика».

Политика может быть назначена на группу устройств нажатием кнопки «Назначить политики» (Рисунок 32 [2]) и выполнением действий, приведенных в пп. 2.4.4.2.

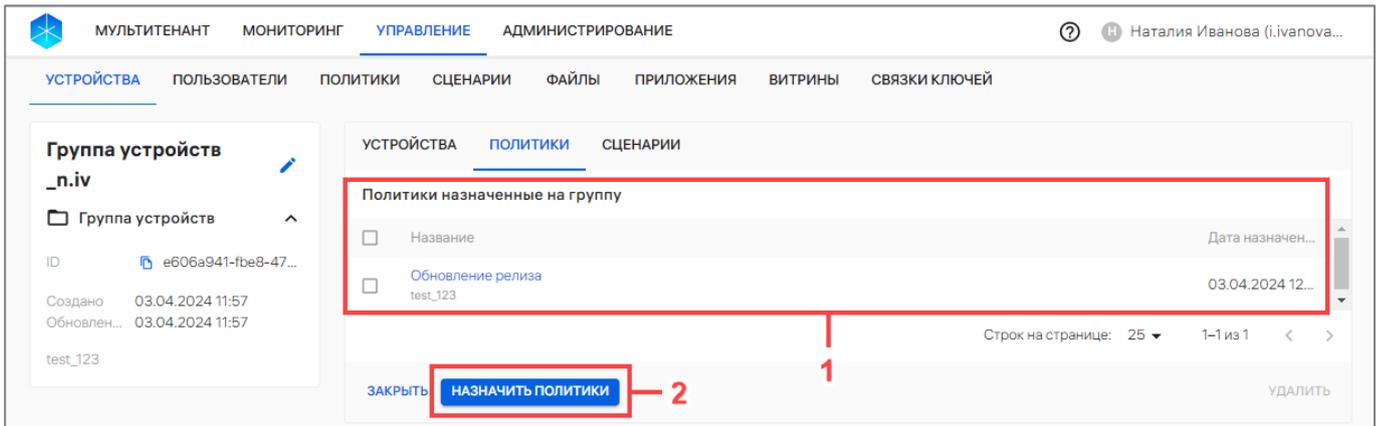


Рисунок 32

Информация о назначенных политиках отображается в следующих столбцах:

- «Название» – название политики, которая представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5);
- «Дата назначения» – дата и время назначения политики на группу устройств.

2.1.2.3. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу устройств (Рисунок 33), а при его отсутствии отображается сообщение «На группу не назначен ни один офлайн-сценарий».

ПРИМЕЧАНИЕ. Перед назначением офлайн-сценария на группу устройств необходимо убедиться, что добавлен хотя бы 1 офлайн-сценарий. Процесс добавления офлайн-сценариев приведен в п. 2.5.1.

При добавлении устройств в группу устройств все ранее назначенные на группу офлайн-сценарии будут применены на устройстве, в том числе при импорте устройства.

ПРИМЕЧАНИЕ. Процесс назначения офлайн-сценария на группы устройств и отвязки через карточку группы устройств приведен в пп. 2.5.2.3 и пп. 2.5.3.2 соответственно.

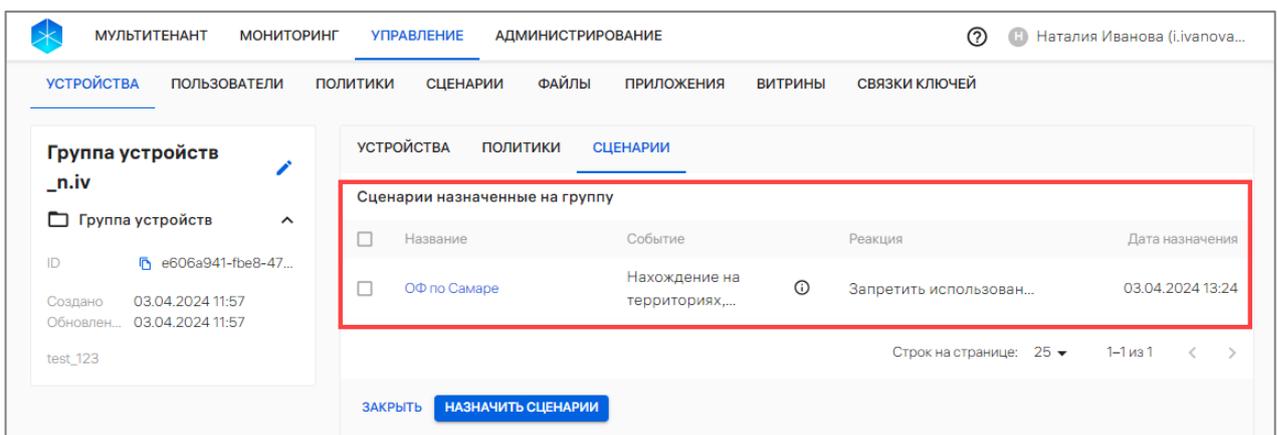


Рисунок 33

АДМГ.20134-01 90 01-3

В рабочей области информация о назначенных офлайн-сценариях отображается в столбцах, приведенных в таблице (Таблица 12).

Таблица 12

Параметр	Описание
Название	– название офлайн-сценария; – комментарий – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 43))
Реакция	Действие, которое должно произойти с устройством из группы устройств в результате назначения данного офлайн-сценария
Дата назначения	Дата и время назначения офлайн-сценария на группу устройств

2.1.3. Работа с карточкой пользователя

Для просмотра карточки пользователя необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- для отображения списка пользователей в области фильтров выбрать «Поиск по пользователям»;
- выбрать необходимого пользователя и нажать на имя.

В результате откроется карточка пользователя, интерфейс которой включает:

- общую информацию о пользователе (Рисунок 34 [1]), состоящую из параметров, приведенных в таблице (Таблица 13);

Таблица 13

Параметр	Описание
Пользователь	– фамилия, имя и отчество пользователя; – тип пользователя (Приложение 1)
ID	Идентификатор пользователя, который можно скопировать, нажав кнопку  «Копировать id пользователя в буфер обмена»
Должность	Должность, занимаемая пользователем
Email	Электронная почта пользователя
Тел. рабочий	Рабочий телефон пользователя
Создание	Дата и время добавления пользователя
Обновление	Дата и время последнего обновления информации о пользователе

– вкладки карточки (Рисунок 34 [2]) с дополнительной информацией о пользователе:

- «Устройства» (пп. 2.1.3.1);
- «Группы» (пп. 2.1.3.2);
- «Политики» (пп. 2.1.3.3).

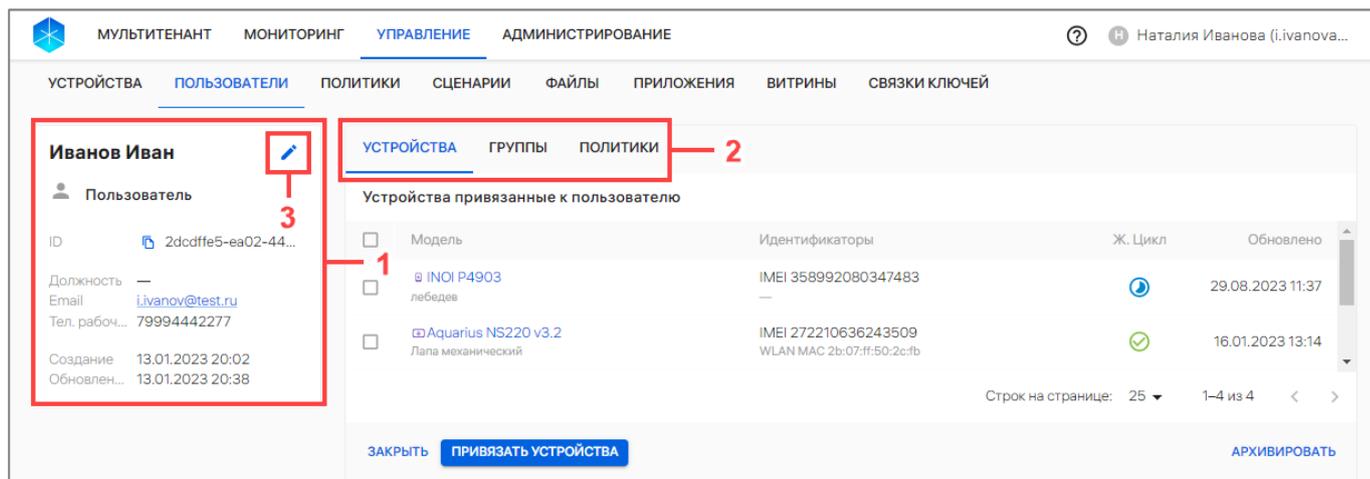


Рисунок 34

Для редактирования данных о пользователе необходимо нажать на значок «Редактировать» (Рисунок 34 [3]) и внести необходимые изменения в следующие поля:

- «ФИО»;
- «Почта рабочая»;
- «Должность»;
- «Телефон рабочий».

ПРИМЕЧАНИЕ. Редактированию вручную подлежат данные только пользователей с типом «Пользователь». Для обновления данных пользователей с типом «Пользователь из орг.подразделения» необходимо повторно получить данные из LDAP.

2.1.3.1. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к пользователю (Рисунок 35 [1]).

Для редактирования списка устройств во вкладке «Устройства» необходимо нажать кнопку «Привязать устройства» (Рисунок 35 [2]) и выполнить действия, приведенные в пп. 2.3.5.2.

ПРИМЕЧАНИЕ. На все привязанные и отвязанные устройства будут применены новые перекомбинированные политики и офлайн-сценарии.

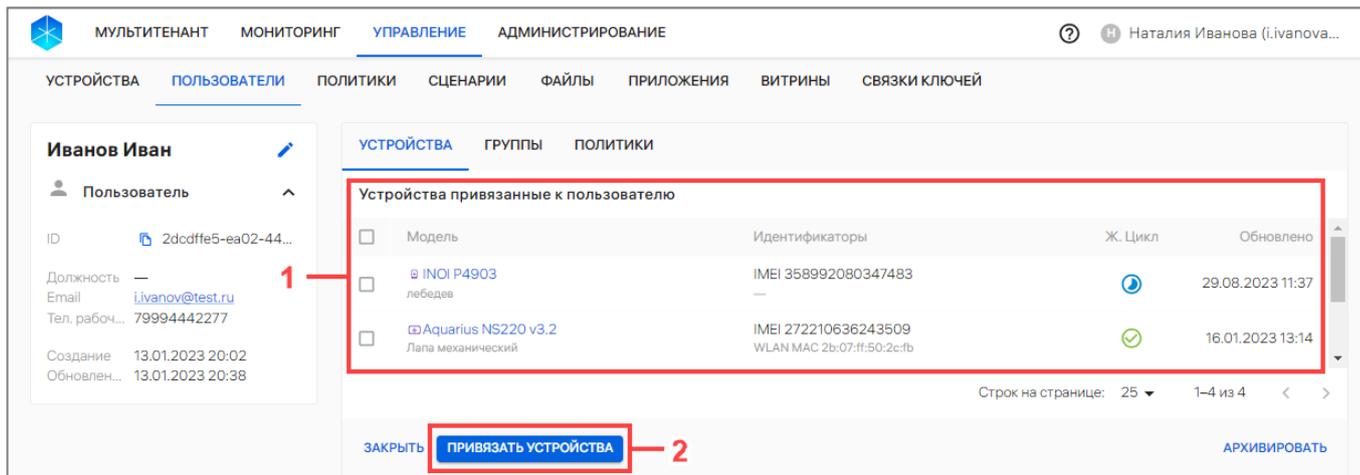


Рисунок 35

Информация об устройствах отображается в столбцах, приведенных в таблице (Таблица 14).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 14

Параметр	Описание
Модель	– тип устройства (Приложение 1); – модель устройства (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку устройства (п. 2.1.1); – комментарий – дополнительная информация (заполняется при необходимости)
Идентификаторы	– IMEI устройства; – MAC-адрес WLAN устройства
Ж. Цикл	Статус жизненного цикла устройства (Приложение 1)
Обновлено	Дата и время обновления данных устройств

2.1.3.2. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к пользователю групп пользователей (Рисунок 36), а при их отсутствии отображается сообщение «Пользователь не состоит ни в одной группе».

Описание способов привязки пользователя к группе пользователей приведено в п. 2.3.4.

Название группы пользователей представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы.

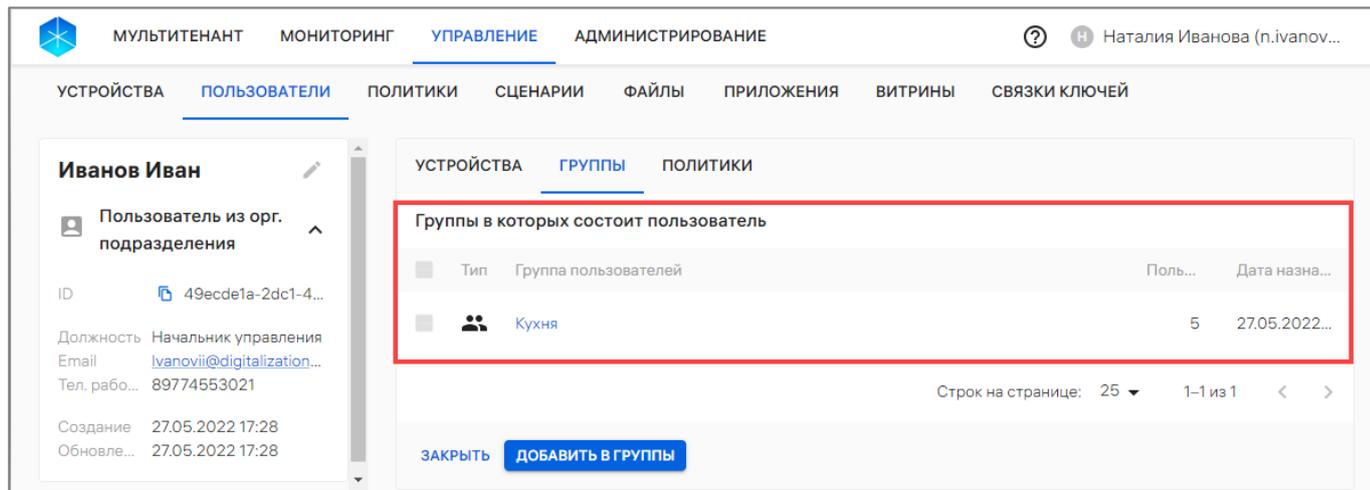


Рисунок 36

Информация о группах пользователей отображается в столбцах, приведенных в таблице (Таблица 15).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: \uparrow от старых к новым, \downarrow от новых к старым.

Таблица 15

Параметр	Описание
Тип	Тип группы пользователей (Приложение 1)
Группа пользователей	– название группы пользователей, к которой привязан данный пользователь; – комментарий – дополнительная информация (заполняется при необходимости)
Пользователей	Количество участников группы
Дата назначения	Дата и время привязки пользователя к группе

2.1.3.3. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей, к которой привязан данный пользователь (Рисунок 37 [2]), а при отсутствии назначенных политик отображается сообщение «На пользователя не назначено ни одной политики».

В случае пересечения с другими политиками отобразится полный список названий всех политик на группах устройств или группах пользователей.

Информация о политиках отображается в следующих столбцах (Рисунок 37):

– «Название» – название политики, назначенной на группу пользователей устройства, в которую входит текущий пользователь. Представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке (п. 2.1.5);

– «Содержимое» – краткая информация по правилам, добавленным в политику;

– «Группа» – наименование группы, на которую назначена политика.

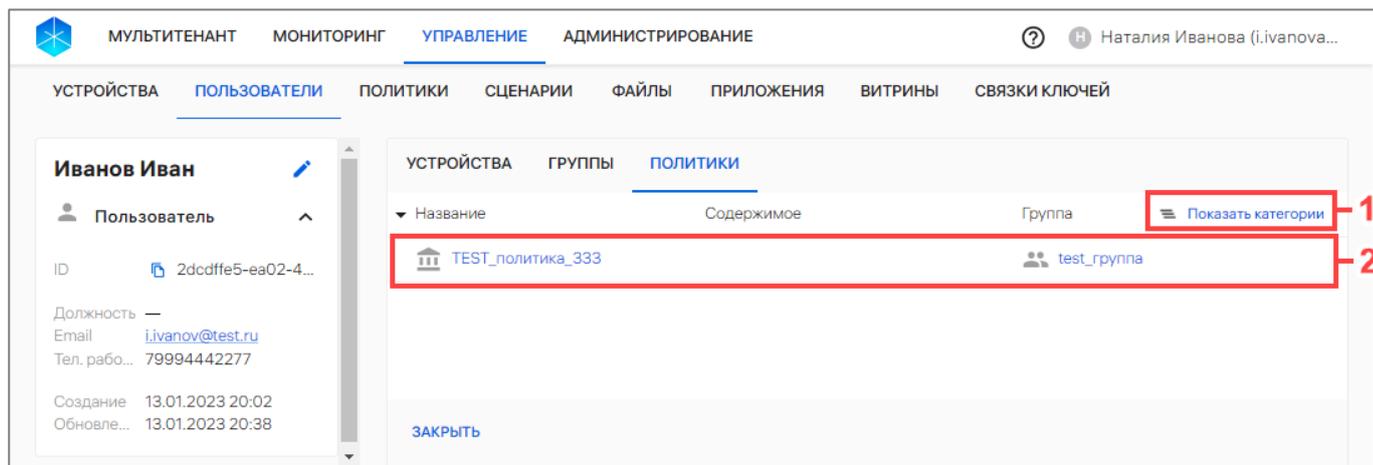


Рисунок 37

Для отображения категорий правил политик, назначенных на группу пользователей, необходимо нажать кнопку  «Показать категории» (см. Рисунок 37 [1]).

Для просмотра вложенной информации о политике необходимо нажать значок , в результате чего откроется вложенная информация о политике.

2.1.4. Работа с карточкой группы пользователей

Для просмотра карточки группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название выбранной группы пользователей.

В результате откроется карточка группы пользователей, интерфейс которой включает:

- общую информацию о группе пользователей (Рисунок 38 [1]), состоящую из параметров, приведенных в таблице (Таблица 16);

Таблица 16

Параметр	Описание
Название	Название группы пользователей
Тип	Тип группы пользователей (Приложение 1)
ID	Идентификатор группы пользователей, который может быть скопирован нажатием кнопки  «Копировать»
Создано	Дата и время добавления группы пользователей
Обновление	Дата и время последнего обновления группы пользователей
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 38 [2]) с дополнительной информацией о группе пользователей:

- «Пользователи» (пп. 2.1.4.1);
- «Политики» (пп. 2.1.4.2);
- «Сценарии» (пп. 2.1.4.3).

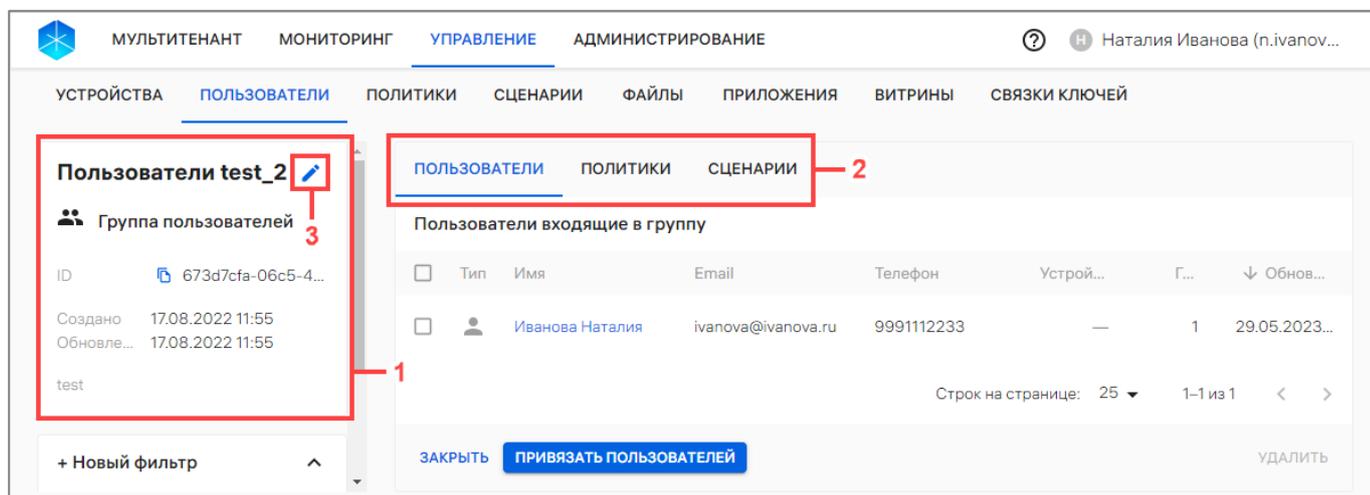


Рисунок 38

Для редактирования данных группы с типом  «Группа пользователей» необходимо нажать на значок  «Редактировать» (см. Рисунок 38 [3]) и внести необходимые изменения в следующие поля:

- «Имя группы»;
- «Комментарий».

ПРИМЕЧАНИЕ. Редактирование группы с типом  «Организационное подразделение» недоступно. Значок  «Редактировать» и кнопки «Удалить», «Привязать пользователей» у такой группы неактивны.

2.1.4.1. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список пользователей для данной группы пользователей (Рисунок 39 [1]), а при отсутствии списка отображается сообщение «В группе нет пользователей».

Для редактирования списка пользователей необходимо нажать кнопку «Привязать пользователей» (Рисунок 39 [2]) и выполнить действия, приведенные в пп. 2.3.4.3.

При необходимости для поиска устройств возможно применение фильтров (Рисунок 39 [3]). Описание фильтров и процесса поиска приведено в подразделе 1.5.

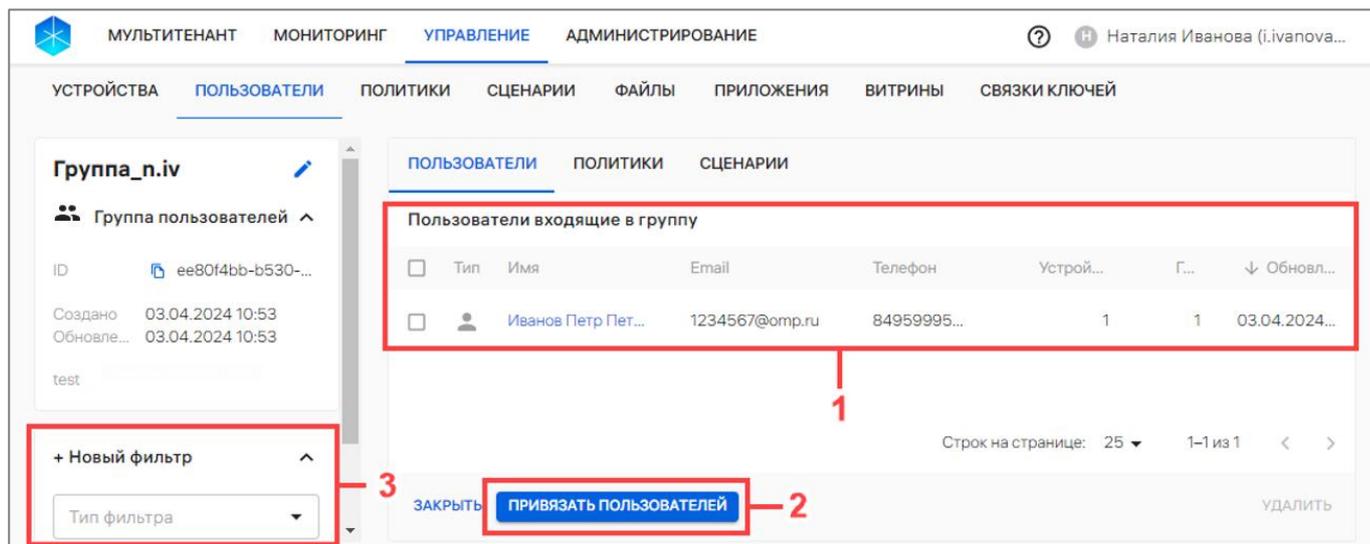


Рисунок 39

Информация о пользователях отображается в столбцах, приведенных в таблице (Таблица 17).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 17

Параметр	Описание
Тип	Тип пользователей, входящих в группу (Приложение 1)
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку пользователя (п. 2.1.3))
Email	Рабочая почта пользователя
Телефон	Номер телефона пользователя
Устройства	Количество устройств, привязанных к пользователю
Группы	Количество групп, в которые включен пользователь
Обновлено	Дата и время обновления данных пользователя

2.1.4.2. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей (Рисунок 40 [1]), а при отсутствии списка отображается сообщение «На группу не назначена ни одна политика».

Для редактирования списка политик необходимо нажать кнопку «Назначить политики» (Рисунок 40 [2]) и далее выполнить действия, описанные в пп. 2.4.4.3.

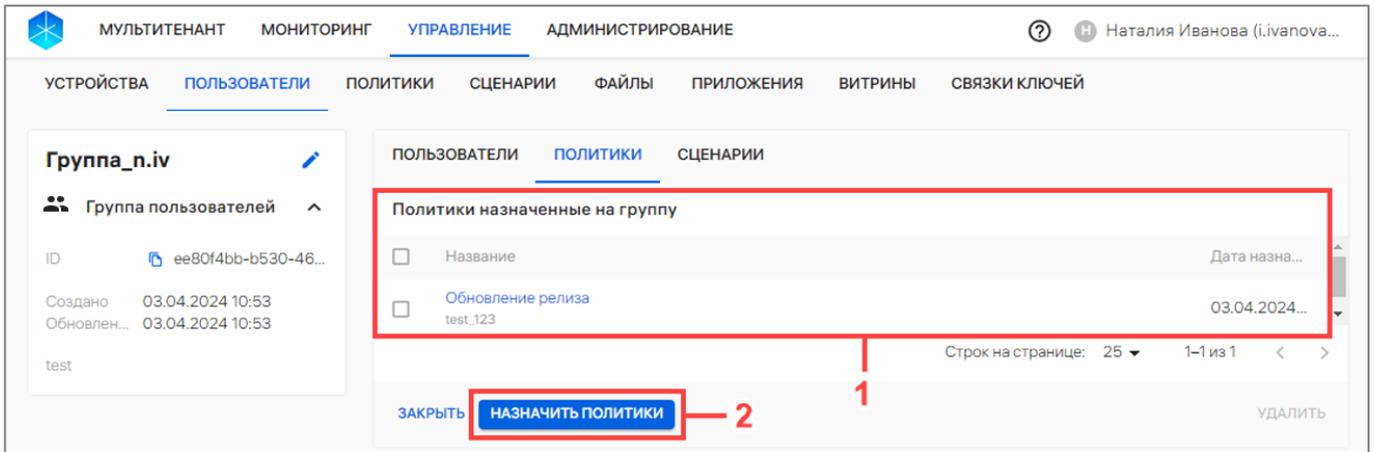


Рисунок 40

Информация о политиках отображается в столбцах, приведенных в таблице (Таблица 18).

Таблица 18

Параметр	Описание
Название	Название политики, назначенной на группу пользователей (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5))
Дата назначения	Дата назначения политики

2.1.4.3. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу пользователей (Рисунок 41 [1]), а при его отсутствии отображается сообщение «На группу не назначен ни один офлайн-сценарий».

ПРИМЕЧАНИЕ. Для назначения и отвязки офлайн-сценария необходимо нажать кнопку «Назначить сценарии» (Рисунок 41 [2]) и выполнить действия, приведенные в пп. 2.5.2.4 и пп. 2.5.3.2.

ВНИМАНИЕ! Перед назначением офлайн-сценария на группу пользователей необходимо убедиться, что добавлен хотя бы 1 офлайн-сценарий. Процедура добавления офлайн-сценариев описана в п. 2.5.1.

При добавлении пользователей в группу пользователей, все ранее назначенные на группу офлайн-сценарии будут применены на пользователя, в том числе при импорте.

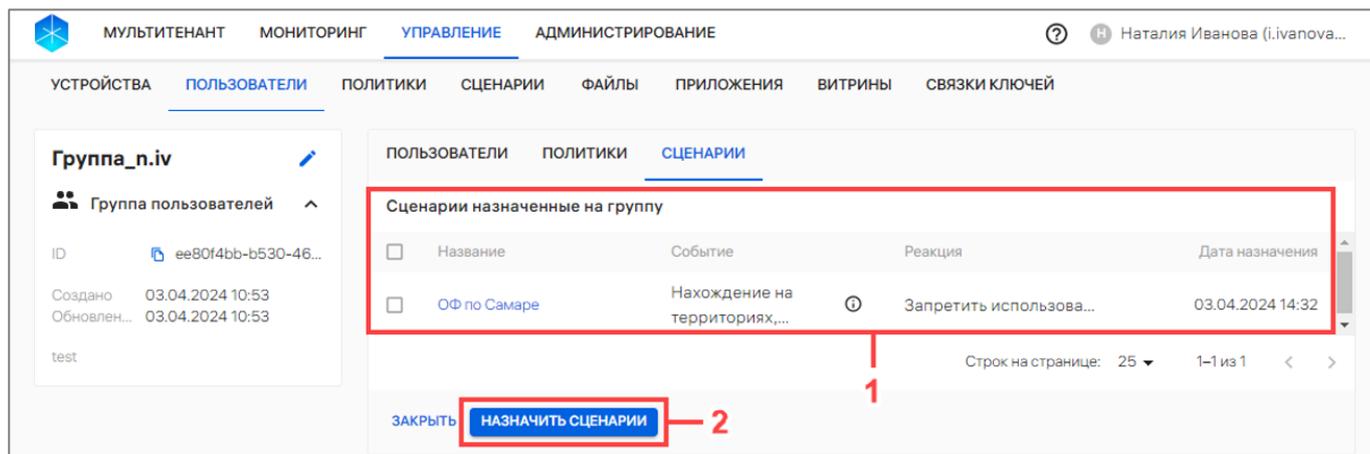


Рисунок 41

В рабочей области информация о назначенных офлайн-сценариях отображается в столбцах, приведенных в таблице (Таблица 19).

Таблица 19

Параметр	Описание
Название	– название офлайн-сценария (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку офлайн-сценария); – комментарий – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 43))
Реакция	Действие, которое должно произойти с группой пользователей в результате назначения данного офлайн-сценария
Дата назначения	Дата и время назначения офлайн-сценария на группу пользователей

2.1.5. Работа с карточкой политики

В карточке политики отображается информация о правилах политики и списках групп пользователей, на которых данная политика назначена.

Для просмотра карточки политики необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать на название политики.

В результате откроется карточка политики, интерфейс которой включает:

– общую информацию о политике (Рисунок 42 [1], состоящую из параметров, приведенных в таблице (Таблица 20));

Таблица 20

Параметр	Описание
Название	Название политики
ID	Идентификатор политики, который можно скопировать, нажав кнопку  «Копировать id политики в буфер обмена»
Создано	Дата и время создания политики
Обновление	Дата и время последнего обновления политики
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 42 [2]) с дополнительной информацией о политике:

- «Правила» (пп. 2.1.5.1);
- «Группы» (пп. 2.1.5.2).

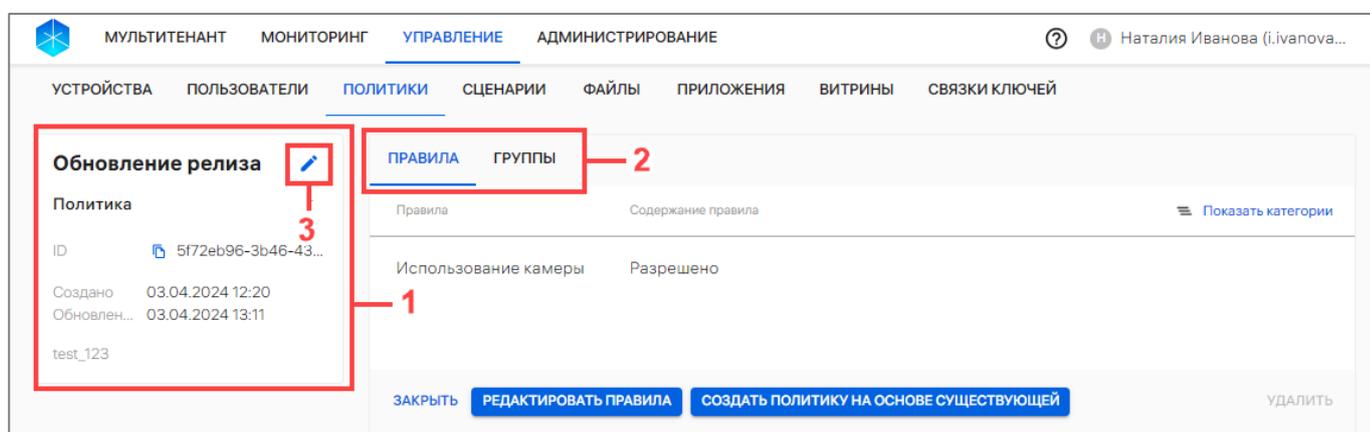


Рисунок 42

Для редактирования данных политики необходимо нажать на значок  «Редактировать» (см. Рисунок 42 [3]) и внести необходимые изменения в следующие поля:

- «Наименование»;
- «Комментарий».

2.1.5.1. Вкладка «Правила»

Во вкладке «Правила» отображается список правил, добавленных в политику, с указанием их категории и содержания. Информация отображается в следующих столбцах (Рисунок 43):

- «Правила» – название правила;
- «Содержание правила» – краткая информация по правилам, добавленным в политику.

Для отображения категории правил необходимо нажать кнопку  «Показать категории» (Рисунок 43).

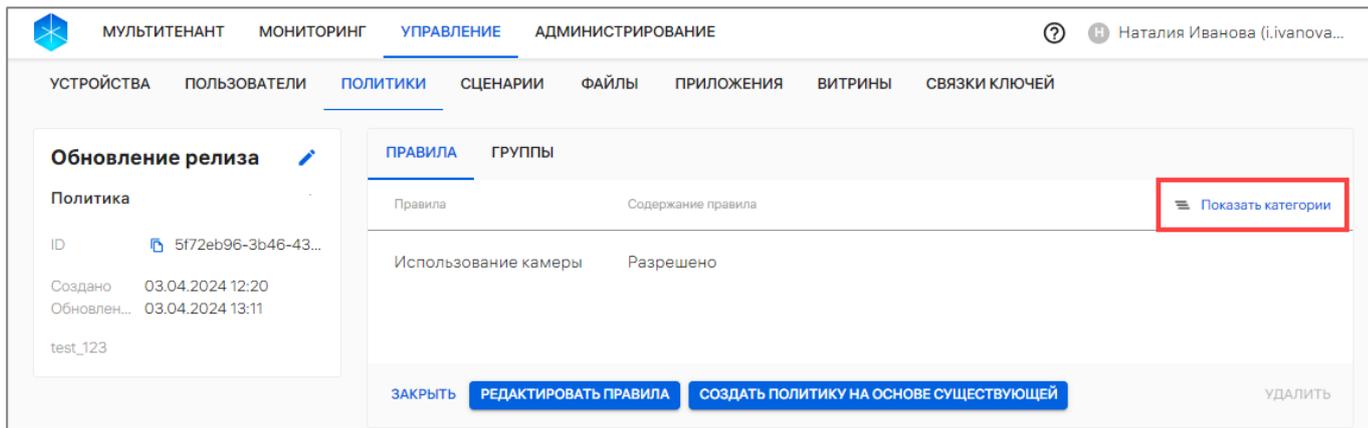


Рисунок 43

Для просмотра информации о каждой категории правил необходимо нажать значок  в строке с категорией (Рисунок 44 [1]), в результате чего отобразится перечень правил, входящих в данную категорию.

Для перехода к списку правил необходимо нажать кнопку  «Показать список» (Рисунок 44 [2]).

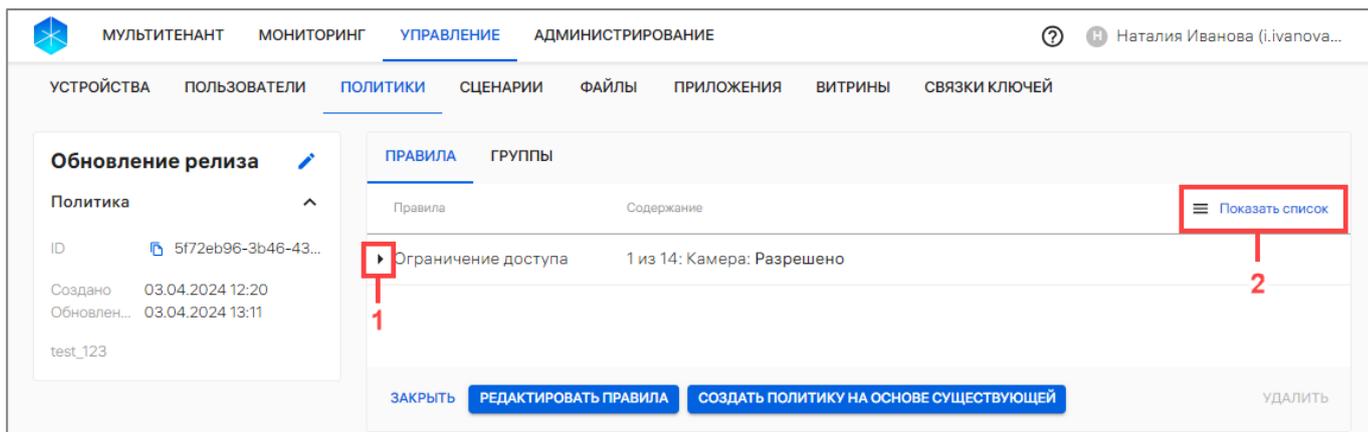


Рисунок 44

Набор правил политики подлежит редактированию. Процесс редактирования приведен в п. 2.4.6.

2.1.5.2. Вкладка «Группы»

Во вкладке «Группы» отображаются группы действия политик (списки групп устройств и групп пользователей), на которые назначена политика (Рисунок 45 [1]).

Для редактирования списка групп устройств или групп пользователей необходимо нажать кнопку «Редактировать группы» (Рисунок 45 [2]) и далее выполнить действия, описанные в пп. 2.4.4.1 и пп. 2.4.7.1.

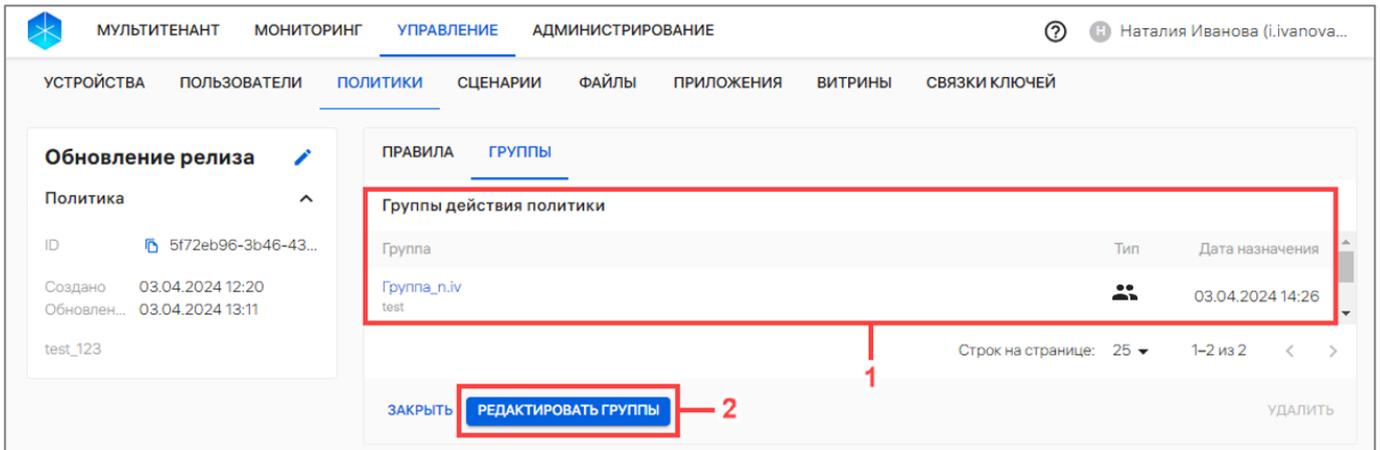


Рисунок 45

Информация о группах, на которые распространяется действие политики, отображается в столбцах, приведенных в таблице (Таблица 21).

Таблица 21

Параметр	Описание
Группа	– название группы устройств или группы пользователей, на которые назначена данная политика (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку группы); – комментарий – дополнительная информация (заполняется при необходимости)
Тип	Тип группы: –  – группа пользователей; –  – группа устройств
Дата назначения	Дата и время назначения политики

2.1.6. Работа с карточкой офлайн-сценария

В карточке офлайн-сценария отображаются параметры, заданные при создании сценария (событие, реакция, наименование, комментарий), а также группы устройств и пользователей, на которые сценарий назначен.

Для просмотра карточки сценария необходимо выполнить следующие действия:

- перейти в подраздел «Сценарии» раздела «Управление»;
- нажать на название офлайн-сценария.

В результате откроется карточка офлайн-сценария, интерфейс которой включает:

- общую информацию об офлайн-сценарии (Рисунок 46 [1]), состоящую из параметров, приведенных в таблице (Таблица 22);

Таблица 22

Параметр	Описание
Название	Название офлайн-сценария
ID	Идентификатор офлайн-сценария, который можно скопировать, нажав кнопку  «Копировать id сценария в буфер обмена»
Событие	Доступные значения приведены в таблице (Таблица 43)
ID меток входа	ВНИМАНИЕ! Данное поле отображается, если выбраны события «Нахождение на территории, определяемой NFC-метками». Уникальные идентификаторы меток входа
ID меток выхода	ВНИМАНИЕ! Данное поле отображается, если выбраны события «Нахождение на территории, определяемой NFC-метками». Уникальные идентификаторы меток выхода
BSSID	ВНИМАНИЕ! Данное поле отображается, если выбраны события «Нахождение в зоне WLAN»/«Вне зоны действия WLAN»
Период	ВНИМАНИЕ! Данное поле отображается, если выбрана реакция «Задать период отправки событий безопасности», либо событие «Отсутствие связи с сервером»
Территории	ВНИМАНИЕ! Данное поле отображается, если выбраны события «Нахождение на территории, определяемой координатами»/ «Нахождение вне территории, определяемой координатами»
Реакция	Доступные значения приведены в таблице (Таблица 43)
Создано	Дата и время создания офлайн-сценария
Комментарий	Дополнительная информация (заполняется при необходимости)

– список групп устройств и групп пользователей, на которые назначен данный офлайн-сценарий (Рисунок 46 [2]).

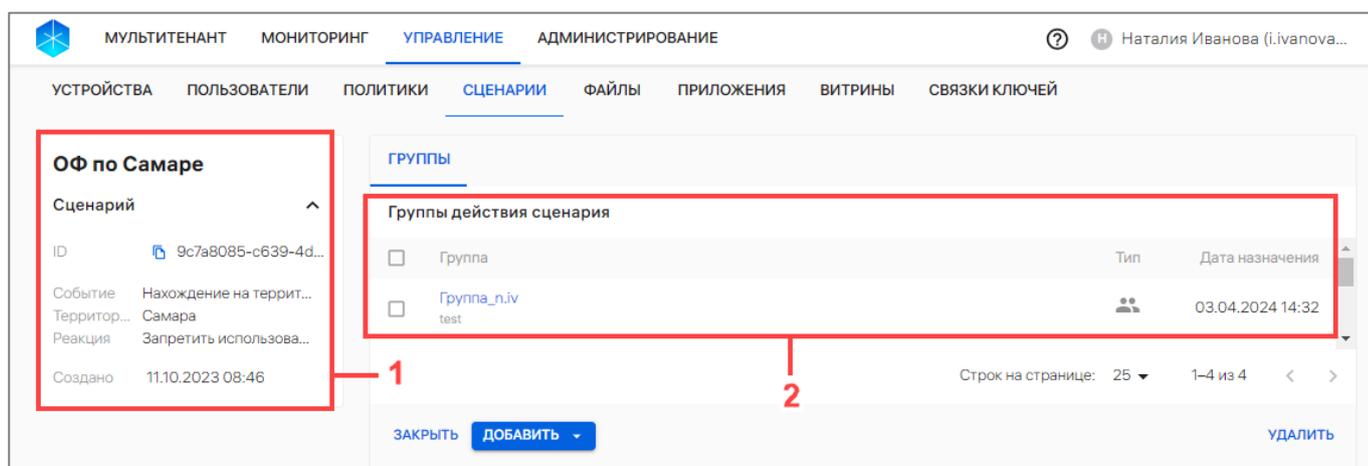


Рисунок 46

В рабочей области, в списке групп устройств и групп пользователей, на которые назначен данный офлайн-сценарий, информация отображается в столбцах, приведенных в таблице (Таблица 23).

Таблица 23

Параметр	Описание
Группа	– название группы устройств или группы пользователей (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку групп устройств или групп пользователей); – комментарий – дополнительная информация (заполняется при необходимости)
Тип	Тип группы: –  – группа устройств; –  – группа пользователей
Дата назначения	Дата и время назначения офлайн-сценария на группу

2.1.7. Работа с карточкой файла

С помощью карточки файла возможно выполнить следующие действия:

- просмотреть информацию о файле;
- добавить версию файла;
- скачать версию файла;
- удалить версию файла.

Для просмотра карточки файла необходимо выполнить следующие действия:

- перейти в подраздел «Файлы» раздела «Управление»;
- нажать на название необходимого файла.

В результате откроется карточка файла, интерфейс которой включает:

- общую информацию о файле (Рисунок 47 [1]), состоящую из параметров, приведенных в таблице (Таблица 24);
- версии файла (Рисунок 47 [2]).

Таблица 24

Параметр	Описание
ID	Идентификатор файла, который можно скопировать, нажав значок 
Источник	Источник откуда был загружен рабочий файл
Ветка	Ветка в Git-репозитории
Количество	Общее количество версий рабочего файла
Создан	Дата и время создания файла
Обновлен	Дата и время последнего обновления файла
Комментарий	Дополнительная информация (заполняется при необходимости)

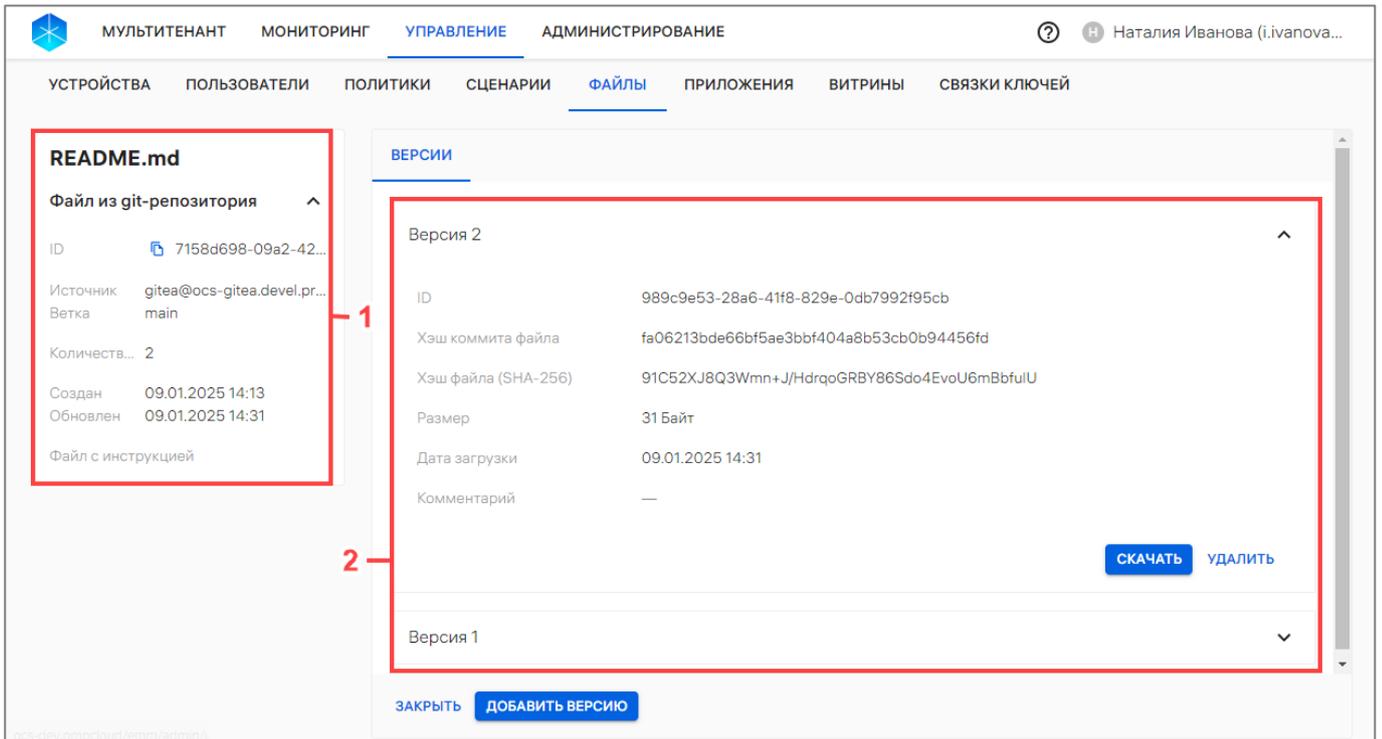


Рисунок 47

2.2. Подраздел «Устройства»

Подраздел «Устройства» Консоли администратора ПУ предназначен для работы со списком устройств/групп устройств.

Для перехода в подраздел необходимо выбрать в верхней панели раздел «Управление», подраздел «Устройства». В результате в рабочей области отобразится список устройств/групп устройств (Рисунок 48 [2]).

ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 48 [1]).

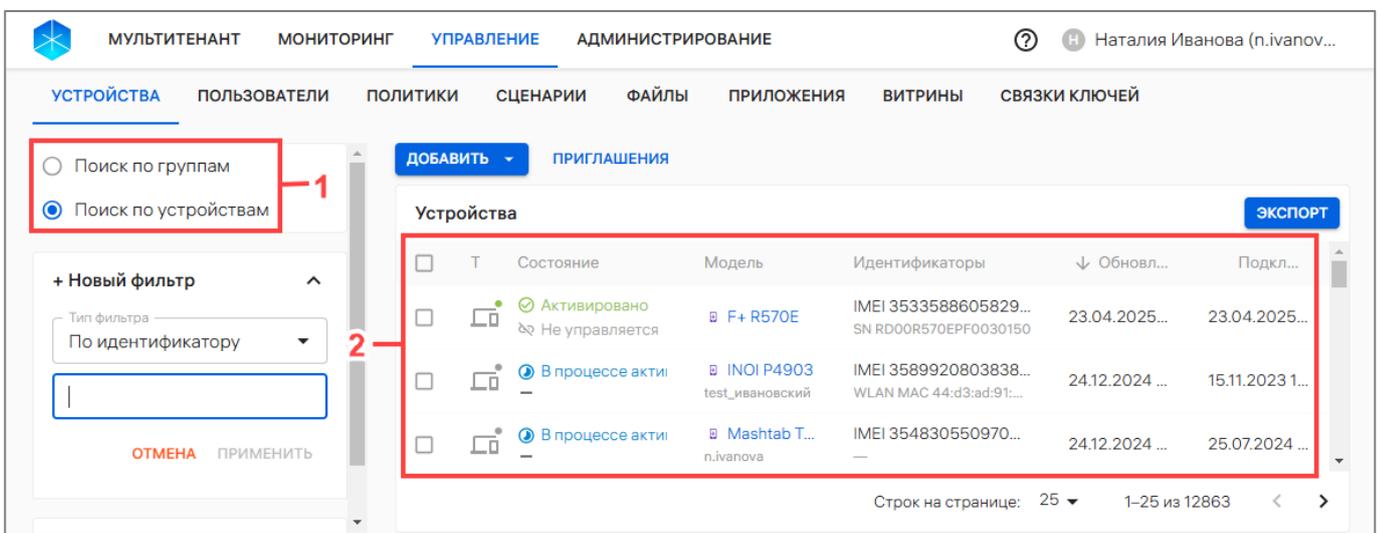


Рисунок 48

ПРИМЕЧАНИЕ. Архивные устройства отображаются в списке устройств только в случае, если включена соответствующая настройка (п. 4.1.3).

В рабочей области подраздела «Устройства» информация об устройствах отображается в столбцах, описания которых приведены в таблице (см. Таблица 11). При отсутствии информации о добавленных устройствах или групп устройств отображается сообщение «Нет данных».

При выборе в области фильтров «Поиск по группам» (Рисунок 49 [1]) информация о группах устройств в рабочей области отображается в столбцах (Рисунок 49 [2]), приведенных в таблице (Таблица 25).

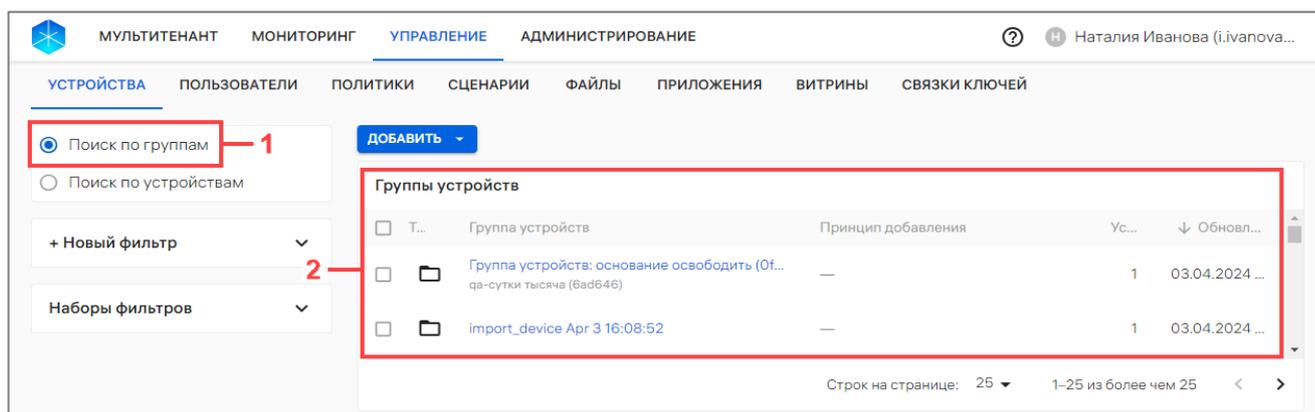


Рисунок 49

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 25

Параметр	Описание
Тип	Тип группы устройств (Приложение 1)
Группа устройств	– название группы устройств (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку группы устройств); – комментарий - дополнительная информация (заполняется при необходимости)
Принцип добавления	Значение, по которому устройства были добавлены в группу
Устройства	Количество устройств, привязанных к группе
Обновлено	Параметр сортировки по дате обновления политики

В Консоли администратора ПУ предусмотрена возможность добавления устройств или групп устройств одним из следующих способов:

- вручную в соответствии с пп. 2.2.1.1 и п. 2.2.2;
- с помощью CSV-файла в соответствии с п. 2.2.3;
- с помощью приглашения на самостоятельную регистрацию устройства в соответствии с пп. 2.2.1.2.

2.2.1. Добавление устройства в ПУ

2.2.1.1. Добавление устройства вручную

Для добавления устройства вручную необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить устройство» (Рисунок 50);

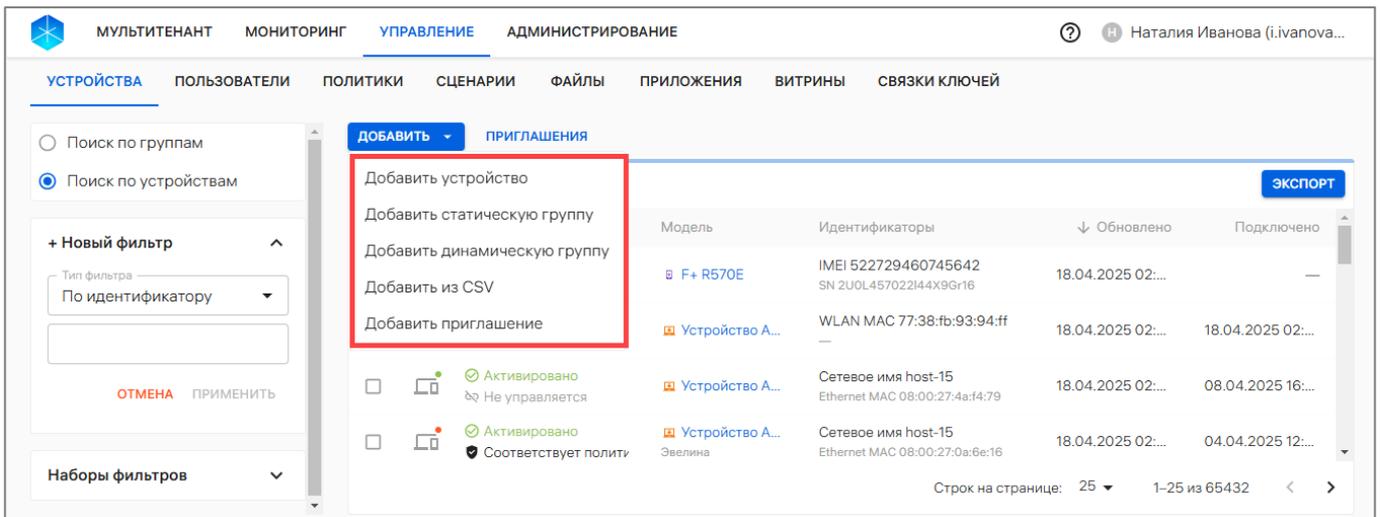


Рисунок 50

– в открывшемся окне (Рисунок 51) заполнить поля, приведенные в таблице (Таблица 26).

ПРИМЕЧАНИЕ. Для отображения полей «IMEI», «Серийный номер», «Ethernet MAC», «WLAN MAC», «Имя устройства» необходимо установить галочку в чекбоксе напротив требуемого параметра. После ввода значения нажать Enter на клавиатуре и при необходимости добавить второе значение для полей: «IMEI», «Ethernet MAC», «WLAN MAC». При необходимости удалить параметр, нажать на значок  справа от значения. Для полной очистки нажать на значок  «Очистить» в конце поля.

ВНИМАНИЕ! Рекомендуется заполнить все существующие идентификаторы устройства, чтобы уменьшить риск создания дублей;

- после ввода значений необходимо подтвердить либо отменить действия.

При успешном добавлении устройства отобразится соответствующее сообщение и откроется карточка добавленного устройства (п. 2.1.1).

МУЛЬТИТЕНАНТ МОНИТОРИНГ **УПРАВЛЕНИЕ** АДМИНИСТРИРОВАНИЕ ? Н Наталия Иванова (i.ivanova)

УСТРОЙСТВА ПОЛЬЗОВАТЕЛИ ПОЛИТИКИ СЦЕНАРИИ ФАЙЛЫ ПРИЛОЖЕНИЯ ВИТРИНЫ СВЯЗКИ КЛЮЧЕЙ

< Создание устройства вручную

IMEI Серийный номер Ethernet MAC WLAN MAC Имя устройства

Рекомендуется заполнить все существующие идентификаторы, это уменьшит риск создания дубликатов устройства.

IMEI

Серийный номер

Ethernet MAC

WLAN MAC

Имя устройства

Доступные платформы

Аврора Android Linux

Модель устройства

Комментарий

До 512 символов

СОЗДАТЬ

Рисунок 51

Таблица 26

Параметр	Значения	Описание
IMEI	Ввести международный идентификатор мобильного оборудования. Ввод значения с клавиатуры. Количество символов – 15 цифр. ПРИМЕЧАНИЕ. Если устройство поддерживает работу 2 SIM-карт, в поле допускается ввод любого из 2 значений IMEI	ПРИМЕЧАНИЕ. Если на устройствах под управлением ОС Аврора или ОС Android поле IMEI не заполнено, то после успешной активации значение IMEI отобразится в карточке устройства автоматически
Серийный номер	Ввести серийный номер, который присвоен устройству	

Параметр	Значения	Описание
	производителем. Может содержать от 1 до 20 символов	
Ethernet MAC	Ввести MAC-адрес Ethernet устройства, который состоит из 6 пар символов, разделенных двоеточием	
WLAN MAC	Ввести MAC-адрес WLAN устройства. Ввод значения с клавиатуры. Количество символов – 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	ПРИМЕЧАНИЕ. Если на устройстве под управлением ОС Аврора или ОС Android поле MAC WLAN не заполнено, то после успешной активации значение MAC WLAN отобразится в карточке устройства автоматически
Имя устройства	Ввод значения с клавиатуры. (Например, инвентарное имя устройства внутри компании). Может содержать от 1 до 16 символов	Поле не является обязательным для заполнения
Платформа	Выбор доступной платформы из списка: – Аврора; – Android; – Linux	Поле обязательно для заполнения
Модель устройства	Выбор модели устройства из раскрывающегося списка	Полное название типа устройств зависит от модели устройства
Комментарий	Ввод значения с клавиатуры. Максимальная длина – 512 символов	Поле не является обязательным для заполнения

2.2.1.2. Добавление и активация устройства в ПУ с помощью приглашения на самостоятельную регистрацию

С помощью приглашения возможно автоматически добавить новое устройство с любой из поддерживаемых ОС в ПУ и активировать его.

ВНИМАНИЕ! Повторная активация уже добавленного устройства в ПУ доступна в случаях если:

- устройство имеет статус «Очищено». В этом случае счетчик переактиваций для устройства (в день) не учитывается;
- задан счетчик переактиваций в приглашении, отличный от нуля, и если он для устройства не превышен, то можно использовать приглашение для переактивации устройства.

Для добавления и активации устройства в ПУ необходимо выполнить следующие действия:

- создать приглашение на самостоятельную регистрацию устройства (п. 2.2.4);
- установить приложение «Аврора Центр» на устройствах, описание которых приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7;
- не переименовывая приглашение (файл должен иметь название `invite.json`), разместить JSON-файл на устройство:
 - для ОС Аврора – `/etc/emm/`;
 - для ОС Android – `files/plugins_data/emm/`;
 - для ОС семейства Linux – `/etc/omp-uem-agent/`.

Далее на устройстве, в зависимости от версии ОС, выполнить следующие действия:

- для ОС Аврора/ОС Android, запустить приложение «Аврора Центр» и дождаться завершения процесса автодобавления и автоактивации устройства;
- для ОС семейства Linux дождаться завершения процесса автодобавления и автоактивации устройства (это может занять некоторое время) или перезапустить `daemon` клиента вручную с помощью команды:

```
sudo systemctl restart ru.omp.uem.service
```

В результате устройство будет добавлено и активировано в ПУ.

2.2.2. Добавление группы устройств вручную

При добавлении группы устройств в ручную доступно:

- добавление статической группы устройств (пп. 2.2.2.1);
- добавление динамической группы устройств (пп. 2.2.2.2).

2.2.2.1. Добавление статической группы устройств

ПРИМЕЧАНИЕ. Состав правил статической группы Администратор может редактировать вручную.

Для добавления статической группы необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить статическую группу» (см. Рисунок 50);
- в открывшемся окне (Рисунок 52) заполнить поля, приведенные в таблице (Таблица 27);
- подтвердить либо отменить действия.

В результате успешного добавления статической группы отобразится соответствующее сообщение и откроется карточка добавленной группы (п. 2.1.2).

Таблица 27

Параметры	Описание
Имя группы	Ввод значения с клавиатуры. Поле обязательно для заполнения. Название группы устройств должно быть уникальным
Комментарий	Ввод значения с клавиатуры. Максимальная длина – 512 символов. Поле с дополнительной информацией не является обязательным для заполнения

Рисунок 52

2.2.2.2. Добавление динамической группы устройств

Динамическая группа устройств — группа с заданными условиями, при соблюдении которых устройства попадают в группу автоматически.

Для добавления динамической группы необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить динамическую группу» (см. Рисунок 50);
- в открывшемся окне раздела «Название, комментарий» (Рисунок 53 [1]) заполнить поля, приведенные в таблице (см. Таблица 27);
- в области фильтров выбрать и задать значения параметров, приведенных в таблице (Таблица 28), по которым устройства будут добавлены в динамическую группу (Рисунок 53 [2]), и далее подтвердить действия, нажав кнопку «Создать».

ПРИМЕЧАНИЯ:

- ✓ Возможно задать несколько параметров для динамической группы. В этом случае в динамическую группу попадут устройства, которые удовлетворяют всем заданным критериям;

✓ Для одного набора параметров можно создать только одну динамическую группу.

В результате успешного создания динамической группы устройств отобразится соответствующее сообщение и откроется карточка добавленной группы (п. 2.1.2), которая будет включать все устройства, удовлетворяющие заданному критерию.

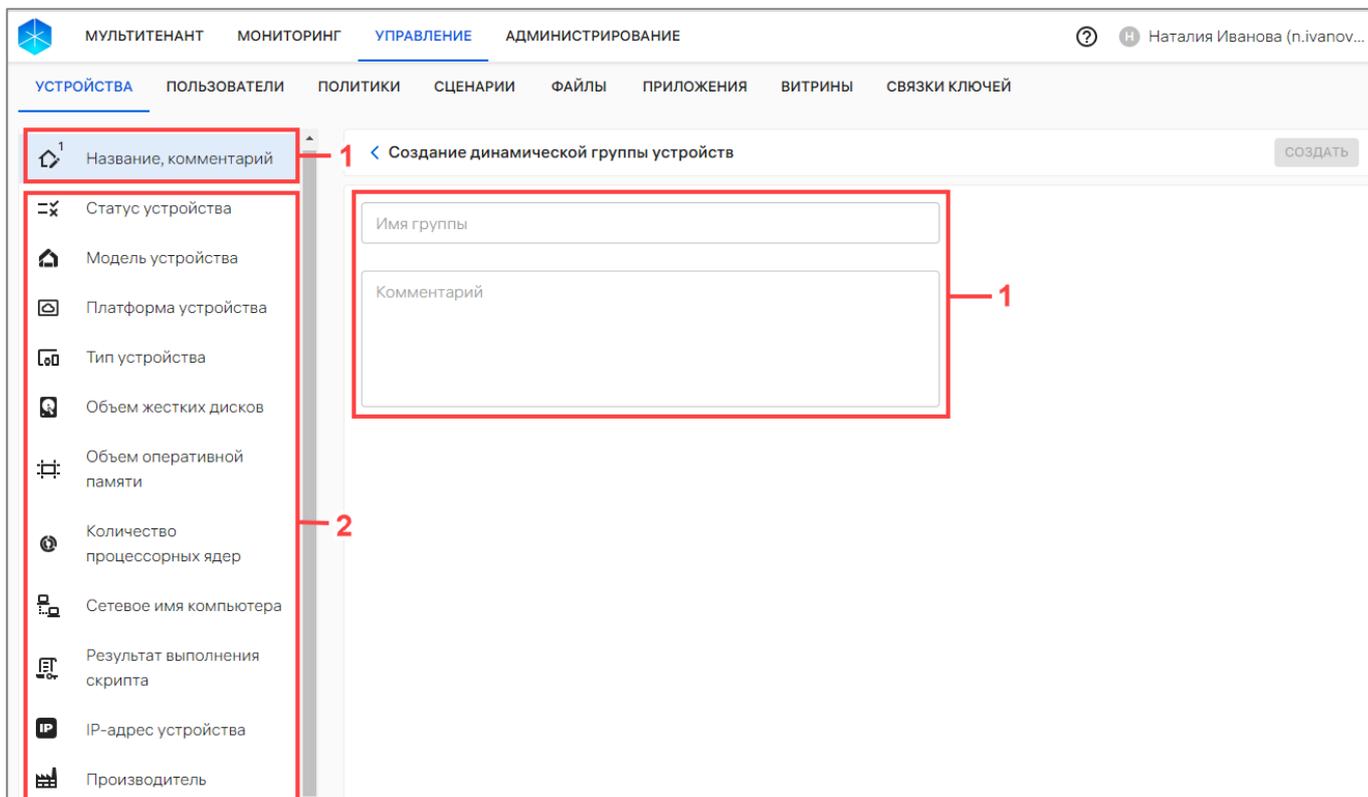


Рисунок 53

Таблица 28

Параметр	Значение
Статус устройства	Выбор значения из раскрывающегося списка: – «Активированные» – в динамическую группу будут автоматически попадать все активированные устройства; – «Не активированные» – в динамическую группу будут попадать все не активированные устройства
Модель устройства	Выбор модели устройства из раскрывающегося списка
Платформа устройства	Выбор значения из раскрывающегося списка: – Аврора; – Android; – Linux

Параметр	Значение
Тип устройства	Выбор типа устройства из раскрывающегося списка: – Планшет; – КПК; – Смартфон; – Неизвестный тип устройства; – ПК
Объем жестких дисков. ВНИМАНИЕ! Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать объем жесткого диска устройств в формате: – «От» (МиБ); – «До» (МиБ). ПРИМЕЧАНИЕ. Верхняя граница «До» не включается в интервал. При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок  «Удалить»
Объем оперативной памяти. ВНИМАНИЕ! Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать объем оперативной памяти устройств в формате: – «От» (МиБ); – «До» (МиБ). ПРИМЕЧАНИЕ. Верхняя граница «До» не включается в интервал. При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок  «Удалить»
Количество процессорных ядер. ВНИМАНИЕ! Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать количество процессорных ядер устройств в формате: – «От»; – «До». ПРИМЕЧАНИЕ. Верхняя граница «До» не включается в интервал. При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не

Параметр	Значение
	должны пересекаться. Для удаления диапазона нажать на значок  «Удалить»
Сетевое имя компьютера. ВНИМАНИЕ! Данный параметр актуален для устройств ОС семейства Linux	Ввести сетевое имя или маску сетевого имени компьютера, которое должно содержать хотя бы одну букву или цифру, и может включать буквы A-z, цифры 0-9, дефис (-), звездочки (*) и точки (.). Максимальная длина 253 символа, а длина от начала строки до первой точки не должна превышать 63 символа. Если необходимо ввести маску сетевого имени, необходимо ограничить ее звездочкой (*) в начале, внутри и/или в конце части сетевого имени. ПРИМЕЧАНИЕ. Возможно ввести несколько сетевых имен и/или масок сетевого имени компьютера
Результат выполнения скрипта. ВНИМАНИЕ! Данный параметр актуален для устройств ОС Android и ОС семейства Linux	Для ввода значений нажать кнопку «Скрипт». Заполнить поля: – «Путь к скрипту» – ввести путь скрипта, который будет выполнен на устройстве после доставки; – «Результат выполнения скрипта» – ввести ожидаемый результат выполнения скрипта. Результат выполнения скрипта передается, если в файл скрипта была добавлена переменная <code>OMP_SCRIPT_RESULT_FILE</code> . Более подробная информация представлена в приложении (Приложение 3). При необходимости можно добавить еще один скрипт, выполнив шаги приведенные выше. Для удаления скрипта из критерия нажать на значок  «Удалить»
IP-адрес устройства	Для ввода значений нажать кнопку «Диапазон». Указать интервал IP-адресов: – «Начальный адрес»; – «Конечный адрес». ПРИМЕЧАНИЕ. Конечный адрес не включается в интервал. При необходимости можно добавить еще один диапазон, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок  «Удалить»

Параметр	Значение
Производитель	Названия производителя устройства. Ввод значения с клавиатуры. ПРИМЕЧАНИЕ. Возможно ввести несколько производителей

2.2.3. Добавление устройств или группы устройств с помощью CSV-файла

Добавление и обновление устройств или групп устройств, а также привязка устройств к группе в Консоли администратора ПУ, может выполняться с помощью подготовленного шаблона импорта устройств, который предоставляется в виде CSV-файла.

2.2.3.1. Шаблон CSV-файла

CSV-файл возможно создать вручную или скачать и заполнить шаблон.

Для загрузки шаблона CSV-файла необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 50);

– в открывшемся окне нажать «Шаблон .CSV ↓» (Рисунок 54), в результате шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 29).

Импорт устройств из файла CSV

Имя импортируемого файла .csv —

Размер менее 400 МБ — Заголовки столбцов — [Подготовка файла для импорта](#)

Кодировка UTF-8 — Строки — [Настройки импорта на 1 шаге](#)

Формат CSV — Всего ошибок — **Шаблон .CSV**

Особые условия импортирования

Если ошибки в распознавании

Если наложение записей

Импорт устройств в группу

Выберите или перетащите в это окно заполненный файл с устройствами

ЗАГРУЗИТЬ ФАЙЛ

[ЗАКРЫТЬ](#)

Рисунок 54

Пример заполненного CSV-файла:

```
GROUP, IMEI, IMEI, SN, ETHERNET_MAC, WLAN_MAC, MODEL_CODE, PLATFORM, COMMENT, STRATEGY
Группа 1, 352132035783492, , , 6abcdg1, , , MIG C55, AURORA, Комментар 1
Группа 2, 350408012241197, , , 4gghdb6, , , MIG C55, AURORA, Комментар 2
```

АДМГ.20134-01 90 01-3

Также возможно заполнить CSV-файл в табличном виде (Рисунок 55).

Пример:

GROUP	IMEI	IMEI	SN	ETHERNET_MAC	WLAN_MAC	MODEL_CODE	PLATFORM	COMMENT	STRATEGY
Группа 1	352132035783492		6abcdg1			MIG C55	AURORA	Коммент 1	
Группа 2	350408012241197		4gghdb6			MIG C55	AURORA	Коммент 2	

Рисунок 55

ПРИМЕЧАНИЕ. При больших значениях чисел (например, IMEI) необходимо выбрать числовой формат ячейки и количество десятичных знаков, равное 0.

Файл для импорта должен соответствовать следующим требованиям:

- размер файла не должен превышать 400 МБ. Для импорта файлов большего размера рекомендуемая скорость подключения к сети Интернет 100 Мбит/сек и выше. Если скорость подключения к сети Интернет менее 100 Мбит/сек, рекомендуется разделить файл на несколько частей и загружать их поочередно;

- формат файла – .csv;
- кодировка файла – UTF-8.

ПРИМЕЧАНИЕ. Скачанный шаблон CSV-файла имеет нужный формат и кодировку;

- первая строка файла должна содержать названия полей с разделителем (например, "GROUP,IMEI,IMEI,SN,ETHERNET_MAC,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT,STRATEGY").

ПРИМЕЧАНИЕ. После столбца COMMENT может быть добавлен необязательный столбец STRATEGY. Он заполняется если необходимо указать стратегию для конкретной строки (пп. 2.2.3.2). Стратегия в строке может отличаться от основной выбранной и будет являться приоритетной.

Разделитель для всех полей файла определяется по первой строке. В качестве разделителей может использоваться любой символ, кроме: \r, \n и символа замены Unicode (0xFFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «а».

Описание требований к значениям параметров приведены в таблице (Таблица 29).

Таблица 29

Параметр	Описание	Примечание
GROUP	Название группы устройств. Содержит от 2 до 64 символов	Параметр обязателен для заполнения, при: – создании группы устройств; – привязке устройств к группе
IMEI	Международный идентификатор мобильного оборудования. Должен содержать 15 цифр	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы.

Параметр	Описание	Примечание
		ПРИМЕЧАНИЕ. Если на устройстве под управлением ОС Аврора или ОС Android поле IMEI не заполнено, то после успешной активации значение IMEI отобразится в карточке устройства автоматически
SN	Серийный номер, который присвоен устройству производителем. Содержит от 1 до 20 символов	Допустимо использовать только 1 такой параметр. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
ETHERNET_MAC	MAC-адрес Ethernet устройства. Содержит 6 пар символов, разделенных двоеточием	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
WLAN_MAC	MAC-адрес WLAN устройства. Содержит 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы. ПРИМЕЧАНИЕ. Если на устройстве под управлением ОС Аврора или ОС Android поле MAC WLAN не заполнено, то после успешной активации значение MAC WLAN отобразится в карточке устройства автоматически
MODEL_CODE	Модель устройства. Содержит до 255 символов	Параметр не обязателен для заполнения
PLATFORM	ОС устройства. Доступные значения: – AURORA; – ANDROID; – LINUX	Параметр обязателен для заполнения
COMMENT	Дополнительная информация к устройству. Содержит до 512 символов	Параметр не обязателен для заполнения

Параметр	Описание	Примечание
STRATEGY	<p>Правило разрешения конфликтующих записей.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> – SKIP или S – в результате конфликтующая запись не будет перезаписана. Если файл содержит несколько одинаковых записей об устройстве, но с разными группами, то будут созданы все связи устройств с группами из файла; – REPLACE или R – в результате конфликтующая запись будет перезаписана. Если файл содержит несколько одинаковых записей об устройствах, но с разными группами, то устройство будет отвяно от всех групп, в которых оно состояло ранее в системе и привязано ко всем группам из файла 	<p>Параметр не обязателен для заполнения.</p> <p>Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта</p>

2.2.3.2. Добавление устройства или группы устройств с помощью CSV-файла

Для импорта устройств, их группы и связи с группами в Консоли администратора ПУ необходимо выполнить следующие действия:

- подготовить CSV-файл для импорта (пп. 2.2.3.1);
- перейти в подраздел «Устройства» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 50);
- в открывшемся окне задать особые условия импорта, приведенные в таблице (Таблица 30);

Таблица 30

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из	В поле содержится подсказка, доступная для

Наименование полей	Описание	Примечание
	<p>раскрывающегося списка (Рисунок 56 [1]):</p> <ul style="list-style-type: none"> – Прекратить импорт и вернуть файл с описанием ошибок – при обнаружении ошибок будет остановлен импорт и сформирован файл с перечислением некорректных строк и указанием причин ошибок; – Продолжить импорт и вернуть два файла с ошибками и без – импорт продолжится с корректными записями, и после его завершения будут сформированы 2 файла: <ul style="list-style-type: none"> • файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств 	<p>просмотра нажатием значка . В результате отобразится текст подсказки следующего содержания: «При завершении импорта система предоставит 2 файла: список системных сообщений об ошибках распознавания и Журнал успешно импортированных устройств»</p>
Если наложение записей	<p>Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 56 [2]):</p> <ul style="list-style-type: none"> – Игнорировать новую запись, оставить старую – в результате конфликтующие записи не будут перезаписаны. Если файл содержит несколько одинаковых записей об устройствах, но с разными группами, то будут созданы все связи устройств с группами из файла; – Перезаписывать новую строку поверх прежней – в результате конфликтующие записи будут перезаписаны. Если файл содержит несколько одинаковых записей об устройстве, но с разными группами, то устройство будет отвязано от всех групп, в которых оно состояло, и привязано ко всем группам из файла. 	

Наименование полей	Описание	Примечание
	<p>ПРИМЕЧАНИЕ. Если в CSV-файле заполнен столбец «STRATEGY», правило разрешения конфликтов из этого столбца будет иметь приоритет над указанным правилом при настройке импорта. Процесс заполнения CSV-файла приведен в пп. 2.2.3.1</p>	
Импорт устройств в группу	<p>Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 56 [3]):</p> <ul style="list-style-type: none"> – Автоматически создать новую группу с временем и датой импорта – в результате будет создана новая группа устройств (с типом <input type="checkbox"/> «Группа устройств»), в которую будут включены все импортируемые устройства. Если в CSV-файле указана группа (значение в столбце «GROUP»), то такое устройство будет включено в новую группу и в указанную в файле группу; – Не создавать группу – в результате устройства будут добавлены только в группы, указанные в CSV-файле; – Выбрать группу из имеющихся – требуется выбрать из раскрывающегося списка группу, в которую необходимо включить устройство. Если в CSV-файле указана группа (значение в столбце «GROUP»), то устройство будет включено как в группу, указанную в файле, так и в группу, выбранную на этом шаге 	<p>В поле содержится подсказка, доступная для просмотра нажатием значка . В результате отобразится текст подсказки следующего содержания: «В процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую»</p>

Импорт устройств из файла CSV

Имя импортируемого файла .csv —

Размер менее 400 МБ — Заголовки столбцов — [Подготовка файла для импорта](#)

Кодировка UTF-8 — Строки — [Настройки импорта на 1 шаге](#)

Формат CSV — Всего ошибок — [Шаблон .CSV](#)

Особые условия импортирования

Если ошибки в распознавании Прекратить импорт и вернуть файл с описанием ошибок — 1

Если наложение записей Игнорировать новую запись, оставить старую — 2

Импорт устройств в группу Автоматически создать новую группу с временем и датой импорта — 3

Выберите или перетащите в это окно
заполненный файл с устройствами

ЗАГРУЗИТЬ ФАЙЛ — 4

[ЗАКРЫТЬ](#)

Рисунок 56

- далее необходимо загрузить CSV-файл одним из способов:
 - переместить CSV-файл в область загрузки;
 - нажать кнопку «Загрузить файл» (см. Рисунок 56 [4]) с последующим выбором файла для импорта;
- в результате будет запущен импорт устройств из CSV-файла и отобразится шкала загрузки импорта.

Если заполненный файл был загружен корректно или файл содержал ошибки, но при этом в особых условиях импортирования была выбрана опция «Продолжить импорт и вернуть 2 файла с ошибками и без», импорт будет завершен. В окне с результатами импорта шкала загрузки импорта будет заполнена до конца (Рисунок 57).

Импорт устройств из файла CSV

Имя импортируемого файла .csv devices.csv

Размер менее 400 МБ Заголовки столбцов 6 [Подготовка файла для импорта](#)

Кодировка UTF-8 Строки 2 [Настройки импорта на 1 шаге](#)

Формат CSV Всего ошибок 0 [Шаблон .CSV](#)

Особые условия импортирования

Если ошибки в распознавании Прекратить импорт и вернуть файл с описанием ошибок

Если наложение записей Игнорировать новую запись, оставить старую

Импорт устройств в группу Автоматически создать новую группу с времен... Группа: [import_device Aug 26 13:22:50](#)

Импорт завершен

Ошибок не найдено

Устройств создано 2 Список импортированных устройств [ValidDevices \(.csv, 307 Байт\)](#)

Групп из файла создано 2 Список строк с ошибками —

Связей с группами из файла создано 2 Общий отчёт об импорте [ImportReport \(.rtf, 27,12 КБ\)](#)

[ЗАКРЫТЬ](#)

Рисунок 57

Если заполненный файл был загружен некорректно и при этом в особых условиях импортирования была выбрана опция «Прекратить импорт и вернуть файл с описанием ошибок», импорт будет остановлен. В окне с результатами импорта шкала загрузки импорта устройств будет прервана на этапе, где были обнаружены ошибки (Рисунок 58 [6]).



Рисунок 58

В окне с результатами импорта устройств отображается следующая информация:

- название импортируемого файла (см. Рисунок 58 [1]);
- соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 58 [2]);
- количество столбцов всех импортируемых строк и ошибок в файле (Рисунок 58 [3]);
- ссылки (см. Рисунок 58 [4]):
 - **Подготовка файла для импорта**, при нажатии на которую произойдет переход на статью справки, описывающую требования и процесс подготовки CSV-файла для импорта устройств;
 - **Настройки импорта на 1 шаге**, при нажатии на которую произойдет переход на статью справки, описывающую шаги импорта;
 - **Шаблон .CSV**, при нажатии на которую произойдет скачивание шаблона CSV-файла для импорта устройств;
- особые условия импортирования (см. Рисунок 58 [5], см. Таблица 30);
- шкала прогресса импорта (см. Рисунок 58 [6]);

- сообщение о завершении импорта или прерывании процесса из-за ошибок (см. Рисунок 58 [7]);
- графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (см. Рисунок 58 [8]);
- количество добавленных устройств, групп устройств и их связей (см. Рисунок 58 [9]);
- ссылки на скачивание отчетов (см. Рисунок 58 [10]):
 - отчет со списком импортированных устройств. Формат отчета – .csv;
 - отчет со списком ошибок, описание которых приведено в подразделе 5.2. Формат отчета – .csv (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);
 - отчет с общей информацией об импорте. Формат отчета – .rtf.

Отследить процесс выполнения импорта также возможно в окне «Процессы» подраздела «Индикаторы» раздела «Мониторинг». Более подробная информация приведена в подразделе 3.

Для повторной загрузки CSV-файла необходимо нажать кнопку «К началу загрузки».

2.2.4. Добавление приглашения на самостоятельную регистрацию устройства

Для добавления приглашения на самостоятельную регистрацию устройства необходимо перейти в подраздел «Устройства» раздела «Управление» и выполнить одно из следующих действий:

1) Нажать кнопку «Добавить», в раскрывающемся списке выбрать пункт «Добавить приглашение» (см. Рисунок 50);

2) Перейти в список приглашений, нажав на кнопку «Приглашения» (Рисунок 59), и на отобразившейся странице нажать на кнопку «Добавить приглашение» (Рисунок 60).

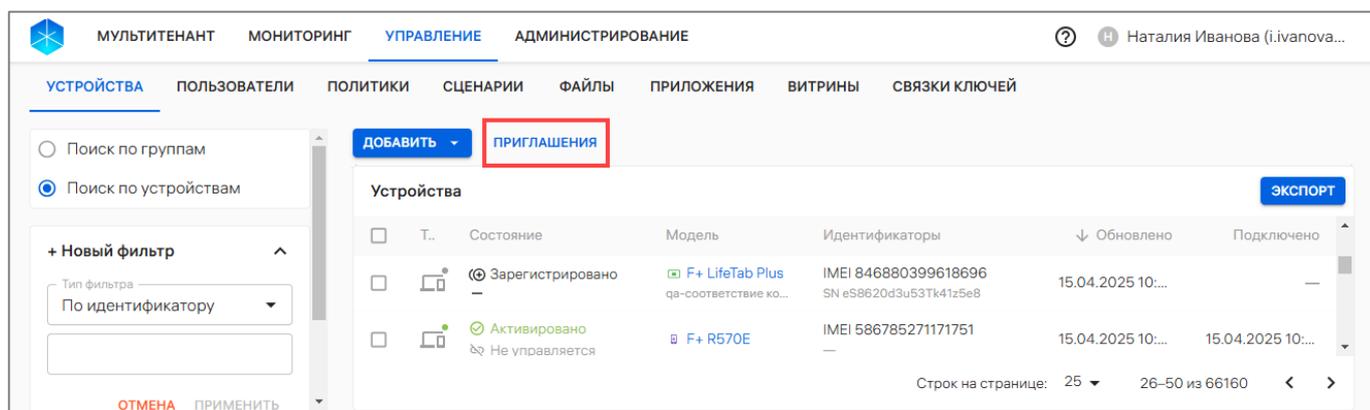


Рисунок 59

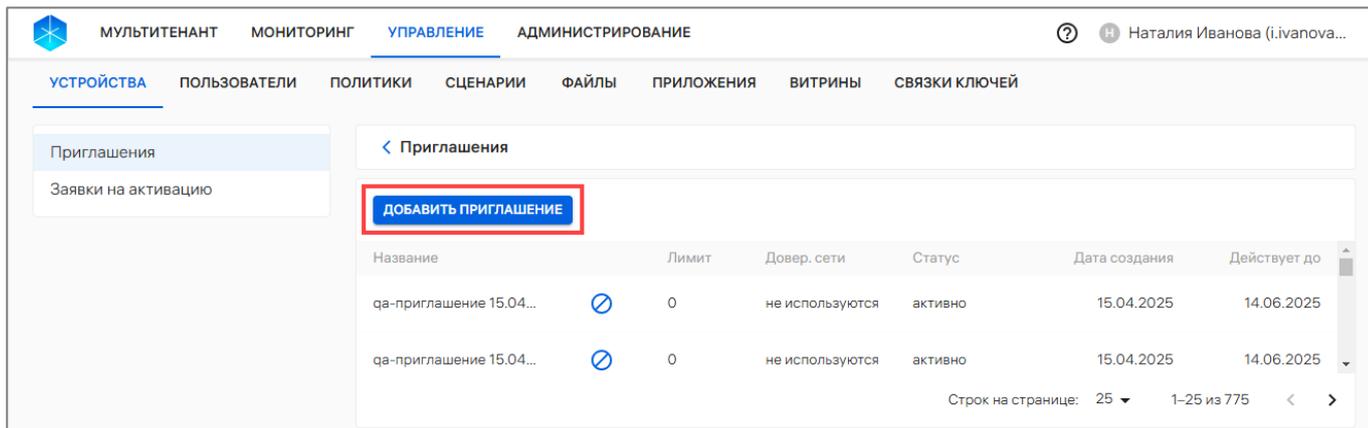


Рисунок 60

В результате в отображившемся окне необходимо заполнить поля:

- «Название» (Рисунок 61 [1]). Ввод значения с клавиатуры. Может содержать от 1 до 50 символов;

- «Лимит переиспользований в сутки» (Рисунок 61 [2]). Ввести максимальное количество переиспользований приглашения для повторной активации устройства в сутки. Количество переиспользований считается для одного устройства и если оно превысит заданный лимит, то повторная активация устройства с помощью приглашения в текущие сутки не сработает. На следующие сутки счетчик переактиваций для устройства сбрасывается. Лимит может быть от 0 до 1000000. В случае 0 использовать приглашение для повторной активации устройства будет нельзя;

- если требуется отправлять на рассмотрение устройства из сетей, не входящих в список доверенных, необходимо перевести переключатель «Использовать доверенные сети» (Рисунок 61 [3]) в положение «Включено». По ссылке «Подробнее» доступен переход в статью справки.

Рисунок 61

ПРИМЕЧАНИЕ. Для ОС Android в приглашении на самостоятельную регистрацию устройств возможно дополнительно указать:

1) Сеть WLAN (Рисунок 62), к которой устройство автоматически подключится в процессе самостоятельной регистрации. Для этого необходимо:

- перевести переключатель «Настройки WLAN» в положение «Включен»;
- в поле «Название сети (SSID)» ввести название беспроводной сети (Service Set Identifier) для подключения. Параметр обязателен для заполнения;
- с помощью переключателя «Скрытая сеть» указать транслируется ли название сети WLAN. Переключатель по умолчанию выключен;
- в раскрывающемся списке «Безопасность» необходимо выбрать технологию безопасности сети WLAN:

- WEP (выбрано по умолчанию);
- WPA;

– в поле «Пароль» ввести пароль сети WLAN. Параметр обязателен для заполнения;

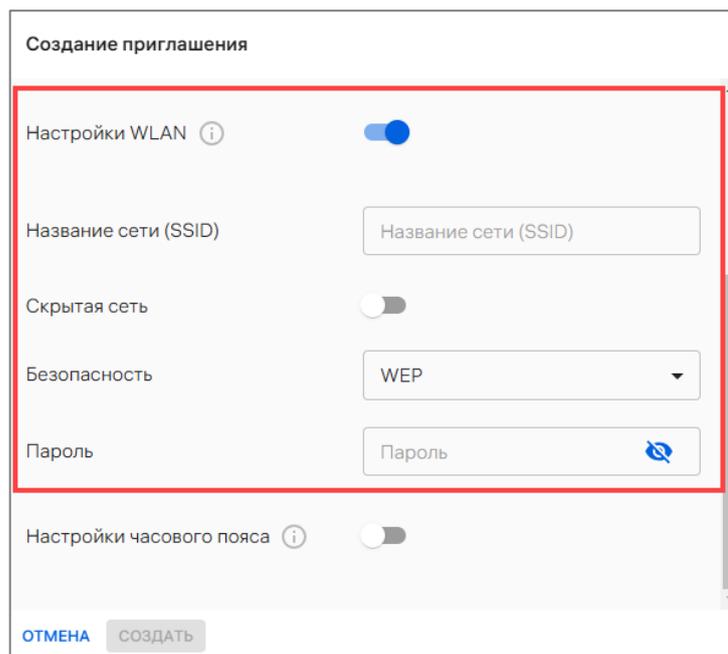


Рисунок 62

2) Часовой пояс (Рисунок 63), который автоматически будет установлен на устройстве в процессе самостоятельной регистрации. Для этого необходимо:

- перевести переключатель «Настройки часового пояса» в положение «Включен»;
- в раскрывающемся списке «Часовой пояс» выбрать нужный часовой пояс. По умолчанию выбран часовой пояс Москва (GMT+03:00).

Создание приглашения

Скрытая сеть

Безопасность WEP

Пароль

Настройки часового пояса

Часовой пояс Москва (GMT+03:00)

ОТМЕНА СОЗДАТЬ

Рисунок 63

После выполнения указанных действий необходимо подтвердить или отменить действие.

Если приглашение успешно создано, отобразится карточка приглашения, на которой будут отображены:

- лимит переиспользований приглашения в сутки (Рисунок 64 [1]);
- использование доверенных сетей (Рисунок 64 [2]);
- QR-код (Рисунок 64 [3]), который необходимо отсканировать на устройстве с ОС Аврора/ОС Android для дальнейшей самостоятельной регистрации устройства (также доступно скачивание QR-кода при нажатии на значок  при наведении на него курсора);

- кнопка «Скачать JSON» (Рисунок 64 [4]), при нажатии на которую будет скачен JSON-файл для дальнейшего размещения его на устройство для самостоятельной регистрации в ПУ (пп. 2.2.1.2);

- кнопка «Закрыть» (Рисунок 64 [5]), при нажатии на которую отобразится предупреждающее сообщение (Рисунок 65), где необходимо подтвердить или отменить действие.

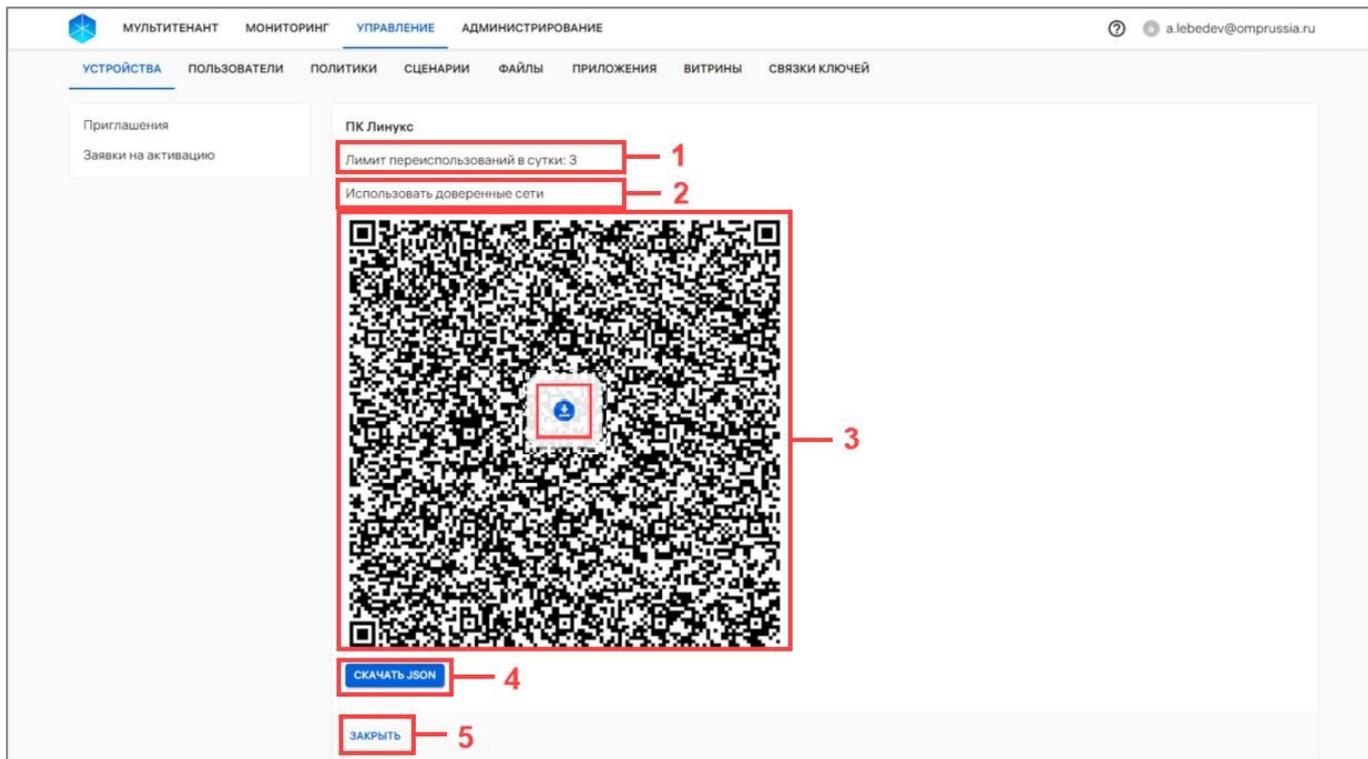


Рисунок 64

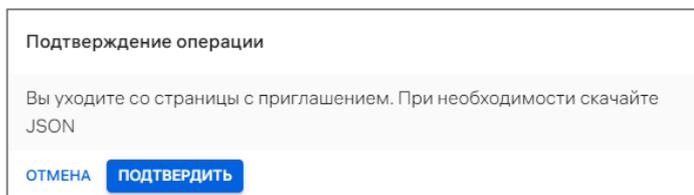


Рисунок 65

Приглашение имеет название `invite.json`.

Пример содержания JSON-файла:

```
{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "accessToken": "g8jOjd812DeMt6ZPqk8GTDF0", "inviteTakeupURL": "http://ocs-dev.omprussia.ru/emm/mobile/api/deviceInvites/f1512c/takeUp", "trustedCertificates": "" }, "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "ru.omp.services.ru.omp.services.AdminReceiver", "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "http://ocs-dev.omprussia.ru/emm/mobile/clientDownload", "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "bZ41Av7s6nrQpXjB2Pg5oKfKL5xPxhLevsESkkVLfg4", "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": true, "android.app.extra.PROVISIONING_WIFI_SSID": "Wi-Fi", "android.app.extra.PROVISIONING_WIFI_PASSWORD": "123456789", "android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE": "WPA", "android.app.extra.PROVISIONING_TIME_ZONE": "Europe/Moscow" }
```

ВНИМАНИЕ!

✓ Пример приведен для ознакомления со структурой JSON-файла и может отличаться;

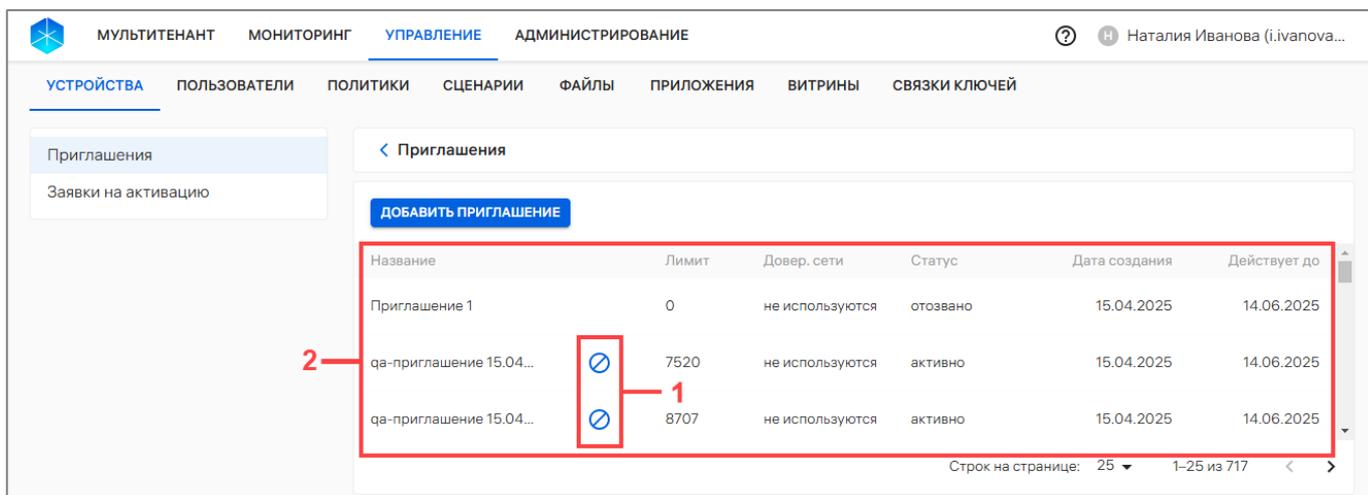
✓ Не рекомендуется изменять название и форматировать сгенерированный JSON-файл (добавлять пробелы, табуляцию, переносы строк), так как это может привести к ошибкам при обработке JSON- файла в процессе добавления и активации устройств по приглашению.

Каждый параметр сопровождается двоеточием, пары ключ-значение разделяются запятой. Описание параметров из примера:

- **accessToken** – токен доступа;
- **inviteTakeURL** – URL, по которому устройство перейдет для начала процесса самостоятельной регистрации;
- **trustedCerts** – список цифровых отпечатков (*fingerprint*) корневых сертификатов для активации устройств, перечисленные через запятую;
- **android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME** – название компонента;
- **android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION** – ссылка на скачивание файла для установки приложения «Аврора Центр»;
- **android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM** – контрольная сумма подписи файла для установки приложения «Аврора Центр»;
- **android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED** – параметр, определяющий, включать ли полную установку системных приложений в процессе установки первоначальной настройки устройства с установкой приложения «Аврора Центр». По умолчанию установка всех системных приложений включена;
- **android.app.extra.PROVISIONING_WIFI_SSID** – название сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;
- **android.app.extra.PROVISIONING_WIFI_PASSWORD** – пароль сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;
- **android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE** – технология безопасности сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;
- **android.app.extra.PROVISIONING_WIFI_HIDDEN** – параметр, определяющий транслируется ли название сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;
- **android.app.extra.PROVISIONING_TIME_ZONE** – часовой пояс, который автоматически будет установлен на устройстве в процессе самостоятельной регистрации.

При выходе из карточки приглашения осуществится переход на страницу со списком приглашений в подразделе «Приглашения», на которой доступно отозвать созданное приглашение, нажав на значок  «Отозвать» (Рисунок 66 [1]), а также возможно просмотреть информацию о каждом приглашении, которая отображается в следующих столбцах (Рисунок 66 [2]):

- «Название» – название приглашения;
- «Лимит» – лимит переиспользований приглашения в сутки;
- «Довер.сети» – использование доверенных для проверки IP-адреса устройства. Возможные значения:
 - «Используются»;
 - «Не используются»;
- «Статус» – статус активности приглашения. Возможные значения:
 - «Активно»;
 - «Приостановлено»;
 - «Отозвано»;
- «Дата создания» – дата создания приглашения;
- «Действует до» – дата, до которой действует токен доступа, соответствующий приглашению.



Название	Лимит	Довер.сети	Статус	Дата создания	Действует до
Приглашение 1	0	не используются	отозвано	15.04.2025	14.06.2025
qa-приглашение 15.04...	7520	не используются	активно	15.04.2025	14.06.2025
qa-приглашение 15.04...	8707	не используются	активно	15.04.2025	14.06.2025

Рисунок 66

2.2.5. Заявки на активацию

Для просмотра списка заявок на активацию устройств по приглашению необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- нажать на кнопку «Приглашения» (см. Рисунок 59);
- перейти в раздел «Заявки на активацию» (Рисунок 67 [1]);
- в рабочей области отобразится список заявок на активацию (Рисунок 67 [3]).

Информация о заявках отображается в столбцах, приведенных в таблице (Таблица 31), и отсортирована по значениям столбца «Дата создания» в порядке убывания.

ПРИМЕЧАНИЕ. По умолчанию список заявок на активацию отображается в статусе «Требуется согласования» (Рисунок 67 [2]). Для отображения списка заявок на активацию во всех статусах, нажать кнопку «Сбросить все». Далее в раскрывающемся списке «Тип фильтра» выбрать «Статус заявки» и выбрать нужный статус:

- «Требуется согласования»;
- «Согласована»;
- «Отклонена».

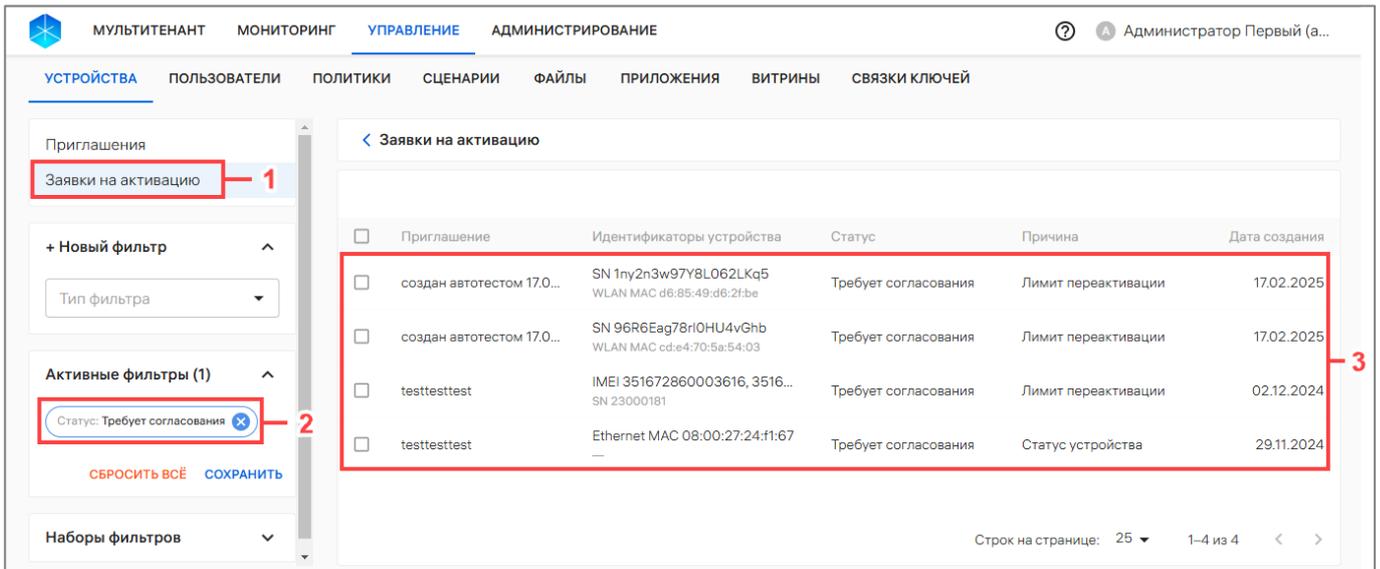


Рисунок 67

Таблица 31

Название столбца	Описание
Приглашение	Название приглашения
Идентификаторы устройства	Отображаются два имеющихся идентификатора устройства по приоритетам, выставленным в настройках администрирования ПУ (подробнее в п. 4.1.3)
Статус	Статус заявки на активацию. Возможные значения: <ul style="list-style-type: none"> – «Требуется согласования»; – «Согласована»; – «Отклонена»; – «Выполнена»
Причина	Статус создания заявки. Возможные значения: <ul style="list-style-type: none"> – «Лимит переактивации»; – «Доверенная сеть». Дополнительно отображается IPv4-адрес, который передало устройство при использовании приглашения. ПРИМЕЧАНИЕ. Содержит значение, определяемое инфраструктурой, поэтому при неверной настройке инфраструктуры может содержать произвольное значение;

Название столбца	Описание
	– «Статус устройства»; – «Вручную»
Дата создания	Дата создания заявки на активацию

Чтобы согласовать или отклонить заявки на активацию по приглашению, необходимо:

– выбрать нужную заявку в списке, установив галочку в чекбоксе для доступа к списку быстрых действий. Для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 68 [1]);

– в списке быстрых действий выбрать значок (Рисунок 68 [2]):

- «Согласовать» - для согласования заявки;
- «Отклонить» - для отклонения заявки;

ПИМЕЧАНИЯ:

✓ Согласовать заявки возможно только в статусах «Требуется согласования» и «Отклонена»;

✓ Отклонить заявки возможно только в статусах «Требуется согласования» и «Согласована»;

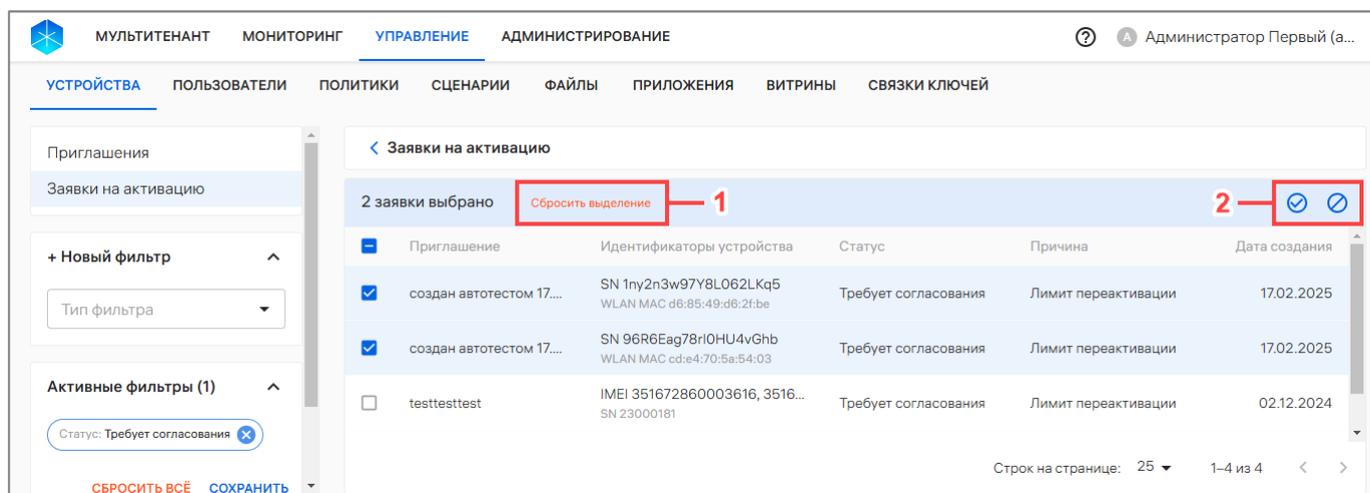


Рисунок 68

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 69).

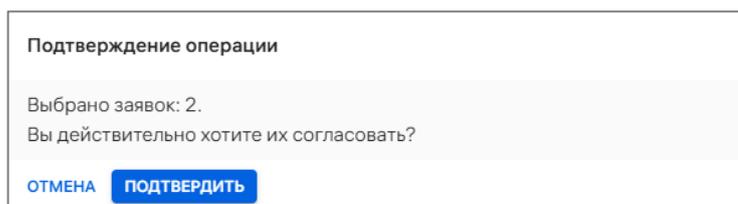


Рисунок 69

В результате успешного подтверждения, заявки будут согласованы или отклонены.

2.2.6. Экспорт списка устройств в CSV-файл

Для экспорта списка устройств в файл формата `.csv` необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- выбрать в области фильтров «Поиск по устройствам»;
- нажать кнопку «Экспорт» (Рисунок 70);

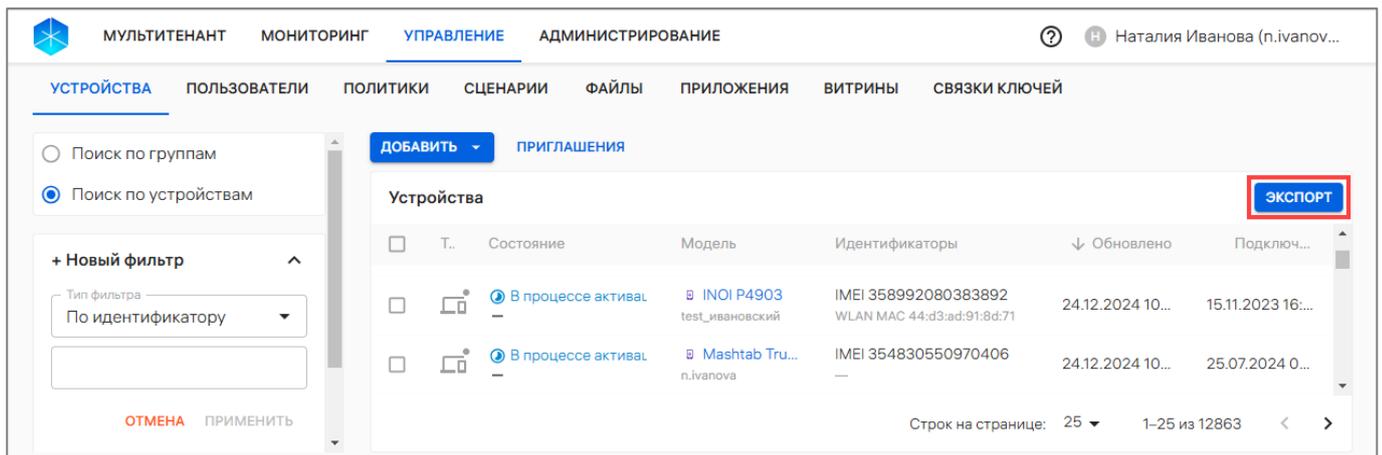


Рисунок 70

– в отобразившемся окне подтверждения экспорта устройств подтвердить либо отменить действия (Рисунок 71).

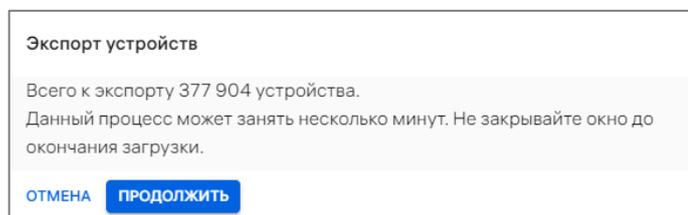


Рисунок 71

В результате подтверждения действия начнется процесс экспорта, который может занять несколько минут, после чего на ЭВМ будет скачан файл формата `.csv` с результатами экспорта.

Файл с результатами экспорта содержит следующие параметры устройств, разделенные запятой:

- **imeis** – международный идентификатор мобильного оборудования (состоит из 15 цифр). Если у устройства несколько IMEI, то они будут перечислены через точку с запятой;
- **sn** – серийный номер, который присвоен устройству производителем;
- **ethernetMACs** – MAC-адрес Ethernet устройства. Состоит из 6 пар символов, разделенных двоеточием. Если у устройства несколько MAC-адресов Ethernet, то они будут перечислены через точку с запятой;

АДМГ.20134-01 90 01-3

– **wifiMACs** – MAC-адрес WLAN устройства. Состоит из 6 пар символов, разделенных двоеточием. Если у устройства несколько MAC-адресов WLAN, то они будут перечислены через точку с запятой;

– **modelName** – модель устройства;

– **platform** – ОС устройства;

– **status** – статус жизненного цикла устройства;

– **compliance** – соответствие устройства назначенной политике;

– **comment** – комментарий к устройству;

– **createdAt** – дата и время добавления устройства в Аврора Центр;

– **connectedAt** – дата и время последнего подключения устройства к Аврора Центр;

– **deviceGroups** – название группы, в которую входит устройство. Параметр заключен в кавычки. Если устройство входит в несколько групп, их названия будут перечислены через точку с запятой.

ВНИМАНИЕ! Одни и те же группы могут быть перечислены в разном порядке в разных строках. Для успешной работы с экспортированным CSV-файлом необходимо ознакомиться с рекомендацией, приведенной в приложении (Приложение 2).

2.2.7. Привязка устройства к пользователю

В Консоли администратора ПУ предусмотрена возможность привязки устройств к пользователю, которая может быть выполнена:

– с помощью быстрых действий в списке устройств (пп. 2.2.7.1);

– с помощью быстрых действий в списке пользователей (пп. 2.3.5.1);

– вручную через карточку устройства (пп. 2.2.7.2);

– вручную через карточку пользователя (пп. 2.3.5.2);

– с помощью импорта CSV-файла (п. 2.2.3).

При привязке устройства к пользователю на устройстве будут действовать все офлайн-сценарии и политики, назначенные на группу пользователя либо скомбинированная политика, если политики были назначены на группу устройств, в которую входит устройство.

ПРИМЕЧАНИЕ. Перед привязкой устройства, необходимо убедиться, что добавлен хотя бы 1 пользователь. Процесс добавления пользователя приведен в п. 2.3.1 – 2.3.3.

2.2.7.1. Привязка устройства к пользователю с помощью списка быстрых действий

Для привязки устройства к пользователю с помощью списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 72 [1]);

– в списке быстрых действий выбрать значок  «Привязать устройства к пользователям» (Рисунок 72 [2]);

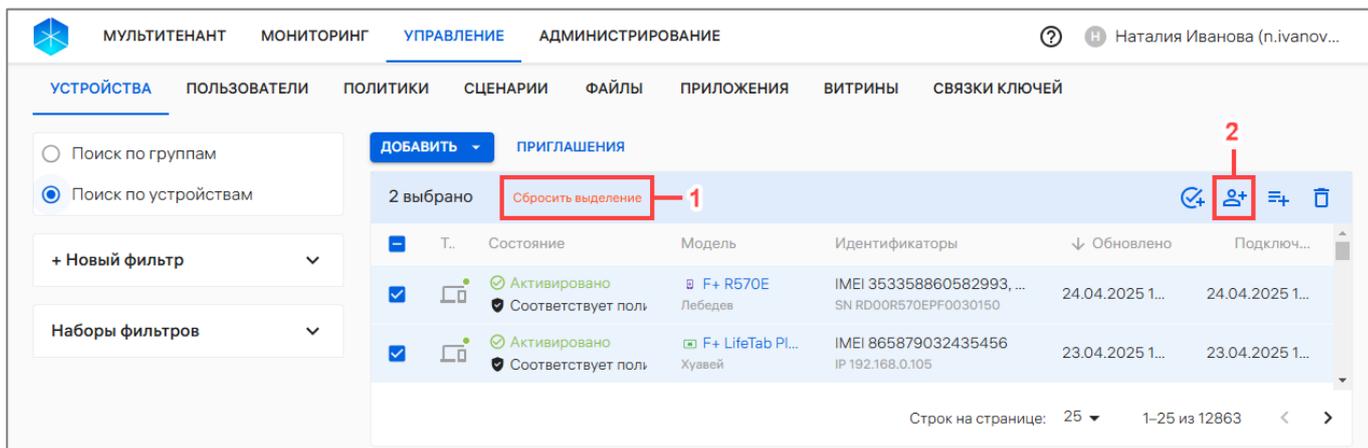


Рисунок 72

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте либо телефону пользователя (Рисунок 73 [1]). Далее, при необходимости, возможно добавить дополнительного пользователя, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также, возможно удалить из списка выбранных пользователей, нажав значок  «Убрать из списка» справа от пользователя (Рисунок 73 [3]);

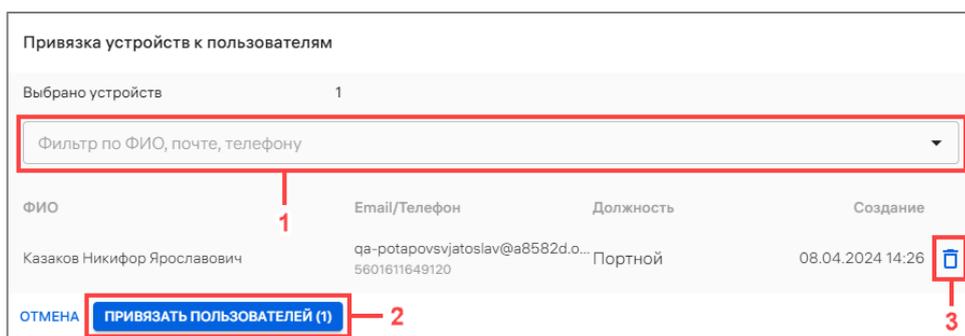


Рисунок 73

– нажать кнопку «Привязать пользователей» (см. Рисунок 73 [2]).

В результате успешной привязки пользователей к устройству отобразится соответствующее сообщение.

Если на группу, в которую включен пользователь, назначена политика и/или офлайн-сценарий, они начнут действовать на привязанном устройстве (если оно активировано).

2.2.7.2. Привязка устройства к пользователю из карточки устройства

Для привязки устройства к пользователю из карточки устройства необходимо выполнить следующие действия:

АДМГ.20134-01 90 01-3

- перейти в подраздел «Устройства» раздела «Управление»;
- выбрать в области фильтров «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку устройства, при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке устройства перейти во вкладку «Пользователи»;
- нажать кнопку «Привязать пользователей» (см. Рисунок 16 [2]);
- в отобразившемся окне (см. Рисунок 73) выполнить действия, описанные в пп. 2.2.7.1.

2.2.8. Привязка устройств к группе устройств

В Консоли администратора ПУ предусмотрены 2 типа групп устройств:

–  динамическая – группа с заданными условиями, при соблюдении которых устройства автоматически попадают в группу. Например, в динамическую группу активированных устройств попадают все устройства, успешно прошедшие активацию. Редактирование или удаление динамической группы невозможно;

–  статическая – группа, созданная Администратором Платформы управления. Состав группы изменяется Администратором Платформы управления.

Осуществить привязку устройств к статической группе можно с помощью:

- списка быстрых действий (пп. 2.2.8.1);
- карточки устройства (пп. 2.2.8.2);
- карточки группы устройств (пп. 2.2.8.3);
- заполненного CSV-файла в соответствии с пп. 2.2.3.1. После добавления устройств в группу с помощью импорта CSV-файла на устройства будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

Перед привязкой устройств необходимо убедиться, что добавлена хотя бы 1 группа устройств (п. 2.2.2).

2.2.8.1. Привязка устройств к группе устройств с помощью списка быстрых действий

Для привязки устройств к группе устройств с помощью списка быстрых действий необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- выбрать устройства в списке устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 74 [1]);
- в списке быстрых действий выбрать значок  «Привязать устройства к группам» (Рисунок 74 [2]);

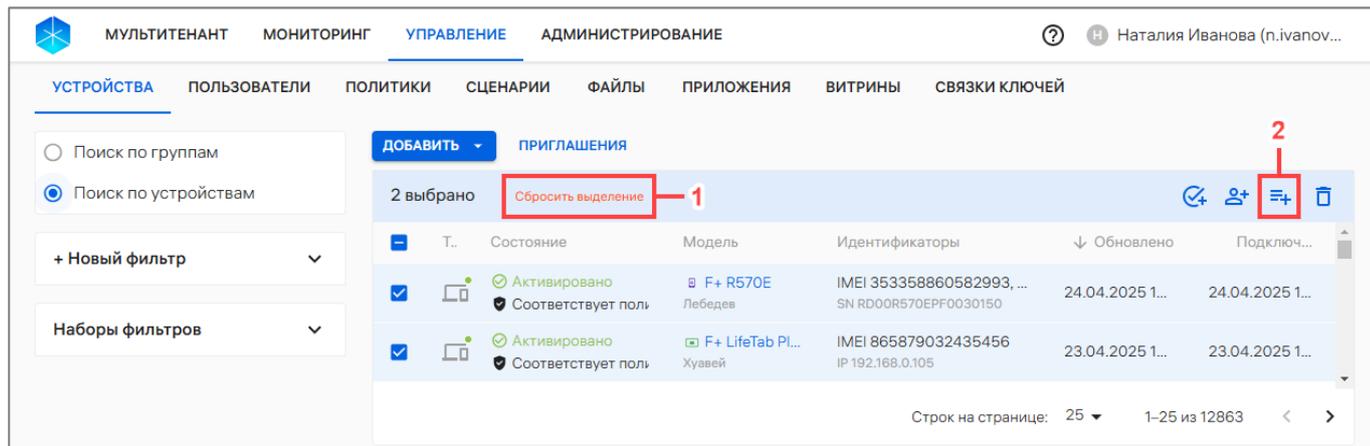


Рисунок 74

– в отобразившемся окне выбрать необходимую группу устройств из раскрывающегося списка (Рисунок 75 [1]) или воспользоваться фильтром. Далее, при необходимости, возможно добавить дополнительную группу, выбрав ее из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранную группу, нажав на значок  «Убрать из списка» (Рисунок 75 [3]);



Рисунок 75

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 76 [1]) и нажав кнопку «Создать статическую группу» (Рисунок 76 [2]);



Рисунок 76

– нажать кнопку «Добавить в группы» (см. Рисунок 75 [2]).

В результате успешной привязки устройства к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. На активированные устройства будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.8.2. Привязка устройств к группе устройств из карточки устройств

Для привязки устройств к группе из карточки устройств необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке устройства перейти во вкладку «Группы»;
- нажать кнопку «Добавить в группы» (см. Рисунок 17 [2]);
- в открывшемся окне необходимо выполнить действия, описанные в пп. 2.2.8.1.

В результате успешной привязки устройства к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. На активированном устройстве будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.8.3. Привязка устройств к группе устройств из карточки группы устройств

Для привязки устройств к группе устройств из карточки группы устройств необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке группы устройств перейти во вкладку «Устройства»;
- нажать кнопку «Привязать устройства» (см. Рисунок 31 [2]);
- в отобразившемся окне выполнить действия, описанные в пп. 2.2.8.1.

В результате на активированных устройствах будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.9. Активация устройств

Для активации устройств в Консоли администратора ПУ необходимо сгенерировать QR-код, после чего статус устройств с параметра «Жизненный цикл» поменяется на «В процессе активации». Для устройств во всех статусах доступна повторная генерация QR-кода (повторная активация).

При успешной активации на устройстве назначаются все политики, назначенные на:

- группы устройств, в которые входит устройство;
- на группу пользователей, к которым привязано устройство.

АДМГ.20134-01 90 01-3

Если при активации устройства на него не были назначены политики, устройство в параметре «Жизненный цикл» примет значение «Активировано», а в параметре «Политики» – статус  «Не управляется» и передаст свое состояние Консоли администратора ПУ.

Настроенные для работы устройства в параметре «Политики» имеют следующие статусы:

-  «Не управляется»;
-  «Соответствует политике»;
-  «Не соответствует политике».

Порядок настройки устройств для работы с ПУ приведен в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

Активация устройств возможна следующими способами:

- вручную (пп. 2.2.9.1), если необходимо самостоятельно активировать 1 устройство;
- с помощью списка быстрых действий (пп. 2.2.9.2), если необходимо активировать несколько устройств;
- с помощью отправки QR-кода на Email (пп. 2.2.9.3), если необходимо, чтобы пользователи активировали свои устройства самостоятельно;
- с помощью загрузки JSON-файла (пп. 2.2.9.4), если необходимо активировать все устройства группы одним QR-кодом;
- с помощью приглашения на самостоятельную регистрацию устройства (пп. 2.2.1.2);
- при первом включении устройства (ускоренная активация), если для устройства были выполнены все условия ускоренной активации. Подробное описание процесса ускоренной активации на устройстве приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

2.2.9.1. Активация устройств вручную

Активация устройств вручную возможна из карточки устройства. Для этого необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в карточке устройства нажать кнопку «Активировать» (Рисунок 77).

ПРИМЕЧАНИЕ. При повторной генерации использовать предыдущий QR-код будет невозможно;

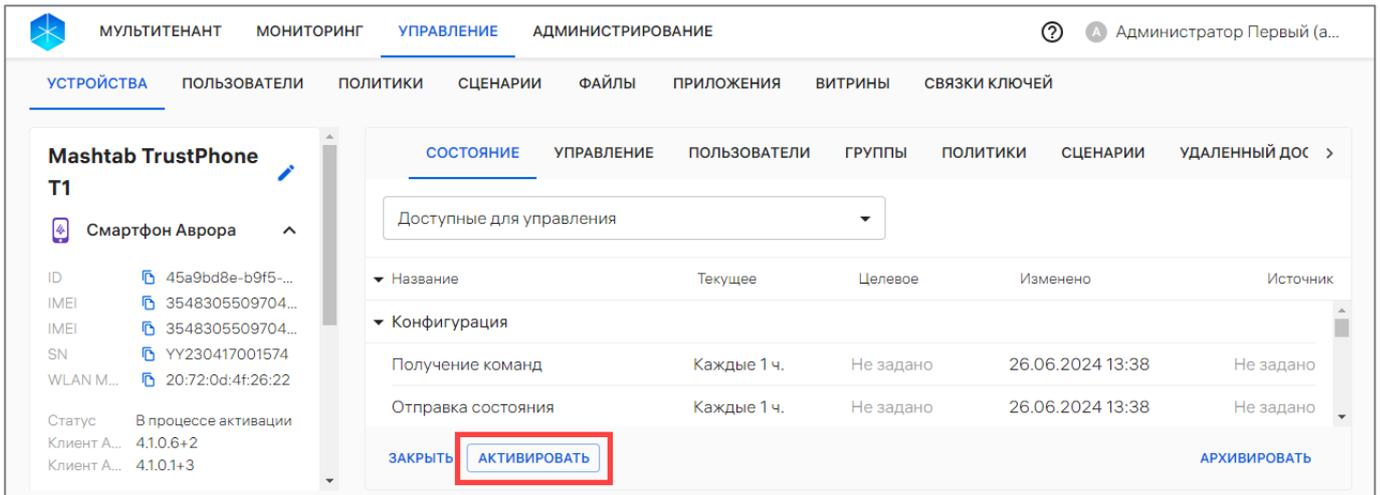


Рисунок 77

- отобразится окно активации устройств (Рисунок 78);
- если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса (Рисунок 78 [1]) и нажать кнопку «Дальше» (Рисунок 78 [2]);

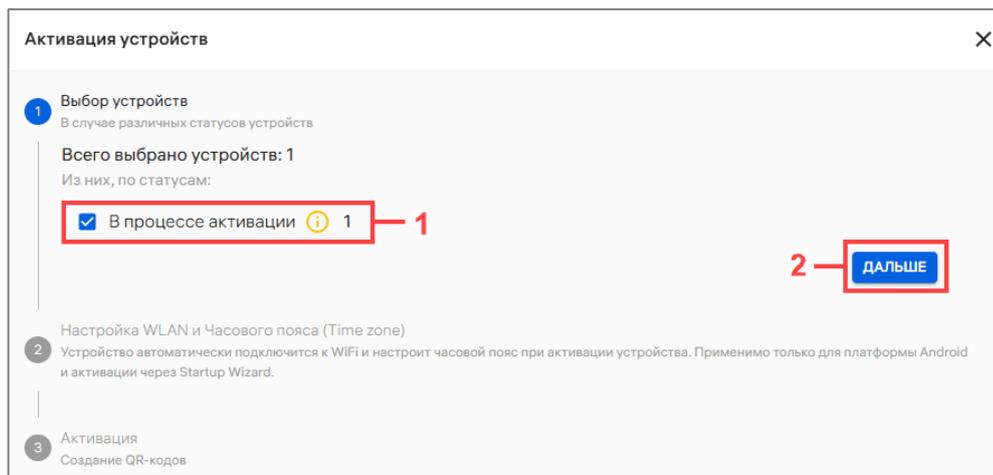


Рисунок 78

- для ОС Android в отобразившемся окне (Рисунок 79) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.4 и нажать кнопку «Дальше»;

Активация устройств

В процессе активации ⓘ 1

2 Настройка WLAN и Часового пояса (Time zone)
Устройство автоматически подключится к WiFi и настроит часовой пояс при активации устройства

Включить настройки WLAN

Название сети (SSID)

Скрытая сеть

Безопасность

Пароль

Включить настройки часового пояса

Часовой пояс

НАЗАД ДАЛЬШЕ

3 Активация
Создание QR-кодов

Рисунок 79

– откроется окно, где необходимо нажать кнопку «Активация вручную» (Рисунок 80);

Активация устройств

Название сети (SSID)

Скрытая сеть

Безопасность

Пароль

Включить настройки часового пояса

Часовой пояс

3 Активация
Создание QR-кодов

Выберите действие

Mashtab TrustPhone T1 IMEI 354830550970406, 3548...

НАЗАД

Рисунок 80

– в результате отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (Рисунок 81).



Рисунок 81

В результате успешного создания QR-кода будет отображена следующая информация (Рисунок 82):

– единый QR-код для установки приложения «Аврора Центр» и активации устройства, который необходимо отсканировать в приложении «Аврора Центр» на каждом устройстве;

- дата истечения QR-кода;
- контрольная сумма MD5;
- часовой пояс;
- название компонента;

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр».

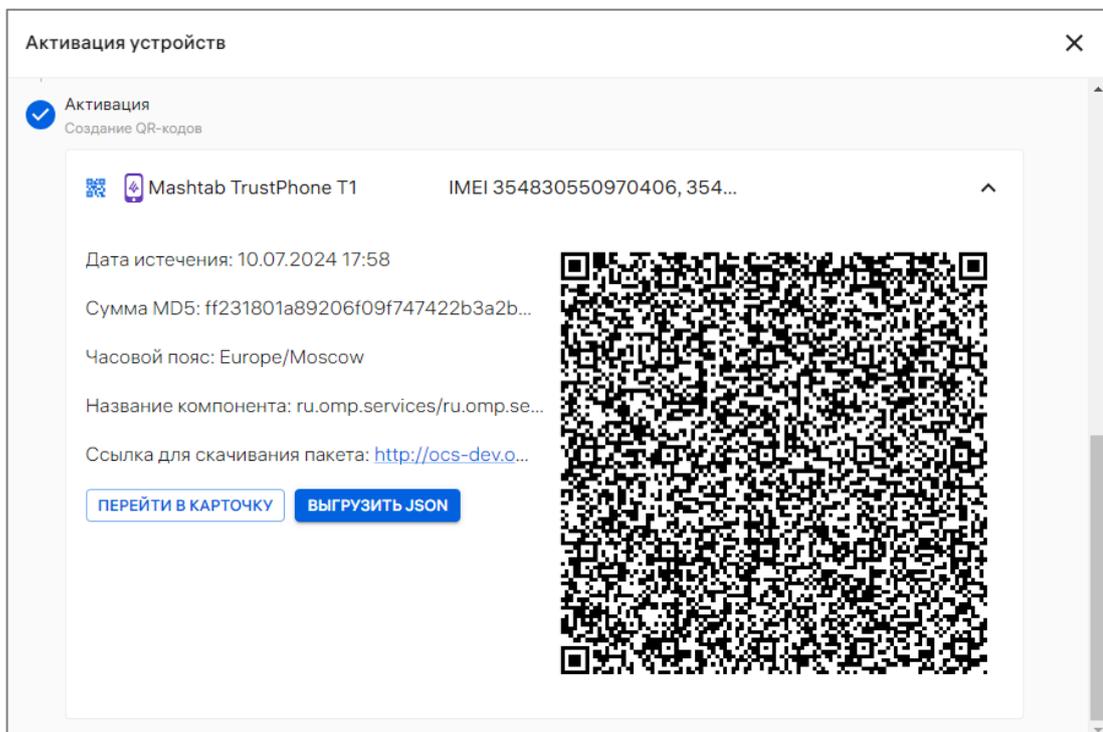


Рисунок 82

При успешной активации на устройство назначаются все политики и офлайн-сценарии, назначенные на:

- группу устройств, в которую входит устройство;
- на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в столбце «Соответствие политике» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

2.2.9.2. Активация устройств при помощи списка быстрых действий

Для активации устройств при помощи списка быстрых действий необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- выбрать устройства, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 83 [1]);
- в списке быстрых действий выбрать значок  «Активировать» (Рисунок 83 [2]).

ПРИМЕЧАНИЕ. С помощью списка быстрых действий может быть выполнена активация одного или нескольких устройств;

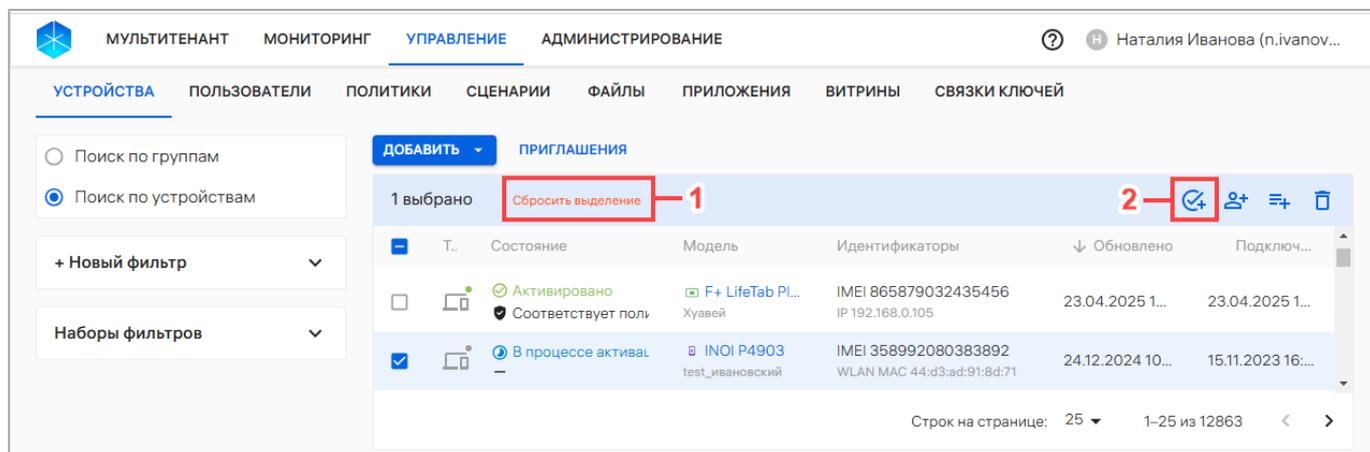


Рисунок 83

- отобразится окно активации устройств (см. Рисунок 78);
- если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса устройства (см. Рисунок 78 [1]) и нажать кнопку «Дальше» (см. Рисунок 78 [2]);
- для ОС Android в отобразившемся окне (см. Рисунок 79) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.4 и нажать кнопку «Дальше»;

– в открывшемся окне необходимо нажать кнопку «Активация вручную» (см. Рисунок 80);

– отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (см. Рисунок 81).

В результате успешного создания QR-кода будет отображена следующая информация:

– единый QR-код для установки приложения «Аврора Центр» и активации устройства.

ПРИМЕЧАНИЕ. QR-код будет отображен для каждого из выбранных устройств (Рисунок 84 [1], Рисунок 84 [2]), который необходимо отсканировать в приложении «Аврора Центр» на каждом устройстве;

– дата истечения QR-кода;

– контрольная сумма MD5;

– часовой пояс;

– название компонента;

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр».

ПРИМЕЧАНИЕ. Установка приложения «Аврора Центр» и активация устройства будут автоматически выполняться при корпоративной привязке устройства с ОС Аврора (подробнее в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7) к ПУ. В остальных случаях QR-код можно использовать только для активации устройства.

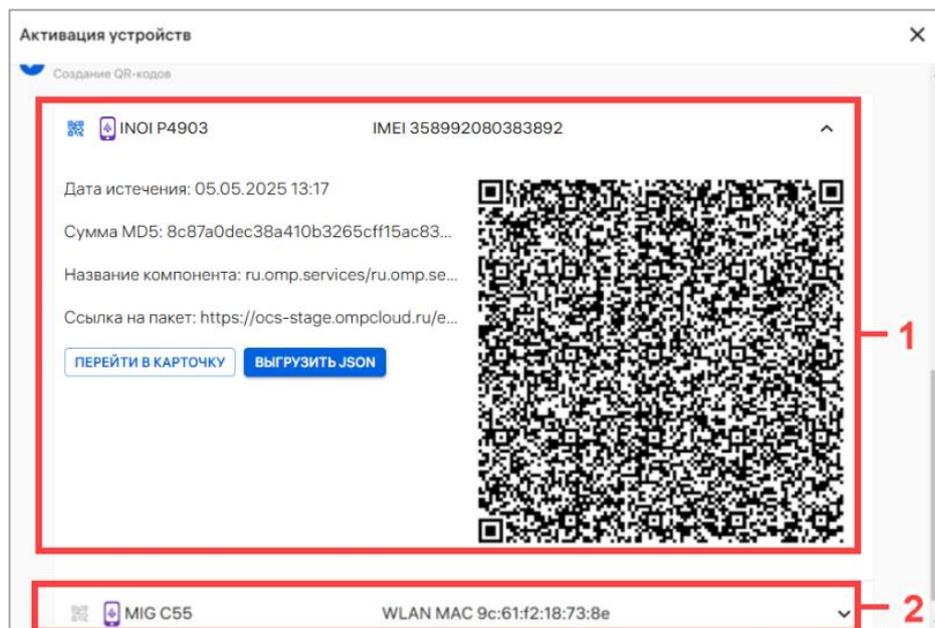


Рисунок 84

При успешной активации на устройство назначаются все политики и офлайн-сценарии, назначенные на:

- группу устройств, в которую входит устройство;
- на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в параметре «Политика» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

ПРИМЕЧАНИЕ. Срок действия QR-кода указан в поле «Дата истечения». По истечении срока действия сгенерированный QR-код будет недействителен.

ВНИМАНИЕ! В случае настроек ППО по умолчанию QR-код генерируется на 5 минут. Этого времени может не хватить для того, чтобы все устройства успели пройти активацию, если устройств много или QR-коды для активации отправляются на Email пользователей. Настройки срока действия QR-кода можно изменить. Подробная информация приведена в документе «Руководство администратора» АДМГ.20134-01 91 01.

QR-код можно скопировать, нажав на него правой кнопкой мыши, и выбрать из списка пункт «Сохранить картинку как...», после чего QR-код можно отправить в виде изображения.

Далее пользователю необходимо отсканировать QR-код и выполнить активацию устройства. Подробное описание активации устройства приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

2.2.9.3. Активация устройств с помощью отправки QR-кода на Email

Для активации устройств с помощью Email на указанный адрес направляется электронное письмо с QR-кодом. Для этого необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (см. Рисунок 83 [1]);
- в списке быстрых действий выбрать значок  «Активировать» (см. Рисунок 83 [2]).

ПРИМЕЧАНИЕ. С помощью списка быстрых действий может быть выполнена активация одного или нескольких устройств;

- отобразится окно активации устройств (см. Рисунок 78);
- если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса (см. Рисунок 78 [1]) и нажать кнопку «Дальше» (см. Рисунок 78 [2]);

– для ОС Android в отобразившемся окне (см. Рисунок 79) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.4 и нажать кнопку «Дальше»;

– откроется окно, где необходимо нажать кнопку «Отправить на Email» (Рисунок 85);

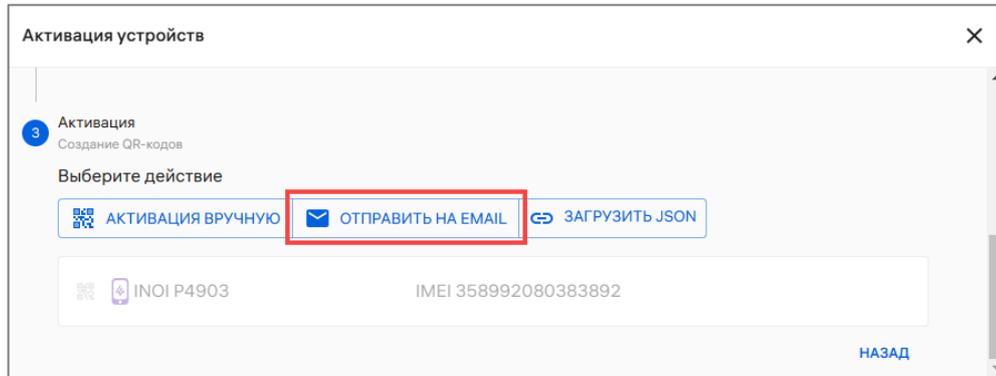


Рисунок 85

– в результате отобразится окно отправки QR-кода на Email, где необходимо ввести Email для писем с активацией (Рисунок 86 [1]);

– нажать кнопку «Отправить» (Рисунок 86 [2]).



Рисунок 86

На указанный адрес будет отправлено электронное письмо с QR-кодом для активации, который пользователю необходимо отсканировать на устройстве в приложении «Аврора Центр».

Подробное описание активации устройств приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

При успешной активации на устройстве назначаются все политики и офлайн-сценарии, назначенные на:

- группу устройств, в которую входит устройство;
- на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в параметре «Политика» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

2.2.9.4. Активация группы устройств с помощью JSON-файла

Для активации устройств с помощью JSON-файла необходимо подготовить (пп. 2.2.9.4.1) и загрузить (пп. 2.2.9.4.2) JSON-файл.

Если первоначальная настройка устройств не осуществлялась, необходимо выполнить ускоренную активацию. Подробное описание приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

Если первоначальная настройка устройств была выполнена, необходимо отсканировать QR-код, сгенерированный для группы устройств, в которую входят устройства. Подробное описание приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

2.2.9.4.1. Подготовка JSON-файла

Активация устройств единым QR-кодом осуществляется с помощью JSON-файла, который можно сгенерировать в ПУ.

Для генерации JSON-файла необходимо выполнить действия, описанные в пп. 2.2.9.2, до этапа отображения окна активации устройств, где будет отображена следующая информация:

- единый QR-код для установки приложения «Аврора Центр» и активации устройства;
- дата истечения QR-кода;
- контрольная сумма MD5;
- часовой пояс;
- название компонента;
- ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр».

ПРИМЕЧАНИЕ. Установка приложения «Аврора Центр» и активация устройства будут автоматически выполняться при корпоративной привязке устройства с ОС Аврора (подробнее в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7) к ПУ. В остальных случаях QR-код можно использовать только для активации устройства.

Далее на этапе отображения единого QR-кода необходимо нажать кнопку «Выгрузить JSON» (Рисунок 87).

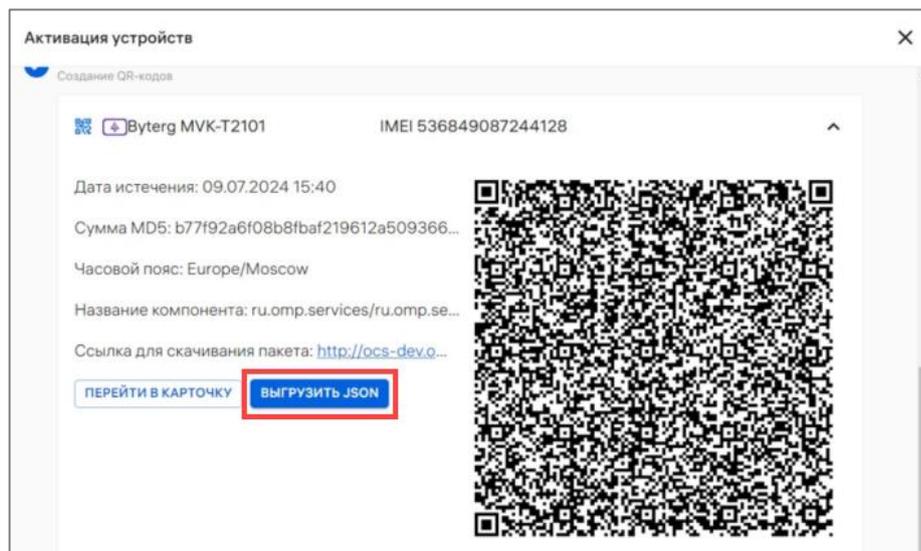


Рисунок 87

В результате на ЭВМ будет выгружен JSON-файл.

Пример содержания JSON-файла:

```
{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {"accountDo
main":"","clientID":"aurora-mobility-
management","gatewayURI":"http://ocs-
dev.ompcloud.ru/emm/mobile","password":"o9qaaoppSonulzkebtsxdd%2dbii",
trustedCerts":""}, "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONEN
T_NAME":"ru.omp.services/ru.omp.services.AdminReceiver", "android.app.ex
tra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"http://ocs-
dev.ompcloud.ru/emm/mobile/clientDownload", "android.app.extra.PROVISION
ING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"bZ41Av7s6nrQpXjBhLevsESkkVLfg4",
android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true, "and
roid.app.extra.PROVISIONING_TIME_ZONE":"Europe/Moscow", "android.app.ext
ra.PROVISIONING_WIFI_HIDDEN":"true", "android.app.extra.PROVISIONING_WIF
I_PASSWORD":"243432243324", "android.app.extra.PROVISIONING_WIFI_SECURIT
Y_TYPE":"WEP", "android.app.extra.PROVISIONING_WIFI_SSID":"43243243432",
"expiredAt":"2024-07-09T13:52:01+03:00" }
```

ВНИМАНИЕ! Приведенный пример представлен для ознакомления с содержанием и структурой JSON-файла, и может отличаться от сгенерированного. Не рекомендуется форматировать сгенерированный JSON-файл (добавлять пробелы, табуляцию, переносы строк), так как это может привести к ошибкам при обработке JSON-файла в процессе установки приложения и активации устройств.

Каждый параметр сопровождается двоеточием «:», пары ключ/значение разделяются запятой «,».

Описание требований к значениям параметров из примера:

– **android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE** – содержимое JSON-файла:

- **password** – пароль, присваиваемый для созданной учетной записи устройства. Новый пароль может содержать:

- ◆ от 8 до 255 символов;

АДМГ.20134-01 90 01-3

- ◆ не менее 2 заглавных букв;
- ◆ не менее 2 строчных букв;
- ◆ не менее 3 цифр;
- ◆ не менее 2 спецсимволов.

ПРИМЕЧАНИЕ. При генерации JSON-файла создаются учетные записи устройств. Требования к паролю задаются администратором и могут отличаться от приведенных;

- **gatewayURI** – адрес сервера активации устройств;
- **accountDomain** – доменное имя аккаунтов учетных записей устройств, созданных в выбранном тенанте;
- **clientID** – идентификатор приложения в выбранном тенанте. Значение по умолчанию `aurora-mobility-management`;
- **trustedCerts** – список цифровых отпечатков (fingerprint) корневых сертификатов для активации устройств, перечисленные через запятую;
 - **android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME** – название компонента;
 - **android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM** – контрольная сумма подписи файла для установки приложения «Аврора Центр»;
 - **android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION** – ссылка на скачивание файла для установки приложения «Аврора Центр»;
 - **android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED** – параметр, определяющий, включать ли полную установку системных приложений в процессе установки первоначальной настройки устройства с установкой приложения «Аврора Центр» (актуально для устройств с ОС Android). По умолчанию установка всех системных приложений включена;
 - **android.app.extra.PROVISIONING_WIFI_SSID** – название сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;
 - **android.app.extra.PROVISIONING_WIFI_PASSWORD** – пароль сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;
 - **android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE** – технология безопасности сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;
 - **android.app.extra.PROVISIONING_WIFI_HIDDEN** – параметр, определяющий транслируется ли название сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;
 - **android.app.extra.PROVISIONING_TIME_ZONE** – часовой пояс, который автоматически будет установлен на устройстве в процессе установки приложения «Аврора Центр» и активации устройства;

– **expiredAt** – срок действия QR-кода (дата истечения активации). После указанной даты сгенерированный QR-код будет недействителен.

2.2.9.4.2. Загрузка JSON-файл для активации группы устройств

Для активации группы устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– выбрать группу устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения следует нажать кнопку «Сбросить выделение» (Рисунок 88 [1]);

– в списке быстрых действий выбрать значок  «Активация устройств» (Рисунок 88 [2]);

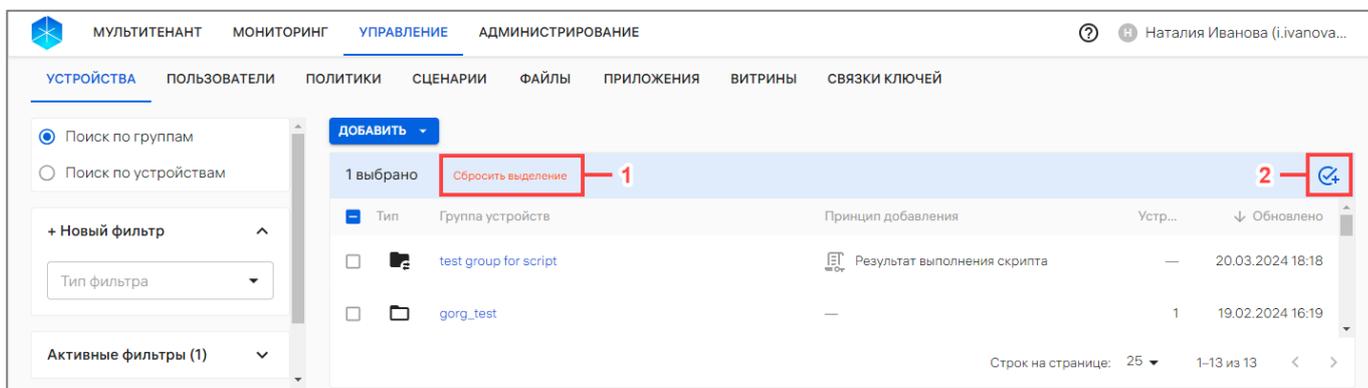


Рисунок 88

– перенести сгенерированный или подготовленный самостоятельно JSON-файл из файлового менеджера в поле загрузки (Рисунок 89);



Рисунок 89

– отобразится информация о загруженном JSON-файле, где необходимо нажать кнопку «Активация вручную» (Рисунок 90 [1]). Для удаления загруженного JSON-файла необходимо нажать кнопку «Удалить JSON» (Рисунок 90 [2]);

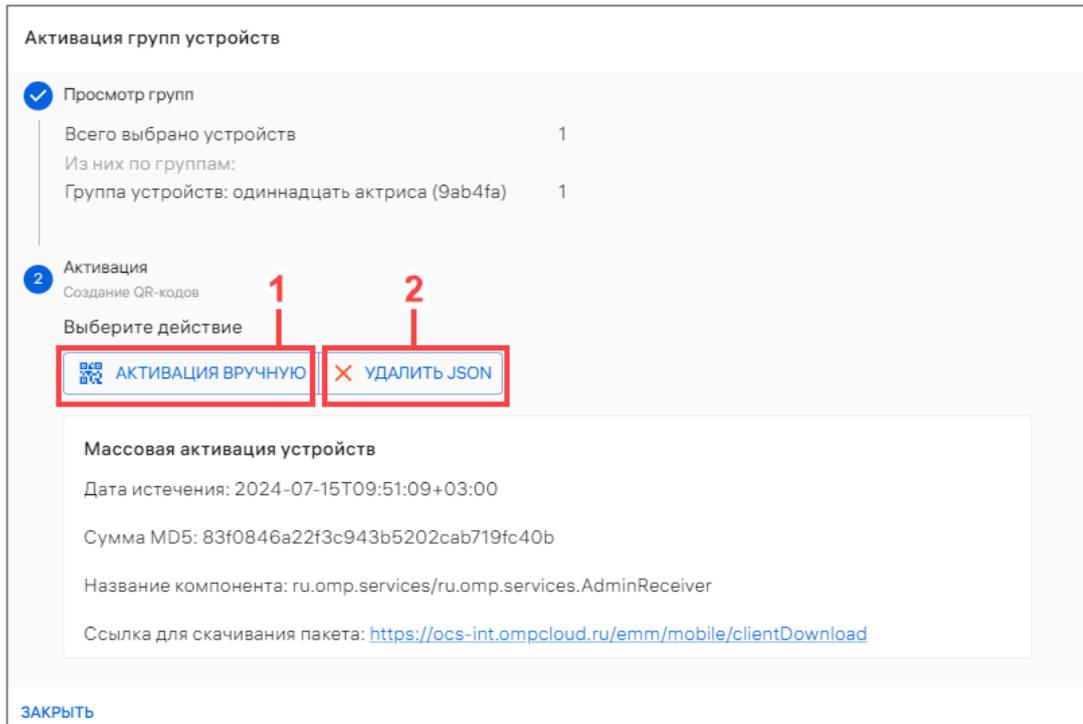


Рисунок 90

– в отобразившемся окне активации устройств необходимо нажать кнопку «Продолжить»;

– если были выбраны группы, содержащие активированные устройства или в статусе «В процессе активации», отобразится окно подтверждения операции (Рисунок 91), где необходимо подтвердить или отменить действия.

В чекбоксе «Не активировать ранее активированные устройства» следует установить галочку в случае отсутствия необходимости активировать ранее активированные устройства либо снять галочку, в случае наличия указанной необходимости.

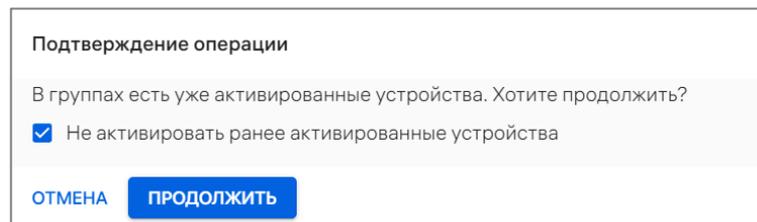


Рисунок 91

В результате JSON-файл будет загружен, и отобразится QR-код для активации группы устройств (Рисунок 92).

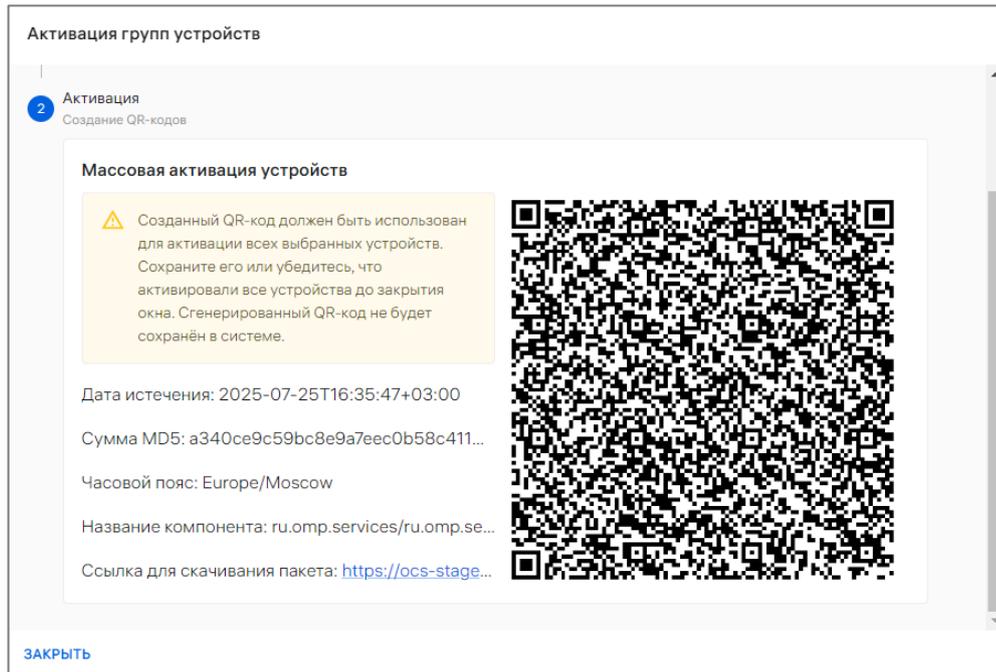


Рисунок 92

Для завершения активации необходимо выполнить следующие действия:

- выполнить ускоренную активацию устройств, если их первоначальная настройка не осуществлялась. Описание процедуры ускоренной активации приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7;
- отсканировать QR-код на каждом устройстве, если они уже прошли первоначальную настройку.

Для закрытия окна активации группы устройств необходимо нажать кнопку «Закрыть».

После загрузки JSON-файла для удобства работы с активацией в рабочей области раздела «Управление» подраздела «Устройства» отобразится индикатор активации (Рисунок 93). При нажатии на индикатор отобразится подробная информация об активации устройств: RequestID активации и количество готовых к активации устройств.

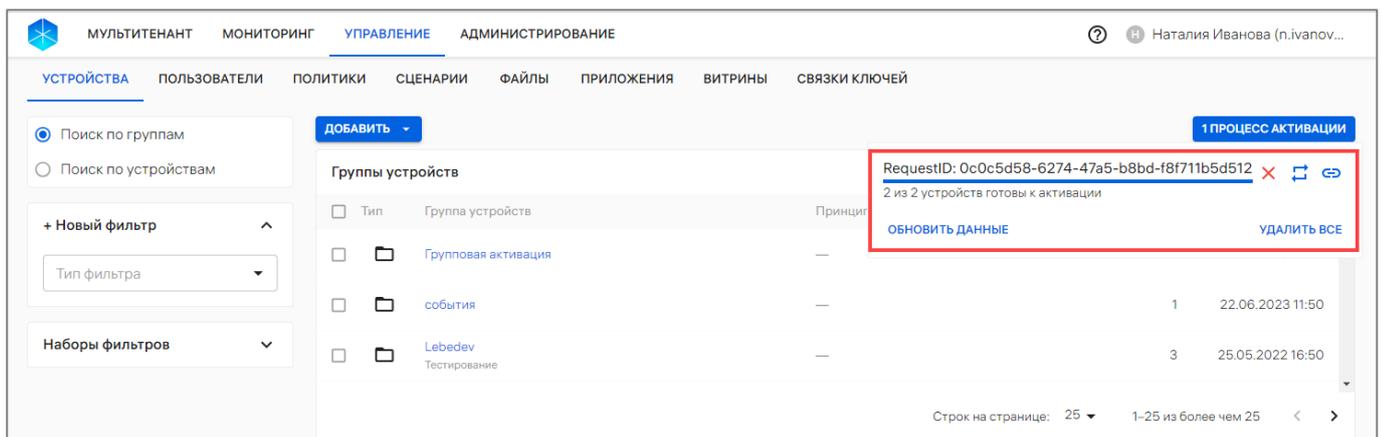


Рисунок 93

Для копирования ссылки процесса необходимо нажать значок  «Скопировать ссылку процесса» (Рисунок 93). Для перезапуска процесса активации необходимо нажать значок  «Перезапустить процесс». Для обновления информации об активации необходимо нажать кнопку «Обновить данные». Для закрытия индикатора следует нажать значок  «Удалить процесс» или «Удалить все».

2.2.10. Применение оперативных команд

ВНИМАНИЕ! Применение оперативных команд доступно только для активированных устройств.

ПРИМЕЧАНИЕ. Для корректного управления устройством необходимо, чтобы на устройстве было выставлено корректное время и был задан часовой пояс.

Для применения команд оперативного управления необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке устройства выбрать доступные команды (Рисунок 94 [1]), задать необходимые значения согласно таблице (Таблица 32) и далее подтвердить или отменить действия.

ПРИМЕЧАНИЕ. Действующие оперативные команды выделены цветным индикатором у соответствующего значка (Рисунок 94 [2]).

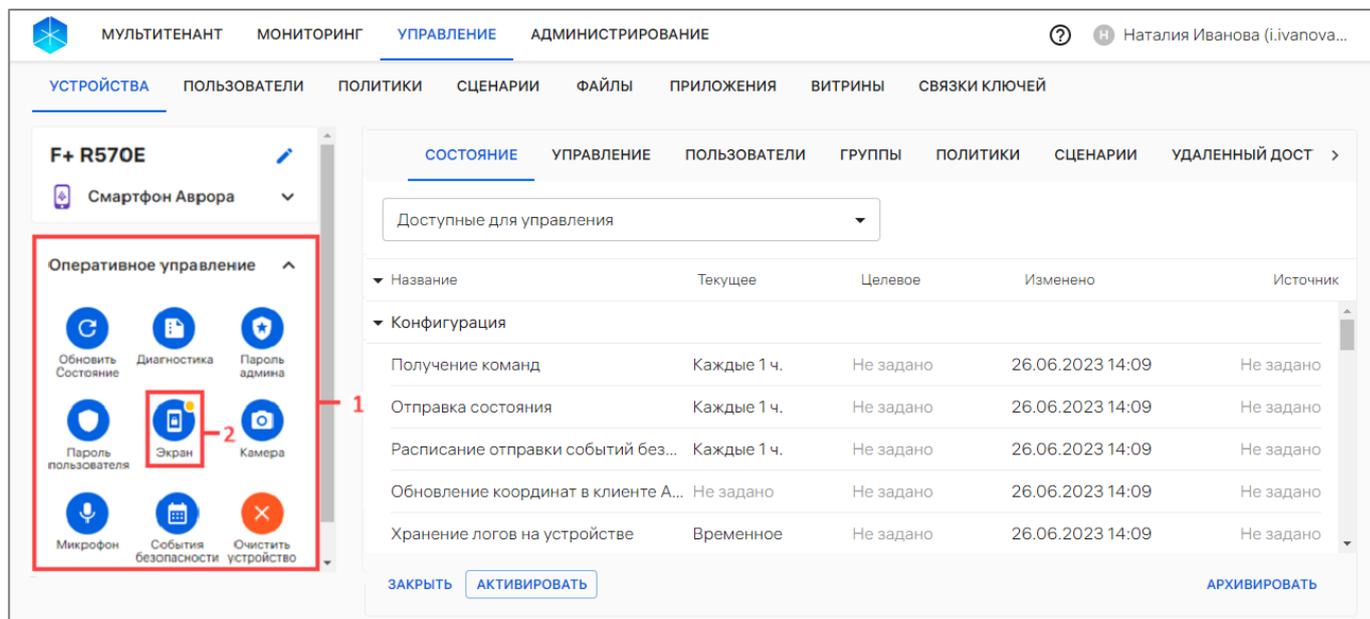


Рисунок 94

В результате успешной отправки оперативной команды отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Выбранная команда будет выполнена на устройстве в соответствии с установленным расписанием получения команд.

Если политика или оперативная команда не были получены на устройстве, то текущее и целевое состояния не будут совпадать. Несоответствия выделяются цветом, а в строке с названием группы политик/состояний отображается значок  (см. Рисунок 14).

Таблица 32

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
Обновить состояние	Установка расписания обновления состояния устройства. Информация о состоянии устройства будет получена, если устройство находится в сети	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4
Диагностика	<p>Получение на электронную почту файла со списком системных сообщений об ошибках устройства (Рисунок 95).</p> <p>Название файла:</p> <ul style="list-style-type: none"> – Reports.tar.bz2 – для ОС Аврора; – report_yyyy-mm-dd_hh-mm-ss.zip – для ОС семейства Linux. Архив содержит: <ul style="list-style-type: none"> • файл omp-uem-agent.db с базой данных приложения «Аврора Центр»; • файл journalctl.log с логами journalctl за последний день. <p>ПРИМЕЧАНИЯ:</p> <ul style="list-style-type: none"> ✓ Для получения отчета с системными сообщениями устройства необходимо первоначально выполнить настройку взаимодействия Сервера приложений ПУ с SMTP-сервером (подробная информация приведена в документе «Руководство администратора» АДМГ.20134-01 91 01); ✓ По умолчанию отчет, содержащий список системных сообщений, отправляется на почтовый ящик, соответствующий текущей учетной записи администратора, которая может быть изменена. <p>Если Email оператора не заполнен или не является действительным (например, в созданном тенанте), необходимо ввести его вручную.</p> <p>ВНИМАНИЕ! Если необходимо вызвать оперативную команду в тенанте, созданном из дефолтного тенанта, обязательно на следующем шаге требуется скорректировать адрес электронной почты, т.к. учетная запись администратора тенанта имеет вид: <имя учетной записи>@<код тенанта>.<домен по умолчанию> (например: n.ivanova@test.omp.ru), что не может являться адресом электронной почты.</p> <p>Процесс сбора и отправления системных сообщений на Email приведен в приложении (Приложение 5)</p>	4.0.2 и выше	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4
Пароль админа	<p>Установка одноразового пароля администратора для разблокировки устройства, если пользователь не знает или не может вспомнить пароль.</p> <p>Пароль должен содержать от 7 до 12 символов.</p> <p>После установки пароля администратор должен загрузить устройство в режиме администратора, ввести одноразовый пароль на устройстве, затем выбрать предлагаемый устройством новый пароль или самостоятельно задать новый пароль.</p> <p>Если учетная запись администратора была заблокирована на устройстве (в процессе ускоренной активации при применении политики создания пользователя), после установки одноразового пароля учетная запись администратора будет разблокирована</p>	4.0.2 и выше	-	-	-	-	-

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
Пароль пользователя	Установка одноразового пароля пользователя для разблокировки устройства, если пользователь не знает или не может вспомнить пароль. Пароль должен соответствовать требованиям парольной политики и содержать от 7 до 12 символов. После установки пароля пользователю необходимо выполнить вход под своей учетной записью, ввести одноразовый пароль, затем выбрать предлагаемый устройством новый пароль или самостоятельно задать новый пароль	4.0.2 и выше	-	-	-	-	-
Экран	Блокировка экрана устройства для предотвращения его использования посторонними лицами в случае утери или кражи. В результате блокировки устройства на экране блокировки отображается сообщение: «Заблокировано при помощи Aurora Device Manager. Заблокировано администратором». Использование устройства до разблокировки невозможно, кроме совершения экстренного вызова. Выбор значения из списка: – «Временная блокировка» – указание периода блокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]». Также доступна возможность ввода сообщения в поле «Сообщение при блокировке», которое будет отображаться на экране заблокированного устройства; – «Временная разблокировка» – период разблокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]»	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4
Камера	Установка запрета/разрешения использовать камеру на устройствах. Выбор значения из списка: – «Временно запретить» – указать временной интервал, в течение которого использование камеры на устройстве будет запрещено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»; – «Временно разрешить» – указать временной интервал, в течение которого использование камеры на устройстве будет разрешено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»	4.0.2 и выше	7 и выше	-	-	-	-
Микрофон	Установка запрета/разрешения использование микрофона на устройствах. Выбор значения из списка: – «Временно запретить» – указать временной интервал, в течение которого использование микрофона на устройстве будет запрещено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]». ПРИМЕЧАНИЕ. При запрещающей команде микрофон будет недоступен для записи звука во всех приложениях и внешних устройствах, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов; – «Временно разрешить» – указать временной интервал, в течение которого использование микрофона на устройстве будет разрешено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»	4.0.2 и выше	-	-	-	-	-

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
События безопасности	Установка расписания отправки сообщений о произошедших на устройствах событиях безопасности. Выбор значения из списка: – «Временная установка» – сообщения доставляются по заданному расписанию и в течение указанного периода. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»; – «Отменить отправку» – на устройствах применяются назначенные политики или настройки по умолчанию, если политик не назначено	4.0.2 и выше	-	-	-	-	-
Очистить устройство	Очистка всех данных пользователя, включая данные с внешнего носителя (карты памяти microSD), для сохранения конфиденциальности данных в случае утери или кражи устройства. ВНИМАНИЕ! Не рекомендуется прерывать процесс очистки, т.к. для последующего включения устройства потребуется переустановка ОС. После завершения очистки на устройстве восстанавливаются заводские настройки. При активации устройства после полной очистки на него будут распространяться все политики, ранее назначенные на группы устройств или группы пользователей, в которые входит данное устройство	4.0.2 и выше	7 и выше	-	-	-	-
Откат на точку восстановления	ПРИМЕЧАНИЯ: ✓ Команда оперативного управления «Откат на точку восстановления» доступна только для устройств ОС семейства Linux и применима только для устройств с файловой системой BTRFS; ✓ Откат можно выполнить только на точки, созданные приложением «Аврора Центр»; ✓ Команда сработает только при наличии связи с приложением «Аврора Центр» на устройстве. Заполнить следующие поля: – «Причина отката» - ввести причину отката (например: «Ошибочное назначение политики с обновлением версии Приложения»). Поле обязательно для заполнения; – «Дата нужной точки отката» - ввести дату нужной точки отката в формате ДД.ММ.ГГГГ. По умолчанию установлена текущая дата; – «Время нужной точки отката» - ввести время нужной точки отката в формате ЧЧ:ММ. По умолчанию установлено текущее время. После введения данных нажать на кнопку «Активировать изменения» и при наличии связи сервера с приложением «Аврора Центр» устройство найдет нужную точку восстановления и начнет делать откат на нее. ВНИМАНИЕ! Откат не произойдет точно на выбранные дату и время, вместо этого устройство выберет точку восстановления, максимально близкую к введенным значениям.	-	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	<p>Логика создания точек восстановления. При создании точки восстановления система автоматически записывает локальные дату и время устройства. Если на момент создания точки восстановления дата и время устройства были изменены вручную, в дальнейшем это может привести к некорректному откату на такие точки. Это связано с тем, что при формировании оперативной команды система «вписывает» значение серверного времени, но точка создается по локальному времени устройства. Например, если на устройстве вручную выставлено 17.03.2024, а серверная дата 17.03.2025, то это резервное копирование данных станет «актуальным» через год.</p> <p>Логика выбора времени и даты точки восстановления при откате. Если дата и время устройства не были изменены вручную при создании точек восстановления, логика выбора будет следующей:</p> <ul style="list-style-type: none"> – на устройстве установлен часовой пояс UTC+7 (+4 к московскому времени), а дата и время синхронизированы с сервером; – на устройстве созданы две точки восстановления: <ul style="list-style-type: none"> • 17.03.2025-05:00 (по времени устройства, что соответствует 01:00 по Москве); • 17.03.2025-09:00 (по времени устройства, что соответствует 05:00 по Москве). <p>Если администратор, находящийся в часовом поясе UTC+3, отправляет команду с указанием времени 17.03.2025-05:00, система выполнит откат на точку 17.03.2025-09:00, так как это соответствует указанному администратором времени с учетом разницы в часовых поясах</p>						

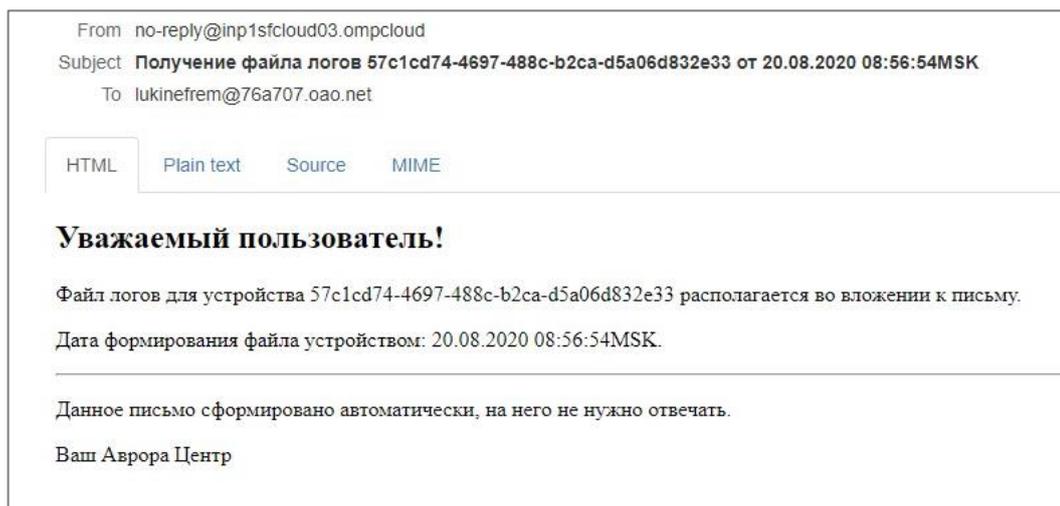


Рисунок 95

2.2.11. Отвязка (исключение) устройств из группы устройств

ВНИМАНИЕ! Невозможно исключить устройства из динамической группы устройств.

Для динамической группы устройств исключение устройств происходит автоматически в случае нарушения условий пребывания в группе.

Исключить устройства из статической группы возможно через:

- карточку устройства (пп. 2.2.11.1);
- карточку группы устройств (пп. 2.2.11.2).

2.2.11.1. Исключение устройства из группы устройств через карточку устройства

Для исключения устройства из группы устройств через карточку устройства необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в карточке устройства перейти во вкладку «Группы»;
- выбрать группу устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 96 [1]);
- в списке быстрых действий нажать значок  «Исключить устройство из группы» (Рисунок 96 [2]);

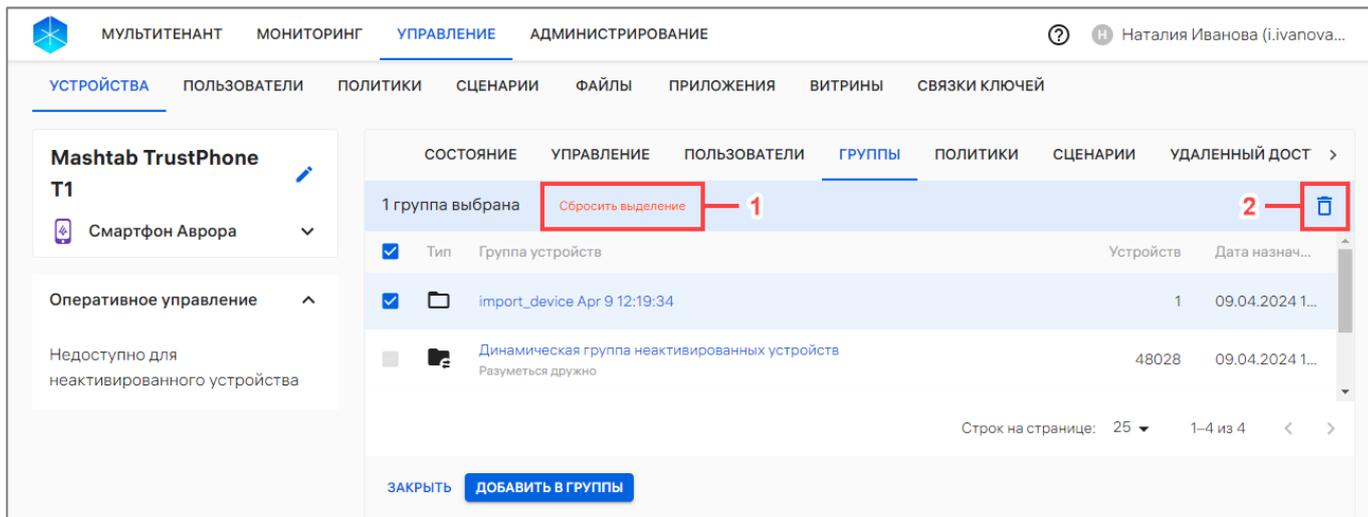


Рисунок 96

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 97).

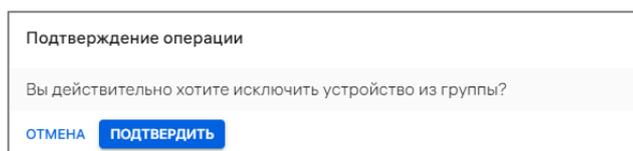


Рисунок 97

В результате успешного подтверждения, политики будут перекомбинированы таким образом, что для устройства будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.11.2.Отвязка устройств от группы устройств через карточку группы устройств

В статической группе устройств отвязать устройство возможно через карточку группы устройств, выполнив следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в карточке группы устройства перейти во вкладку «Устройства»;
- выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 98 [1]);
- в списке быстрых действий нажать значок  «Отвязать устройства от группы» (Рисунок 98 [2]);

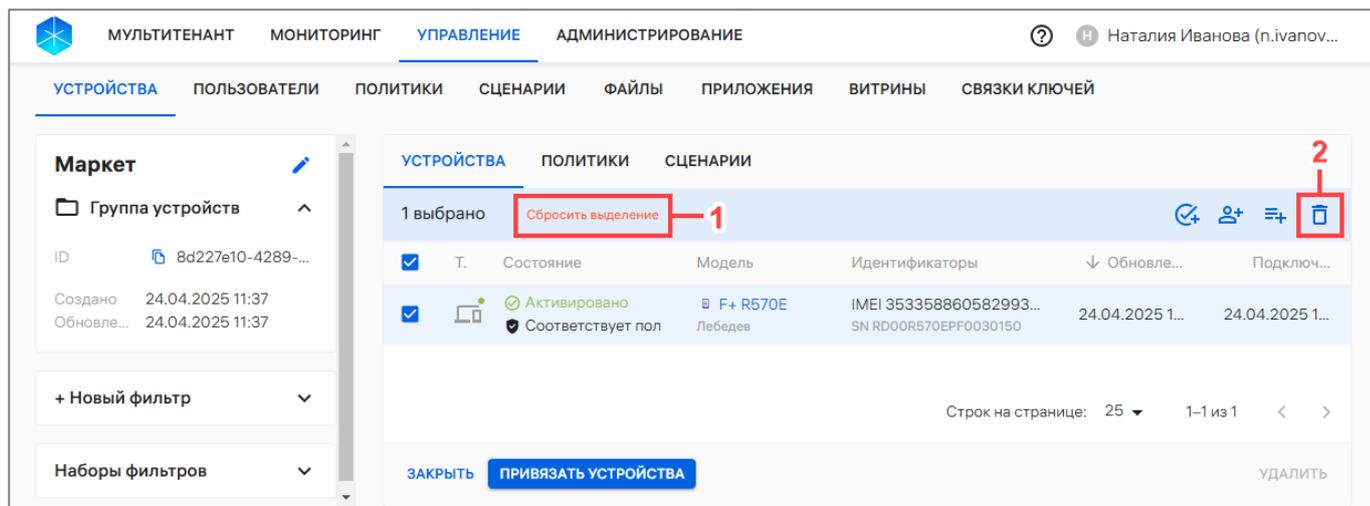


Рисунок 98

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 99).

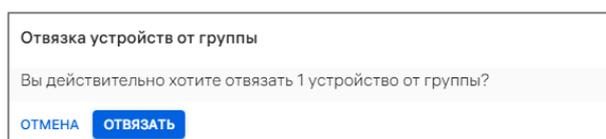


Рисунок 99

В результате успешной отвязки устройства от группы отобразится соответствующее сообщение, политики будут перекомбинированы таким образом, что для устройств будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.12. Архивирование устройства

Под архивированием подразумевается удаление из списка добавленных устройств, после чего устройство повторно добавить в Консоль администратора ПУ невозможно, а возможно только восстановить. Подробное описание восстановления устройства из архива приведено в пп. 2.2.13.

Перед архивированием активированного устройства необходимо очистить его с помощью оперативных команд (п. 2.2.10).

Архивирование устройства может быть выполнено:

- в подразделе «Устройства» с помощью списка быстрых действий (пп. 2.2.12.1);
- с помощью карточки устройства (пп. 2.2.12.2).

2.2.12.1. Архивирование устройства с помощью списка быстрых действий

Для архивирования устройства необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 100 [1]);

– в списке быстрых действий выбрать значок  «Архивировать» (Рисунок 100 [2]);

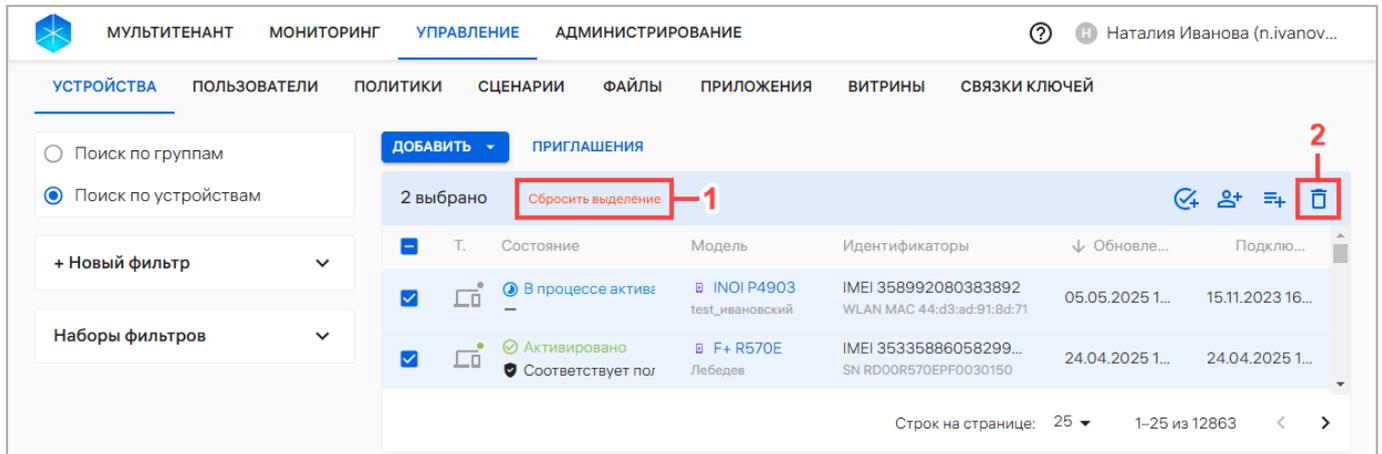


Рисунок 100

– если выбранные устройства были очищены, то отобразится окно подтверждения операции, где необходимо нажать кнопку «Архивировать» (Рисунок 101).

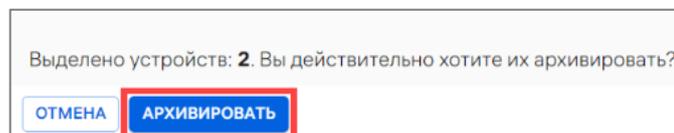


Рисунок 101

Если одно или несколько устройств не очищены, отображается сообщение (Рисунок 102), в котором необходимо выбрать соответствующую кнопку:

– для архивирования только очищенных устройств нажать кнопку «Архивировать только очищенные» (Рисунок 102);

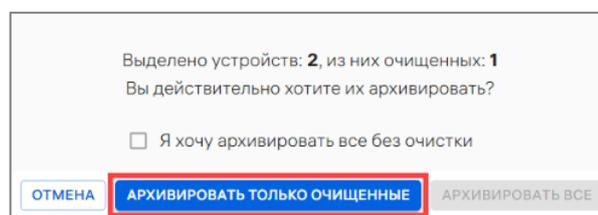


Рисунок 102

– для архивирования без очистки необходимо:

- подтвердить архивирование без очистки, установив галочки в чекбоксе (Рисунок 103 [1]);

- нажать кнопку «Архивировать все» (Рисунок 103 [2]).

АДМГ.20134-01 90 01-3



Рисунок 103

В результате успешного архивирования устройства отобразится соответствующее сообщение, учетные записи устройства будут заблокированы.

ПРИМЕЧАНИЕ. Архивные устройства будут отображаться в списке устройств, если включена соответствующая настройка (п. 4.1.3).

2.2.12.2. Архивирование устройства из карточки устройства

Для архивирования устройства из карточки необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке устройства перейти во вкладку «Состояние»;
- нажать кнопку «Архивировать» (Рисунок 104);

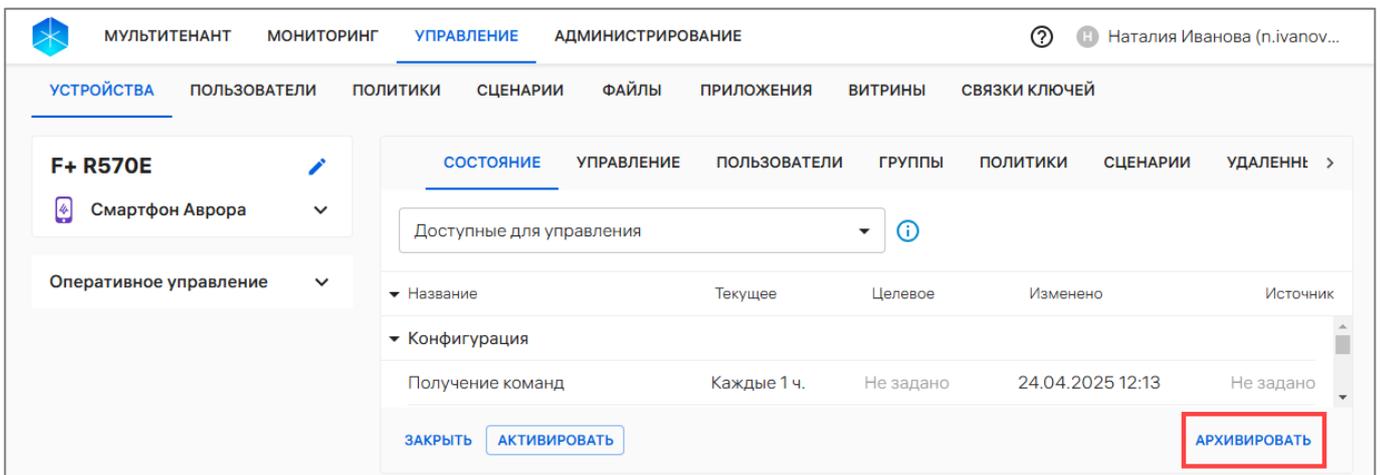


Рисунок 104

– если устройство не очищено, отобразится соответствующее сообщение. Для подтверждения архивирования необходимо нажать кнопку «Архивировать» (Рисунок 105).

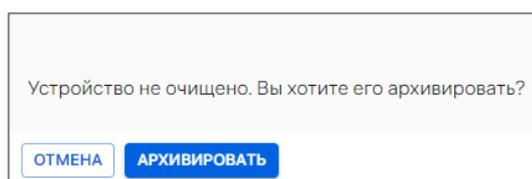


Рисунок 105

В результате успешного архивирования устройства отобразится соответствующее сообщение, учетные записи устройства будут заблокированы.

ПРИМЕЧАНИЕ. Архивные устройства будут отображаться в списке устройств, если включена соответствующая настройка (п. 4.1.3).

2.2.13. Восстановление устройств из архива

Для отображения архивных устройств в подразделе «Устройства» в настройках должен быть активен переключатель «Отображать архивные устройства» (п. 4.1.3).

При восстановлении устройств из архива восстанавливаются все его связи с группами и пользователями.

Для восстановления устройства из архива необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- выбрать архивное устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 106 [1]);
- выбрать значок  «Активировать» (Рисунок 106 [2]);

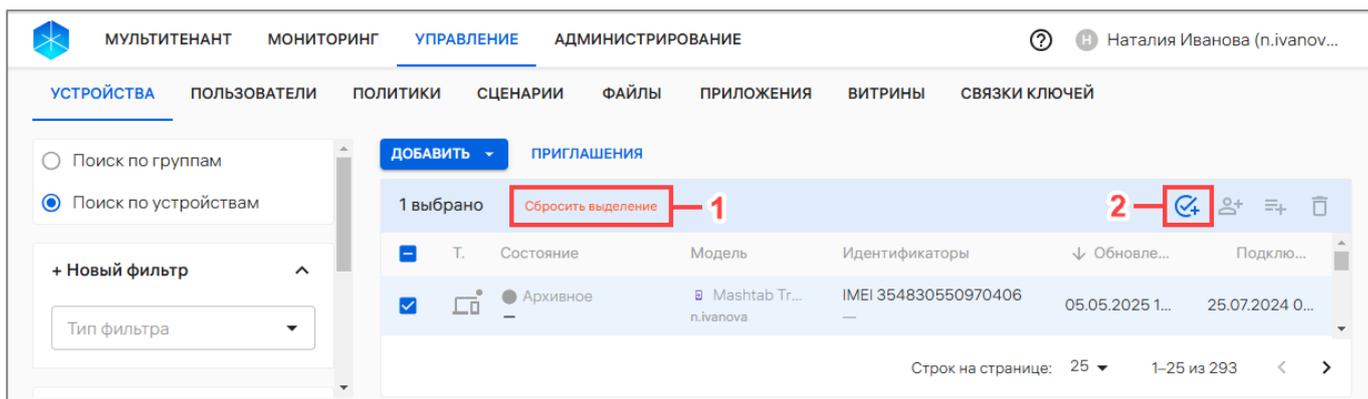


Рисунок 106

- в отобразившемся окне активации устройств установить галочку в чекбоксе «Перенесено в архив» (Рисунок 107 [1]) и нажать кнопку «Дальше» (Рисунок 107 [2]);



Рисунок 107

– при наличии у устройств связей со статистическими группами и/или пользователями на шаге «Восстановление связей» необходимо подтвердить восстановление связей, установив галочку в чекбоксе (Рисунок 108 [1]), и нажать кнопку «Дальше» (Рисунок 108 [2]). Данный шаг подразумевает восстановление связей с группами устройств и пользователями и применение соответствующих политик и офлайн-сценариев. При отсутствии необходимости восстановления связей, установка галочки в чекбоксе на «Восстановить все связи» не является обязательной;



Рисунок 108

– для ОС Android в отобразившемся окне (см. Рисунок 79) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.4 и нажать кнопку «Дальше».

Далее активировать устройства возможно одним из способов:

- нажать кнопку «Активация вручную» (Рисунок 109 [1]) и далее нажать кнопку «Продолжить»;
- нажать кнопку «Отправить на Email» (Рисунок 109 [2]), в открывшемся окне ввести адрес электронной почты и далее нажать кнопку «Отправить».

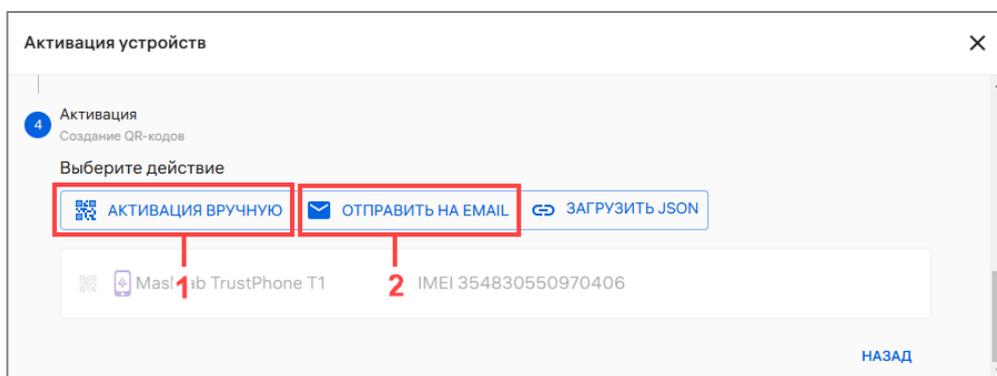


Рисунок 109

В результате будет сгенерирован и отображен QR-код для активации и отобразятся сообщения «Связи архивных устройств восстановлены» и «Процесс создания учетных записей устройств запущен».

Для завершения активации необходимо отсканировать QR-код на устройстве. Описание процесса активации устройств приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

2.2.14. Удаление группы устройств

ПРИМЕЧАНИЕ. Перед удалением группы устройств необходимо:

- предварительно исключить все устройства из группы (п. 2.2.11) – для статической группы устройств;
- отвязать группу устройств от всех политик (п. 2.4.7) и офлайн-сценариев (п. 2.5.3) – для динамической группы.

После выполнения условий, приведенных выше, статическая/динамическая группа может быть удалена из ПУ. Для этого необходимо:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в карточке группы устройств нажать кнопку «Удалить» (Рисунок 110);

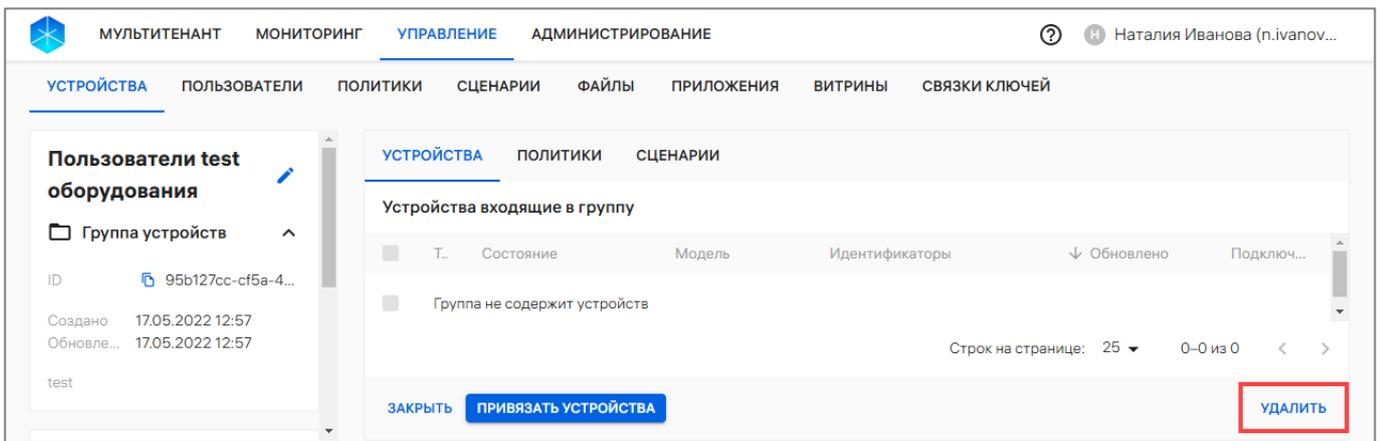


Рисунок 110

- в отобразившемся окне (Рисунок 111) подтвердить либо отменить действия.

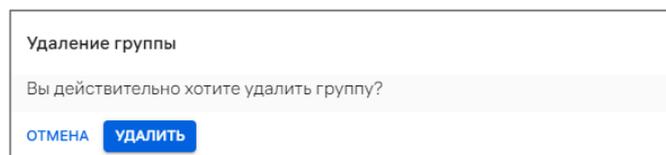


Рисунок 111

В результате успешного удаления отобразится соответствующее сообщение.

2.2.15. Очистка устройств до заводских настроек

ПРИМЕЧАНИЕ. Бизнес-сценарий по экстренному выводу устройства из эксплуатации недоступен для устройств на базе ОС семейства Linux.

Для сброса устройства до заводских настроек необходимо назначить оперативную команду «Очистка устройства» (см. Таблица 32) в соответствии с п. 2.2.10, в результате чего отобразится окно подтверждения операции, где необходимо нажать кнопку «Очистить» (Рисунок 112).

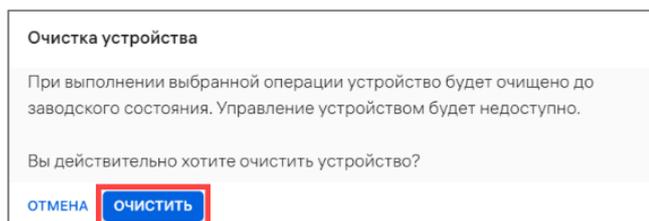


Рисунок 112

В результате успешной очистки все данные пользователя устройства, включая данные с внешнего носителя (карта памяти microSD), удалятся.

ВНИМАНИЕ! Не рекомендуется прерывать очистку устройства, т.к. для последующего включения потребуется переустановка ОС.

После завершения очистки на устройстве будут восстановлены заводские настройки. Для управления очищенным устройством следует активировать его повторно (п. 2.2.9).

При активации устройства после полной очистки на нем будут действовать все политики, ранее назначенные на группы устройств или пользователей, в которые входит это устройство.

2.2.16. Вывод устройства из эксплуатации

ВНИМАНИЕ! Вывод из эксплуатации доступен для устройств в статусе жизненного цикла «Активировано». В иных случаях кнопка «Вывести из эксплуатации» будет не активна.

Для экстренного вывода устройства из эксплуатации необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по устройствам»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке устройств перейти во вкладку «Сценарии»;
- нажать кнопку «Вывести из эксплуатации» (Рисунок 113);

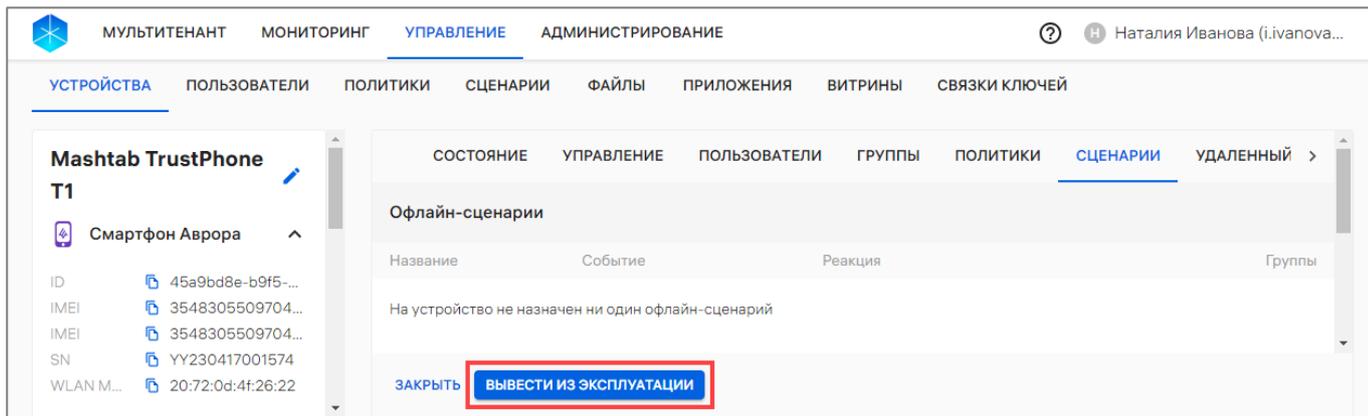


Рисунок 113

– в отобразившемся окне подтверждения операции (Рисунок 114) подтвердить либо отменить действия.



Рисунок 114

В результате успешного вывода устройства из эксплуатации в течение некоторого времени на устройстве будут выполнены следующие операции:

1) На устройствах с ОС Аврора и ОС Android:

– блокировка экрана (с выводением сообщения «Устройство выведено из эксплуатации»);

– очистка устройства (сброс к заводским настройкам);

– архивирование устройства (удаление из списка устройств);

2) На устройствах с ОС семейства Linux:

– если учетная запись пользователя создана через ППО (пользователь acuser), то происходит блокировка экрана (с сообщением «Устройство выведено из эксплуатации»). Иначе экран не блокируется;

– запуск очистки в 3 этапа:

- отмонтирование сетевых папок. Система отключает все подключенные сетевые ресурсы (NFS, SMB/CIFS и др.);

- затирание данных на всех найденных разделах home с использованием алгоритма shred;

- полная очистка дисков (dd). Все диски устройства перезаписываются нулями (dd if=/dev/zero) до тех пор, пока не очистятся критичные для работы ОС директории;

– архивирование (удаление из списка устройств).

ПРИМЕЧАНИЕ. В отличие от ОС Аврора и ОС Android, очистка устройства с ОС семейства Linux подразумевает полное удаление данных с устройства, в том числе ОС.

2.3. Подраздел «Пользователи»

Подраздел «Пользователи» Консоли администратора ПУ предназначен для управления пользователями или группами пользователей.

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Управление», подраздел «Пользователи», в результате чего в рабочей области отобразится информация о пользователях или группах пользователей (Рисунок 115 [2]).

ПРИМЕЧАНИЕ. Для отображения группы пользователей необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 115 [1]).

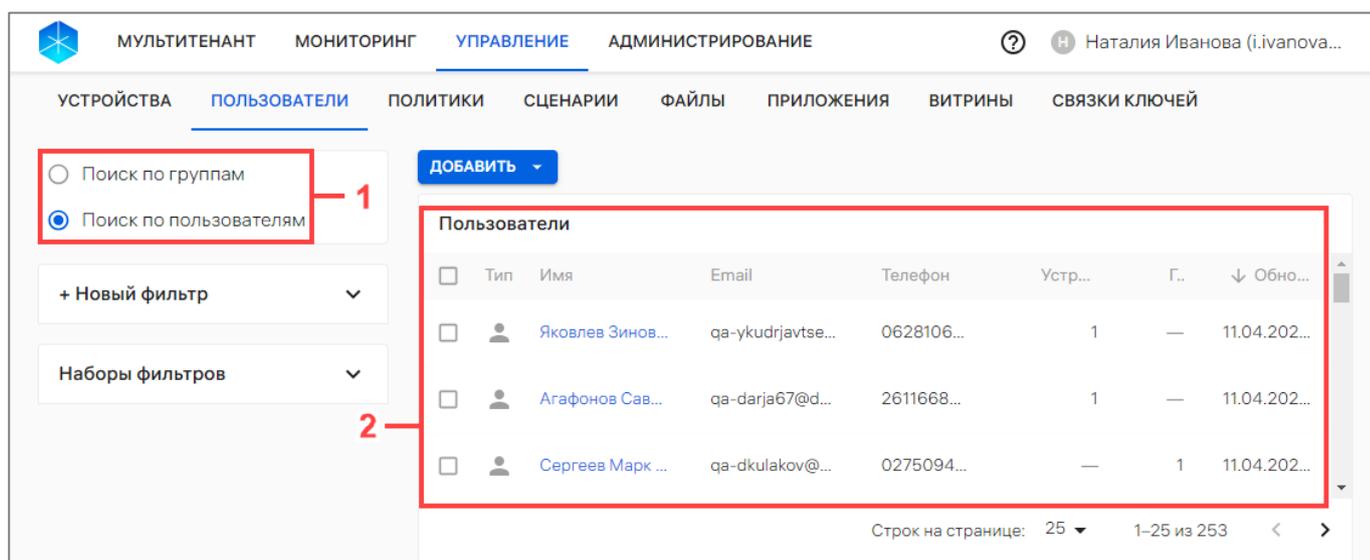


Рисунок 115

В рабочей области информация о пользователях и группах пользователей отображается в столбцах, приведенных в таблице (Таблица 33), а при отсутствии добавленных пользователей или групп пользователей отображается сообщение «Нет данных».

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 33

Параметр	Описание
Пользователи	
Тип	Тип пользователя (Приложение 1)
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую происходит переход к карточке пользователя)
Email	Электронная почта пользователя
Телефон	Номер телефона пользователя
Устройства	Количество устройств, привязанных к пользователю
Группы	Количество групп, к которым привязан пользователь

Параметр	Описание
Обновлено	Дата обновления
Группа пользователей	
Тип	Тип группы пользователей (Приложение 1)
Группа пользователей	– название группы пользователей (представляет собой активную ссылку, при нажатии на которую происходит переход к карточке группы пользователей); – комментарий – дополнительная информация (заполняется при необходимости)
Принцип добавления	Значение, по которому пользователи были добавлены в группу
Пользователей	Количество пользователей, привязанных к группе
Устройств	Количество уникальных устройств, привязанных к пользователям группы
Обновлено	Дата обновления группы

В Консоли администратора ПУ предусмотрена возможность добавления пользователей или групп пользователей одним из следующих способов:

- вручную (п. 2.3.1 и п. 2.3.2);
- с помощью импорта CSV-файла (п. 2.3.3);
- с помощью импорта из LDAP-сервера (пп. 4.1.4.3.1.1).

2.3.1. Добавление пользователя устройства вручную

Для добавления пользователя вручную необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить пользователя» (Рисунок 116);

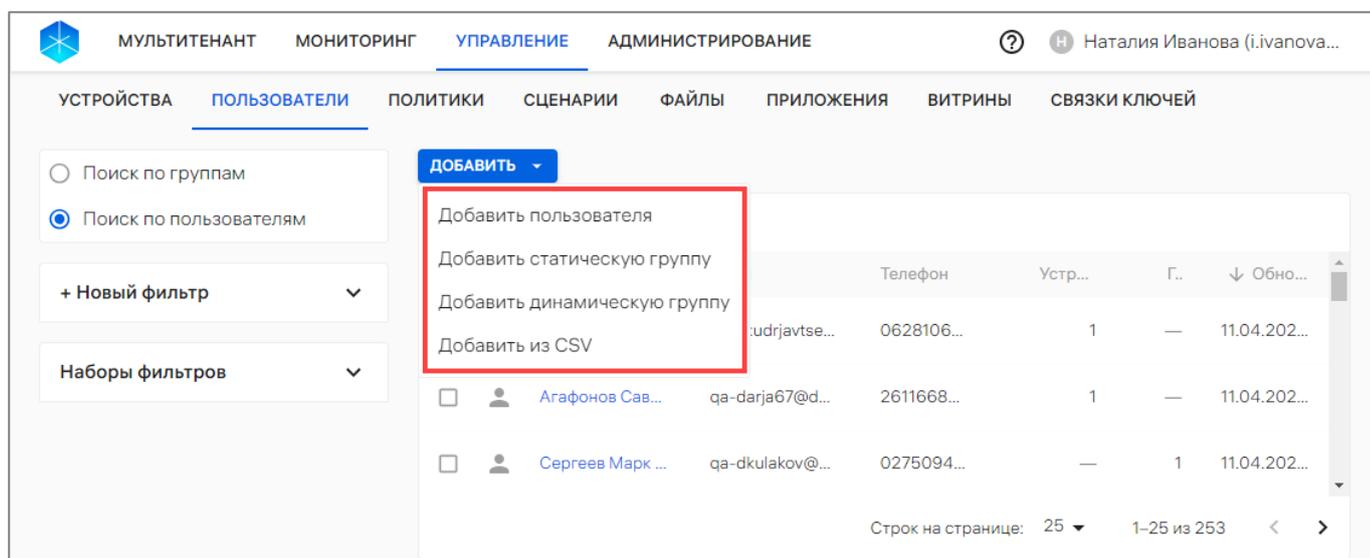


Рисунок 116

– в открывшемся окне (Рисунок 117) ввести данные о пользователе (Таблица 34);

Таблица 34

Поле ввода	Значение	Примечание
Фамилия	Фамилия пользователя	Поле обязательно для заполнения
Имя	Имя пользователя	Поле обязательно для заполнения
Отчество	Отчество пользователя	Поле не обязательно для заполнения
Почта рабочая	Рабочий email пользователя	Поле обязательно для заполнения и является идентификатором пользователя Аврора Центр
Должность	Должность, занимаемая пользователем в компании	Поле не обязательно для заполнения
Телефон рабочий	Номер рабочего телефона пользователя	Поле не обязательно для заполнения

– после заполнения полей подтвердить либо отменить создание пользователя (Рисунок 117).

Создание пользователя вручную

Фамилия* Иванова

Имя* Мария

Отчество Петровна

Почта рабочая* test11@test.ru

Должность

Телефон рабочий 1122334452

ОТМЕНА СОЗДАТЬ

Рисунок 117

В результате успешного добавления пользователя отобразится соответствующее сообщение и откроется его карточка. Описание процесса работы с карточкой пользователя приведено в п. 2.1.3.

2.3.2. Добавление группы пользователей вручную

При добавлении группы пользователей вручную доступно:

- добавление статической группы пользователей (пп. 2.3.2.1);
- добавление динамической группы пользователей (пп. 2.3.2.2).

2.3.2.1. Добавление статической группы пользователей

ПРИМЕЧАНИЕ. Состав правил статической группы Администратор может редактировать вручную.

Для добавления статической группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить статическую группу» (см. Рисунок 116);
- в открывшемся окне (Рисунок 118) заполнить поля (Таблица 35).

Таблица 35

Поле ввода	Значение	Примечание
Имя группы	Название группы пользователей	Поле обязательно для заполнения. Название группы пользователей должно быть уникальным
Комментарий	Дополнительная информация к группе пользователей	Поле не обязательно для заполнения

- нажать кнопку «Создать» (Рисунок 118).

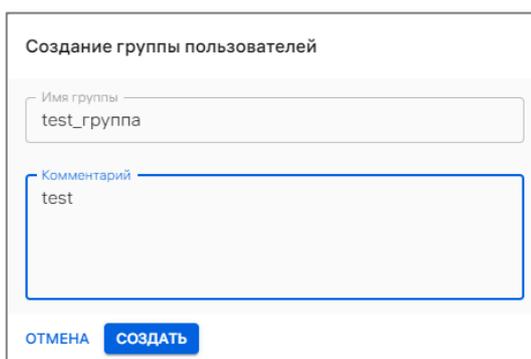


Рисунок 118

В результате успешного создания группы пользователей отобразится соответствующее сообщение и откроется карточка добавленной группы пользователей. Подробное описание работы с карточкой группы пользователей приведено в п. 2.1.4.

2.3.2.2. Добавление динамической группы пользователей

Динамическая группа – группа с заданными условиями, при соблюдении которых пользователи попадают в группу автоматически.

ПРИМЕЧАНИЕ. Нельзя создать несколько динамических групп с одинаковыми условиями. В случае попытки создания еще 1 динамической группы отобразится сообщение об ошибке. Такую группу невозможно удалить (кнопка «Удалить» неактивна).

ПРИМЕЧАНИЕ. Перед тем, как создать динамическую группу пользователей, необходимо настроить интеграцию с сервером LDAP (пп. 4.1.4.3).

Для добавления динамической группы необходимо выполнить следующие действия:

- 1) Перейти в подраздел «Пользователи» раздела «Управление»;
- 2) Нажать кнопку «Добавить»;
- 3) В раскрывающемся списке выбрать пункт «Добавить динамическую группу» (см. Рисунок 116);
- 4) В открывшемся окне (Рисунок 119) заполнить поля, приведенные в таблице (см. Таблица 35);

5) В блоке «Принцип добавления в группу» в раскрывающемся списке «По дополнительным атрибутам пользователя LDAP» выбрать нужный атрибут и затем задать его значение одним из способов:

- если требуется выполнить поиск по точному совпадению атрибута, в поле «Значение» ввести необходимое значение атрибута;
- если требуется задать регулярное выражение для поиска, установить галочку в чекбоксе «Регулярное выражение» и в поле «Значение» ввести необходимое регулярное выражение.

ВНИМАНИЕ! При использовании регулярного выражения необходимо учитывать следующие ограничения:

- регулярное выражение должно быть задано по POSIX стандарту;
- возможен отказ в обслуживании с помощью регулярного выражения (<https://en.wikipedia.org/wiki/ReDoS>) посредством Администратора Платформы управления;
- не определена производительность создания динамических групп пользователей с помощью регулярного выражения, например, при наличии в базе данных десятков тысяч пользователей;

6) Нажать кнопку «Создать».

В результате успешного создания группы пользователей отобразится соответствующее сообщение и откроется карточка добавленной группы пользователей. Подробное описание работы с карточкой группы пользователей приведено в п. 2.1.4.

МОНИТОРИНГ УПРАВЛЕНИЕ АДМИНИСТРИРОВАНИЕ ? А Администратор Первый (а...

УСТРОЙСТВА ПОЛЬЗОВАТЕЛИ ПОЛИТИКИ СЦЕНАРИИ ФАЙЛЫ ПРИЛОЖЕНИЯ ВИТРИНЫ С

< Создание динамической группы пользователей

Имя группы
Группа

Комментарий
Группа пользователей из LDAP

Принцип добавления в группу

По дополнительным атрибутам пользователя LDAP

По дополнительным атрибутам пользователя LDAP
extraAttr

Регулярное выражение

Значение
^M{1}\$

СОЗДАТЬ

Рисунок 119

2.3.3. Добавление пользователей или группы пользователей с помощью CSV-файла

Добавление и обновление, а также привязку пользователей или групп пользователей в ПУ, можно выполнить с помощью подготовленного шаблона импорта. Шаблон предоставляется в виде CSV-файла.

2.3.3.1. Шаблон CSV-файла

CSV-файл возможно создать вручную или скачать и заполнить шаблон.

Для загрузки шаблона CSV-файла необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 116);

– в открывшемся окне нажать «Шаблон .CSV ↓» (Рисунок 120), в результате шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 36).

Импорт пользователей из CSV

Имя импортируемого файла .csv —

Размер менее 400 МБ — Заголовки столбцов — [Подготовка файла для импорта](#)

Кодировка UTF-8 — Строки — [Настройки импорта на 1 шаге](#)

Формат CSV — Всего ошибок — **Шаблон .CSV**

Особые условия импортирования

Если ошибки в распознавании

Если наложение записей

Импорт пользователей в группу

Выберите или перетащите в это окно
заполненный файл с пользователями

ЗАГРУЗИТЬ ФАЙЛ

[ЗАКРЫТЬ](#)

Рисунок 120

Пример заполненного CSV-файла:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMBER,IMEI,SN,ETHERNET_MAC,WLAN_MAC
Пользователи INOI T10,i.ivanov@doc.ru,Игорь,Иванов,,Дежурный,9000900000,350081328638495,,,
Пользователи MIG C55,d.dolin@doc.ru,Дмитрий,Долин,,Руководитель,9000100000,350422453760656,,,
```

Также возможно заполнить CSV-файл в табличном виде (Рисунок 121).

Пример:

GROUP	EMAIL	FIRST_NAME	LAST_NAME	PATRONYMIC	JOB_TITLE	PHONE_NUMBER	IMEI	SN	ETHERNET_MAC	WLAN_MAC
Пользователи INOI T10	i.ivanov@doc.ru	Игорь	Иванов		Дежурный	9000900000	350081328638495			
Пользователи MIG C55	d.dolin@doc.ru	Дмитрий	Долин		Руководитель	9000100000	350422453760656			

Рисунок 121

ПРИМЕЧАНИЕ. При больших значениях чисел (например, IMEI) необходимо выбрать числовой формат ячейки и количество десятичных знаков, равное 0.

Файл для импорта должен соответствовать следующим требованиям:

- размер файла не должен превышать 400 МБ. Импортировать файл размером 400 МБ рекомендуется при скорости подключения к сети Интернет 100 Мбит/сек и выше. Если скорость подключения к сети Интернет менее 100 Мбит/сек, рекомендуется разделить файл на несколько частей и загружать их поочередно;

- формат файла – .csv;

- кодировка файла – UTF-8.

ПРИМЕЧАНИЕ. Скачанный шаблон CSV-файла имеет нужный формат и кодировку;

- первая строка файла должна содержать названия полей с разделителем (например, "GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMBER,IMEI,SN,ETHERNET_MAC,WLAN_MAC,STRATEGY").

ПРИМЕЧАНИЕ. После столбца WLAN_MAC может быть добавлен необязательный столбец STRATEGY. Он заполняется в случае необходимости указать стратегию разрешения конфликтов для конкретной строки. Подробнее см. в описании столбца ниже.

Разделитель для всех полей файла определяется по первой строке. В качестве разделителей может использоваться любой символ, кроме: \r, \n и символа замены Unicode (0xFFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «а».

Описание требований к значениям параметров приведено в таблице (Таблица 36).

Таблица 36

Параметр	Описание	Примечание
GROUP	Название группы пользователей, к которой необходимо привязать пользователя. Содержит от 2 до 64 символов	Параметр обязателен для заполнения при: – создании группы пользователей; – привязке пользователя к существующей группе. ПРИМЕЧАНИЕ. Если в окне настройки импорта в особых условиях выбрана опция «Автоматически создать новую группу с временем и датой импорта» или «Выбрать группу из имеющихся», пользователь будет привязан и к новой/выбранной в опции группе, и к группе, указанной в файле
EMAIL	Рабочая почта пользователя. Должна быть уникальной для каждого пользователя и содержать 1 до 256 символов	Параметр обязателен для заполнения при: – добавлении нового пользователя;
FIRST_NAME	Имя пользователя. Содержит следующие буквы и символы: а-я, А-Я, а-z, А- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	– привязке пользователя к группе

Параметр	Описание	Примечание
LAST_NAME	Фамилия пользователя. Содержит следующие буквы и символы: а-я, А-Я, а-z, А- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	
PATRONYMIC	Отчество пользователя. Содержит следующие буквы и символы: а-я, А-Я, а-z, А- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
JOB_TITLE	Должность пользователя в компании. Содержит следующие буквы и символы: а-я, А-Я, а-z, А- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
PHONE_NUMBER	Номер рабочего телефона пользователя. Содержит только цифры. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
IMEI	Международный идентификатор мобильного оборудования. Содержит 15 цифр	Параметр обязателен для заполнения, если устройство с указанным IMEI необходимо привязать к пользователю
SN	Серийный номер, который присвоен устройству производителем. Содержит от 1 до 20 символов	Параметр обязателен для заполнения, если устройство с указанным серийным номером необходимо привязать к пользователю
ETHERNET_MAC	MAC-адрес Ethernet устройства. Содержит 6 пар символов, разделенных двоеточием	Параметр обязателен для заполнения, если устройство с указанным MAC-адресом Ethernet необходимо привязать к пользователю
WLAN_MAC	MAC-адрес WLAN устройства. Содержит 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	Параметр обязателен для заполнения, если устройство с указанным MAC-адресом WLAN необходимо привязать к пользователю

Параметр	Описание	Примечание
STRATEGY	<p>Правило разрешения конфликтующих записей.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> – SKIP или S – в результате конфликтующая запись не будет перезаписана. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то будут созданы все связи пользователя с группами из файла; – REPLACE или R – в результате конфликтующая запись будет перезаписана. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то пользователь будет отвязан от всех групп, в которых он состоял ранее в системе, и привязан ко всем группам из файла 	<p>Параметр не обязателен для заполнения.</p> <p>Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта</p>

2.3.3.2. Добавление пользователей или группы пользователей с помощью CSV-файла

Для импорта пользователей и группы пользователей, а также привязки пользователей к группе пользователей в Консоли администратора ПУ необходимо выполнить следующие действия:

- подготовить CSV-файл для импорта (пп. 2.3.3.1);
- перейти в подраздел «Пользователи» раздела «Управление»;
- нажать кнопку «Добавить»;
- в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 116);
- в открывшемся окне задать особые условия импортирования, приведенные в таблице (Таблица 37);

Таблица 37

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 122 [1]):	В поле содержится подсказка, доступная для

Наименование полей	Описание	Примечание
	<p>– Прекратить импорт и вернуть файл с описанием ошибок – при обнаружении ошибок будет остановлен импорт и сформирован файл с перечислением некорректных строк и указанием причин ошибок;</p> <p>– Продолжить импорт и вернуть два файла с ошибками и без – импорт продолжится с корректными записями, и после его завершения будут сформированы 2 файла:</p> <ul style="list-style-type: none"> • файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств 	<p>просмотра при наведении курсора на значок  (Рисунок 122 [1],[2]). В результате отобразится текст подсказки следующего содержания: «При завершении импорта система предоставит 2 файла: список системных сообщений ошибок</p>
Если наложение записей	<p>Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 122 [2]):</p> <p>– Игнорировать новую запись, оставить старую – в результате конфликтующие записи не будут перезаписаны. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то будут созданы все связи пользователя с группами из файла;</p> <p>– Перезаписывать новую строку поверх прежней – в результате конфликтующие записи будут перезаписаны. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то пользователь будет отвязан от всех групп, в которые он входил, и привязан ко всем группам из файла.</p> <p>ПРИМЕЧАНИЕ. Если в CSV-файле заполнен столбец «STRATEGY», правило разрешения конфликтов из этого столбца будет иметь приоритет над указанным правилом при настройке импорта. Описание процесса заполнения CSV-файла приведено в пп. 2.3.3.1</p>	<p>распознавания и Журнал успешно импортированных устройств»</p>

Наименование полей	Описание	Примечание
Импорт пользователей в группу	<p>Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 122 [3]):</p> <ul style="list-style-type: none"> – Автоматически создать новую группу с временем и датой импорта – в результате будет создана новая группа пользователей (с типом  «Группа пользователей»), в которую будут включены все импортируемые пользователи. Если в CSV-файле для пользователя указана группа (значение в столбце «GROUP»), то такой пользователь будет включен в новую группу и в указанную в файле группу; – Не создавать группу – в результате пользователи будут добавлены только в группы, указанные в CSV-файле; – Выбрать группу из имеющихся – выберите из раскрывающегося списка группу, в которую необходимо включить импортированных пользователей. Если в CSV-файле для пользователя указана группа (значение в столбце «GROUP»), то пользователь будет включен как в группу, указанную в файле, так и в группу, выбранную на этом шаге 	<p>В поле содержится подсказка, доступная для просмотра при наведении курсора на значок  (Рисунок 122 [3]). В результате отобразится текст подсказки следующего содержания: «В процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую»</p>

Импорт пользователей из CSV

Имя импортируемого файла .csv —

Размер менее 400 МБ — Заголовки столбцов — [Подготовка файла для импорта](#) 

Кодировка UTF-8 — Строки — [Настройки импорта на 1 шаге](#) 

Формат CSV — Всего ошибок — [Шаблон .CSV](#) 

Особые условия импортирования

Если ошибки в распознавании Прекратить импорт и вернуть файл с описанием ошибок ▾  — 1

Если наложение записей Игнорировать новую запись, оставить старую ▾  — 2

Импорт пользователей в группы Автоматически создать новую группу с временем и датой импорта ▾  — 3

Выберите или перетащите в это окно
заполненный файл с пользователями

ЗАГРУЗИТЬ ФАЙЛ — 4

[ЗАКРЫТЬ](#)

Рисунок 122

АДМГ.20134-01 90 01-3

- далее необходимо загрузить CSV-файл одним из способов:
 - переместить CSV-файл в область загрузки;
 - нажать кнопку «Загрузить файл» (см. Рисунок 122 [4]) с последующим выбором файла для импорта;
- в результате будет запущен импорт пользователей из CSV-файла и отобразится шкала загрузки импорта.

Если заполненный файл был загружен корректно или файл содержал ошибки, но при этом в особых условиях импортирования была выбрана опция «Продолжить импорт и вернуть 2 файла с ошибками и без», импорт будет завершен. В окне с результатами импорта шкала загрузки импорта будет заполнена до конца (Рисунок 123).

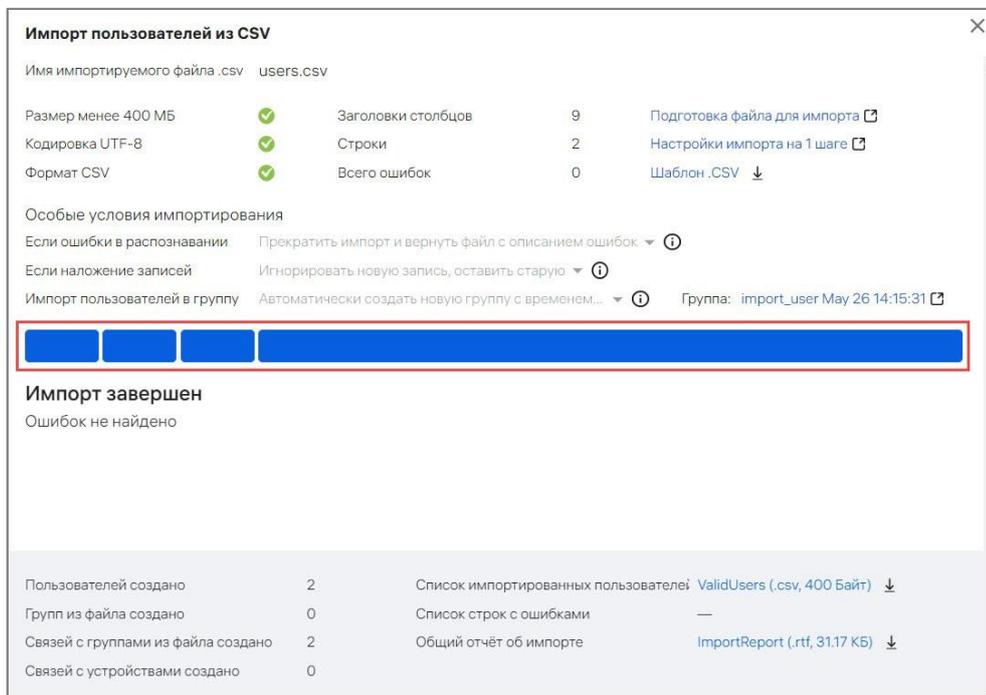


Рисунок 123

Если заполненный файл был загружен некорректно и при этом в особых условиях импортирования была выбрана опция «Прекратить импорт и вернуть файл с описанием ошибок», импорт будет остановлен. В окне с результатами импорта шкала загрузки импорта устройств будет прервана на этапе, где были обнаружены ошибки (Рисунок 124 [6]).

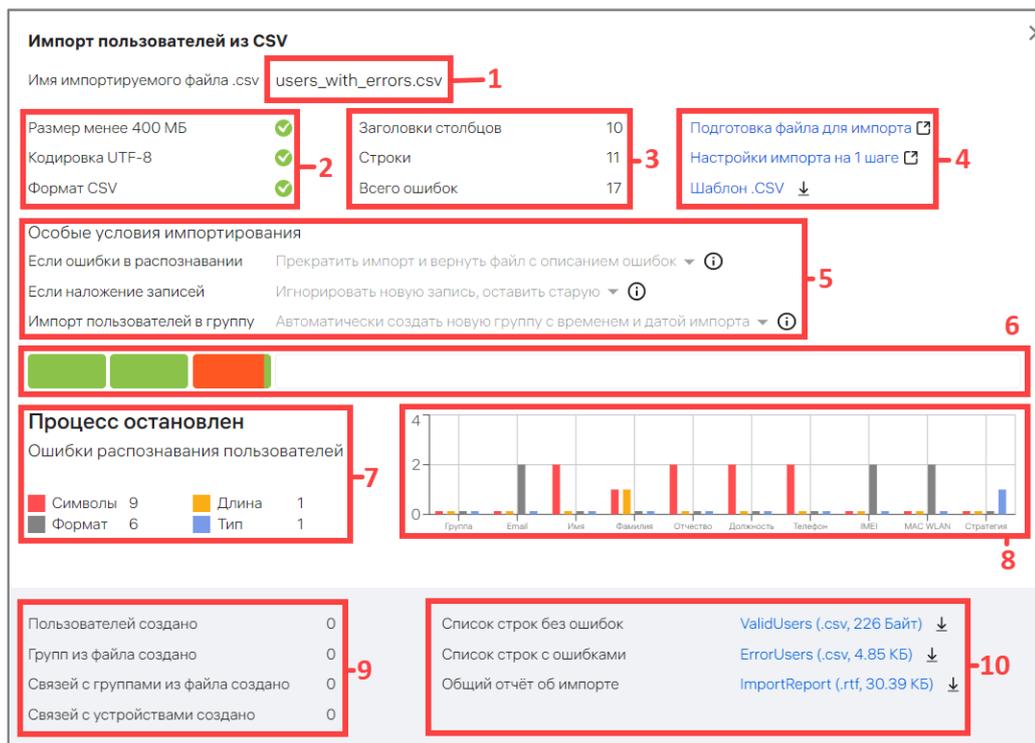


Рисунок 124

В окне с результатами импорта пользователей отображается следующая информация:

- название импортируемого файла (см. Рисунок 124 [1]);
- соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 124 [2]);
- количество столбцов, всех импортируемых строк и ошибок в файле (при их наличии) (см. Рисунок 124 [3]);
- ссылки (см. Рисунок 124 [4]):
 - **Подготовка файла для импорта**, при нажатии на которую произойдет переход на статью справки, описывающую требования и процесс подготовки CSV-файла для импорта пользователей;
 - **Настройки импорта на 1 шаге**, при нажатии на которую произойдет переход на статью справки, описывающую шаги импорта;
 - **Шаблон .CSV**, при нажатии на которую произойдет скачивание шаблона CSV-файла для импорта пользователей;
 - особые условия импортирования (см. Рисунок 124 [5]), см. Таблица 37);
 - шкала прогресса импорта (см. Рисунок 124 [6]);
 - сообщение о завершении импорта или прерывании процесса из-за ошибок (см. Рисунок 124 [7]);
 - графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (см. Рисунок 124 [8]);

- количество созданных пользователей, групп пользователей, связей пользователей с группами и устройствами (см. Рисунок 124 [9]);
- ссылки на скачивание отчетов (см. Рисунок 124 [10]):
 - отчет со списком импортированных пользователей. Формат отчета – `.csv`;
 - отчет со списком ошибок, описание которых приведено в подраздел 5.2. Формат отчета – `.csv` (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);
 - отчет с общей информацией об импорте. Формат отчета – `.rtf`.

Отследить процесс выполнения импорта также возможно в окне «Процессы» подраздела «Индикаторы» раздела «Мониторинг». Более подробная информация приведена в разделе 3.

2.3.4. Привязка пользователей к группе пользователей

В Консоли администратора ПУ предусмотрена возможность привязки пользователя к группе пользователей, которая может быть выполнена:

- с помощью списка быстрых действий (пп. 2.3.4.1);
- вручную через карточку пользователя (пп. 2.3.4.2);
- вручную через карточку группы пользователей (пп. 2.3.4.3);
- с помощью импорта CSV-файла (п. 2.3.3);
- с помощью импорта из LDAP-сервера (пп. 4.1.4.3.1.1).

2.3.4.1. Привязка пользователей к группе пользователей с помощью списка быстрых действий

Привязка пользователей к группам с помощью списка быстрых действий возможна одним из способов:

- через список пользователей;
- через список групп пользователей.

Для этого необходимо:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать:
 - «Поиск по пользователям» – для привязки пользователей через список пользователей;
 - «Поиск по группам» – для привязки пользователей через список групп пользователей;
- выбрать пользователей с типом  «Пользователь»/  «Группа пользователей», установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 125 [1], Рисунок 126 [1]);

– в списке быстрых действий выбрать значок  (Рисунок 125 [2]) или  (Рисунок 126 [2]) «Привязать пользователей к группам»;

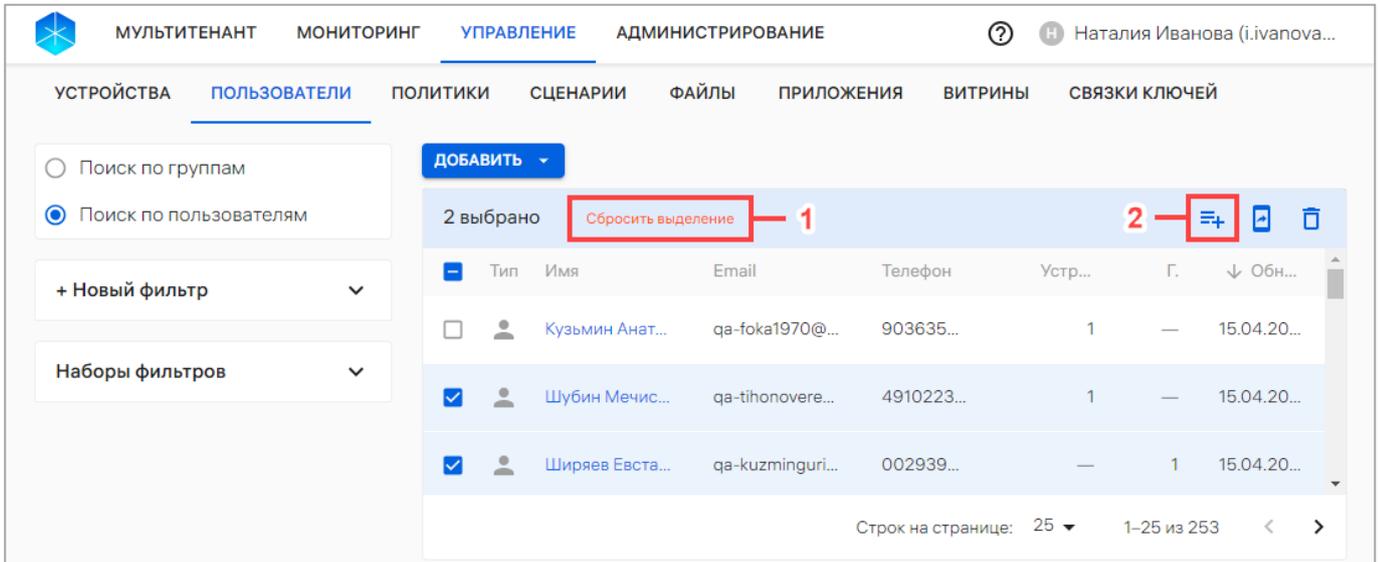


Рисунок 125

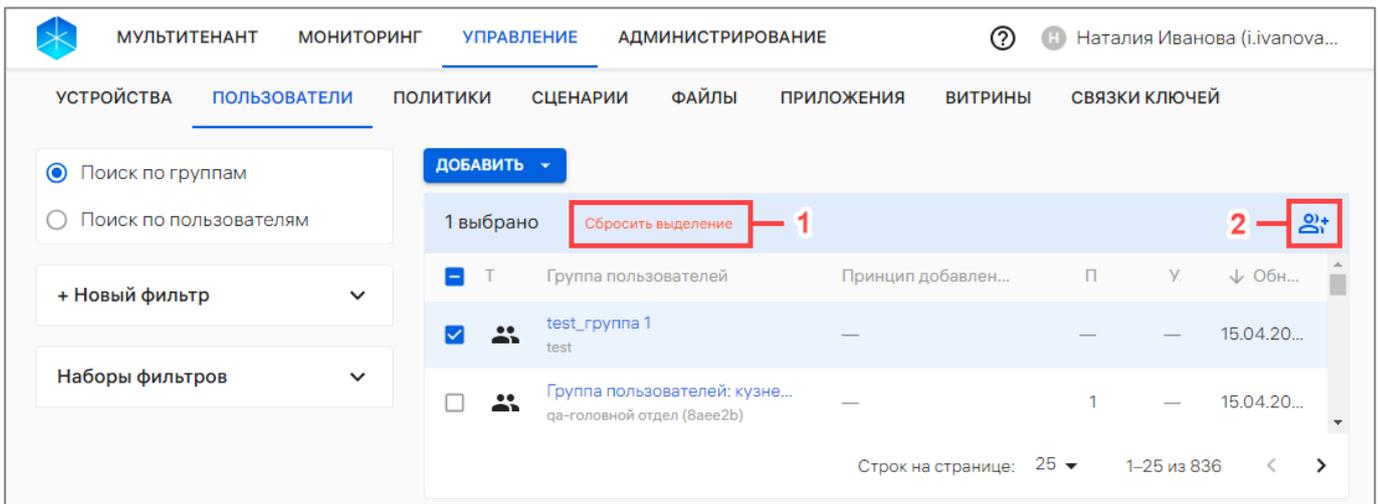


Рисунок 126

– в отобразившемся окне выбрать необходимую группу пользователей (Рисунок 127[1]) или пользователя (Рисунок 128 [1]) из раскрывающегося списка или воспользоваться фильтром. Далее при необходимости возможно добавить дополнительную группу/пользователя, выбрав из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка, нажав значок  «Убрать из списка» справа от названия группы пользователей/пользователя (Рисунок 127 [3], Рисунок 128 [3]).

ПРИМЕЧАНИЕ. Группы с типом «Организационное подразделение» недоступны в списке для выбора, т.к. их состав невозможно изменить вручную;

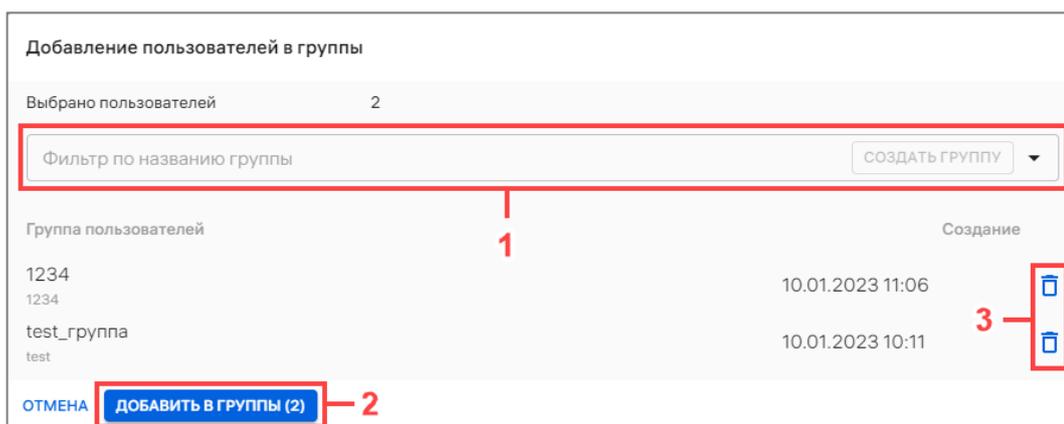


Рисунок 127



Рисунок 128

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 129 [1]) и нажав кнопку «Создать группу» (Рисунок 129 [2]). В результате успешного создания группы отобразится соответствующее сообщение;



Рисунок 129

– нажать кнопку «Добавить в группы» (см. Рисунок 127 [2]) или «Добавить пользователей» (см. Рисунок 128 [2]). В результате успешной привязки пользователей к группам отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу пользователей назначена политика и/или офлайн-сценарий, они начнут действовать для устройств, привязанных к пользователям.

2.3.4.2. Привязка пользователей к группе пользователей через карточку пользователя

Для привязки к пользователю группы пользователей через карточку пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- выбрать в области фильтров «Поиск по пользователям»;
- нажать на имя пользователя для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке пользователя перейти во вкладку «Группы»;
- нажать кнопку «Добавить в группы» (Рисунок 130);
- в отобразившемся окне (см. Рисунок 127) выполнить действия, описанные в пп. 2.3.4.1.

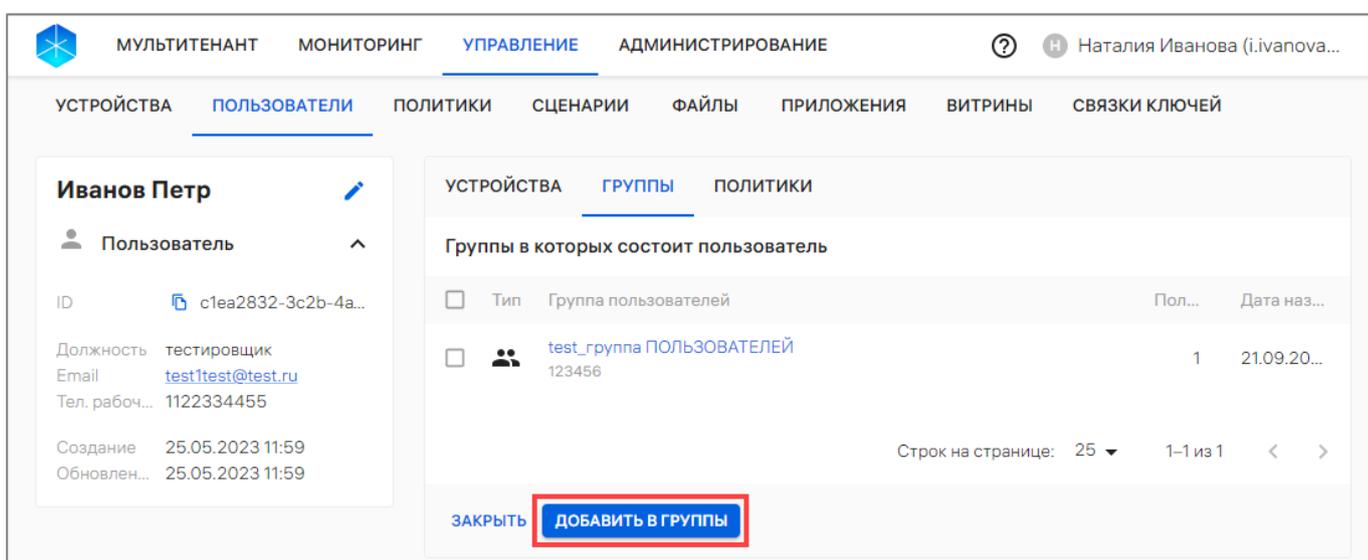


Рисунок 130

2.3.4.3. Привязать пользователей к группе пользователей через карточку группы пользователей

ПРИМЕЧАНИЕ. В группы с типом  «Группа пользователей» возможно добавить только пользователей с типом  «Пользователь».

Для привязки одного или нескольких пользователей к группе пользователей через карточку группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- выбрать в области фильтров «Поиск по группам»;
- нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке группы перейти во вкладку «Пользователи»;
- нажать кнопку «Привязать пользователей» (см. Рисунок 39 [2]);

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте или номеру телефона (Рисунок 131 [1]). Далее при необходимости возможно добавить дополнительного пользователя, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранного пользователя, нажав значок  «Убрать из списка» (Рисунок 131 [3]).

ПРИМЕЧАНИЕ. В списке отображаются только пользователи с типом  «Пользователь»;

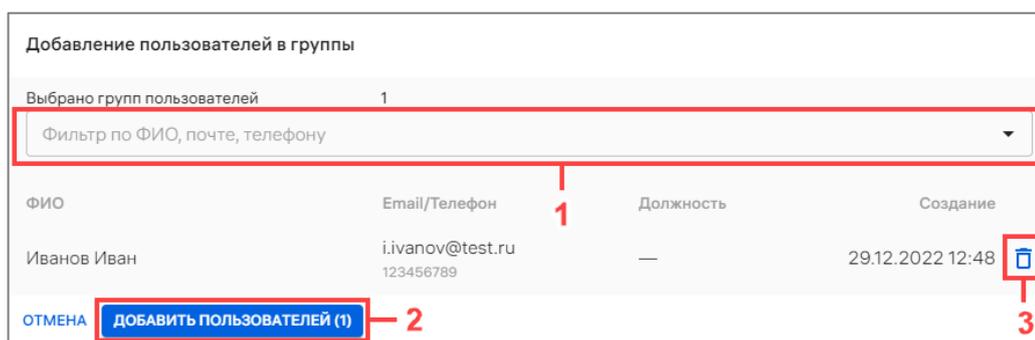


Рисунок 131

– далее нажать кнопку «Добавить пользователей» (см. Рисунок 131 [2]). В результате успешной привязки пользователя к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу пользователей назначена политика и/или офлайн-сценарий, они начнут действовать для активированных устройств, привязанных к пользователям.

2.3.5. Привязка пользователей к устройствам

2.3.5.1. Привязка пользователей к устройствам с помощью списка быстрых действий

Для привязки пользователей к устройствам с помощью списка быстрых действий необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по пользователям»;
- выбрать пользователя, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 132 [1]);

- в списке быстрых действий выбрать значок  «Привязать устройства к пользователям» (Рисунок 132 [2]);

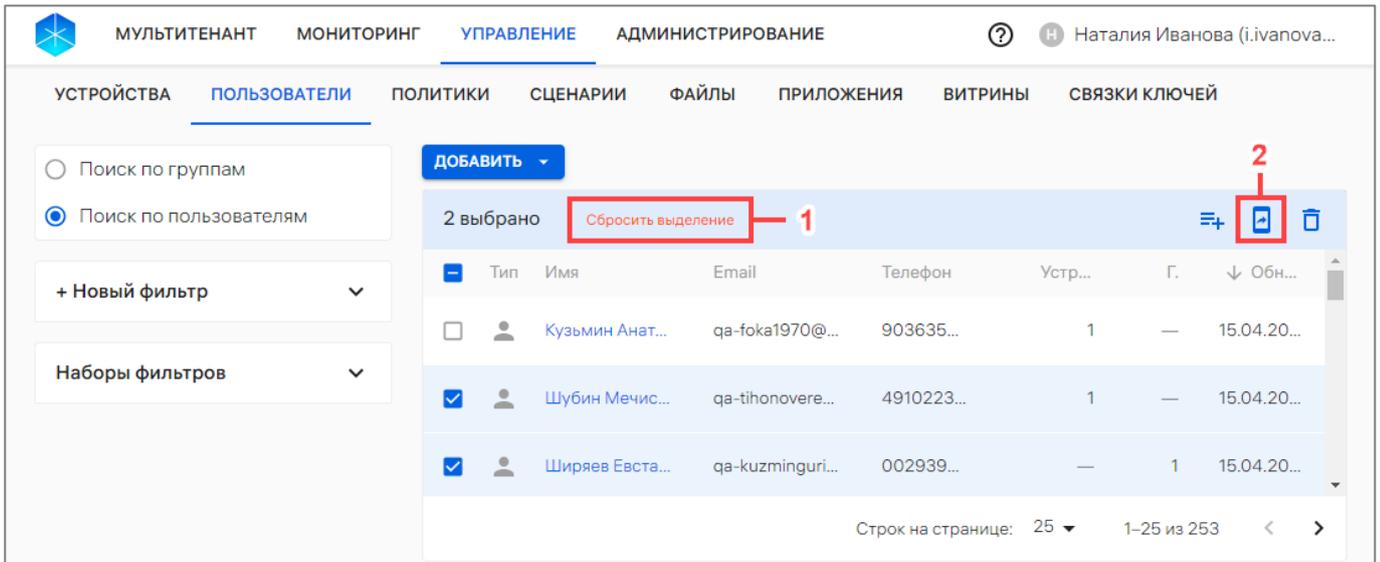


Рисунок 132

– в отобразившемся окне выбрать устройства из раскрывающегося списка или воспользоваться фильтром по идентификатору или комментарию (Рисунок 133 [1]). Далее при необходимости возможно добавить дополнительные устройства, выбрав их из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранные устройства, нажав значок  «Убрать из списка» справа от устройства (Рисунок 133 [3]);

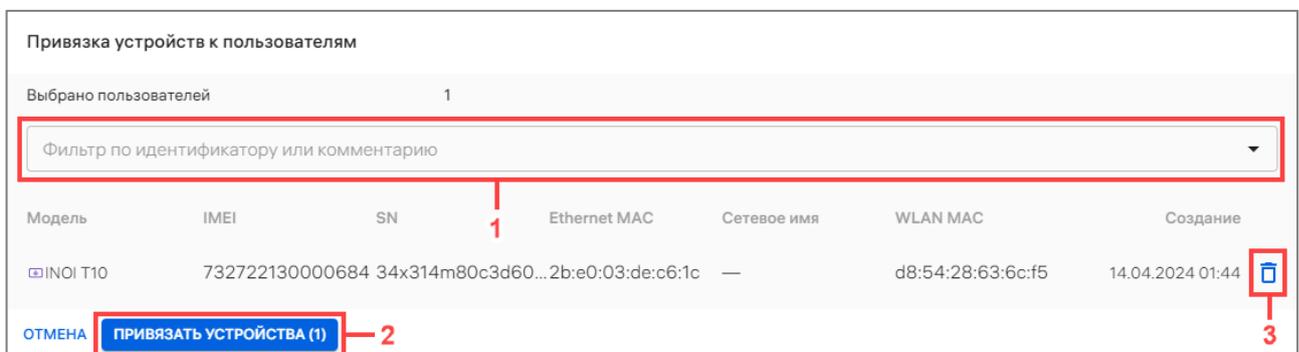


Рисунок 133

– нажать кнопку «Привязать устройства» (см. Рисунок 133 [2]).

В результате успешной привязки устройства отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу, в которую включен пользователь, назначены политика и/или офлайн-сценарии, они начнут действовать на устройстве (если оно активировано).

2.3.5.2. Привязка пользователей к устройствам через карточку пользователя

Для привязки пользователей к устройствам через карточку пользователя необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по пользователям»;
- нажать на имя пользователя для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке пользователя перейти во вкладку «Устройства»;
- нажать кнопку «Привязать устройства» (см. Рисунок 35 [2]);
- в отобразившемся окне (см. Рисунок 133) выполнить действия, описанные в пп. 2.3.5.1.

2.3.6. Отвязать (исключить) пользователей из группы пользователей

 Исключить пользователей с типом «Пользователь» из групп с типом «Группа пользователей» возможно вручную.

Исключить пользователей с типом  «Пользователь из орг. подразделения» из группы с типом  «Организационное подразделение» возможно только через синхронизацию с LDAP-сервером.

Исключить пользователя из группы с типом  «Группа пользователей» возможно через:

- карточку пользователя (пп. 2.3.6.1);
- карточку группы пользователей (пп. 2.3.6.2).

2.3.6.1. Исключение пользователя из группы пользователей через карточку пользователя

Для исключения пользователя из группы пользователей через карточку пользователя необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по пользователям»;
- нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в карточке пользователя перейти во вкладку «Группы»;
- выбрать группу пользователей, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 134 [1]);
- в списке быстрых действий нажать значок  «Исключить пользователя из группы» (Рисунок 134 [2]);

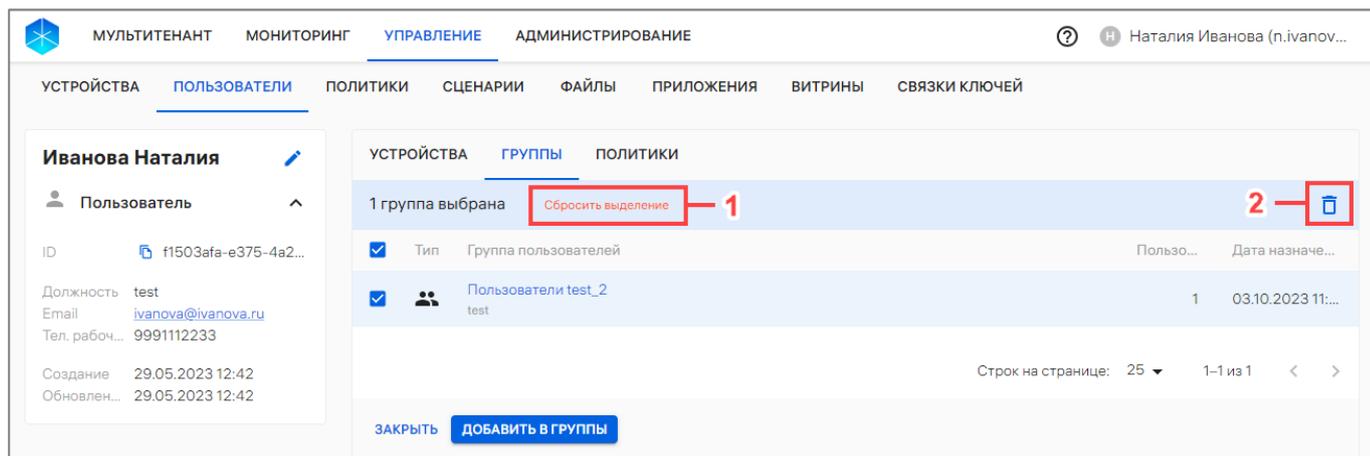


Рисунок 134

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешного исключения пользователя из группы политики будут перекомбинированы таким образом, что для устройства, привязанного к пользователю, будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.3.6.2. Отвязка пользователя от группы пользователей через карточку группы пользователей

Отвязать пользователя возможно через карточку группы пользователя, выполнив следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в карточке группы пользователей перейти во вкладку «Пользователи»;
- выбрать пользователя, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение» (Рисунок 135 [1]);
- в списке быстрых действий нажать значок  «Отвязать пользователей от группы» (Рисунок 135 [2]);

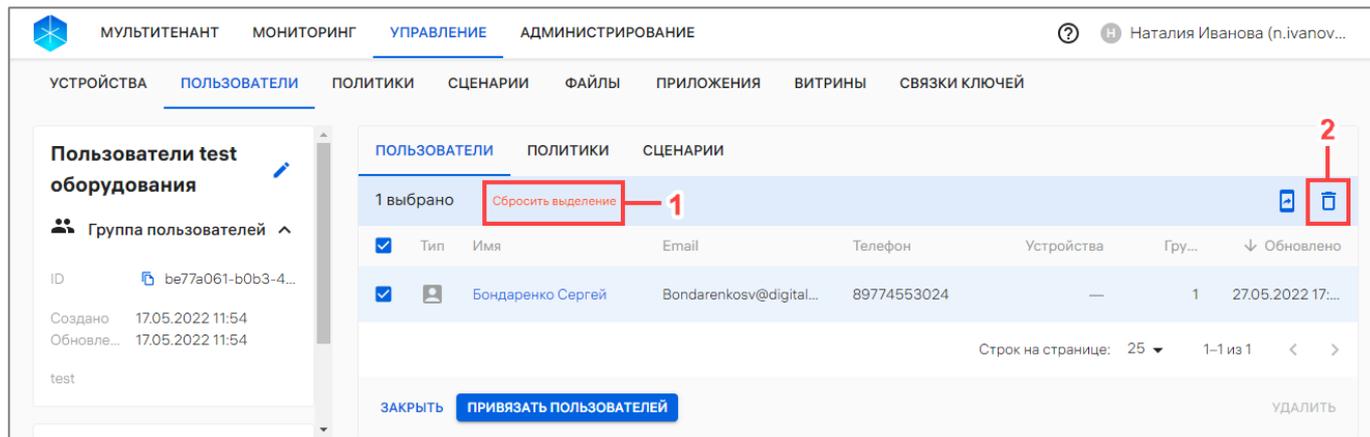


Рисунок 135

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 136);

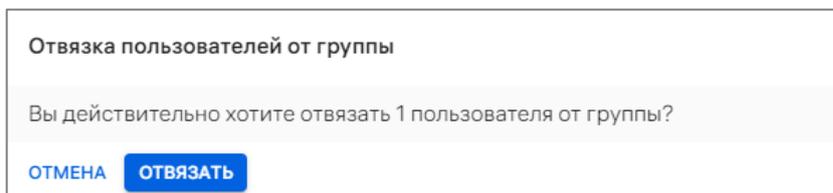


Рисунок 136

В результате успешной отвязки пользователя от группы, политики будут перекомбинированы таким образом, что для устройства, привязанного к пользователю, будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.3.7. Архивирование пользователя

Администратор Платформы управления имеет возможность архивировать пользователя, который был добавлен вручную или с помощью импорта CSV-файла. Пользователь будет заархивирован со всеми его связями с группами и устройствами.

ВНИМАНИЕ! Архивирование пользователя из Орг. Подразделения невозможно.

Архивировать пользователя возможно одним из следующих способов:

1) Через карточку пользователя. Для это необходимо:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по пользователям»;
- выбрать из списка пользователя с типом , при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку пользователя;
- в открывшейся карточке пользователя перейти во вкладку «Устройства» и нажать кнопку «Архивировать» (Рисунок 137);

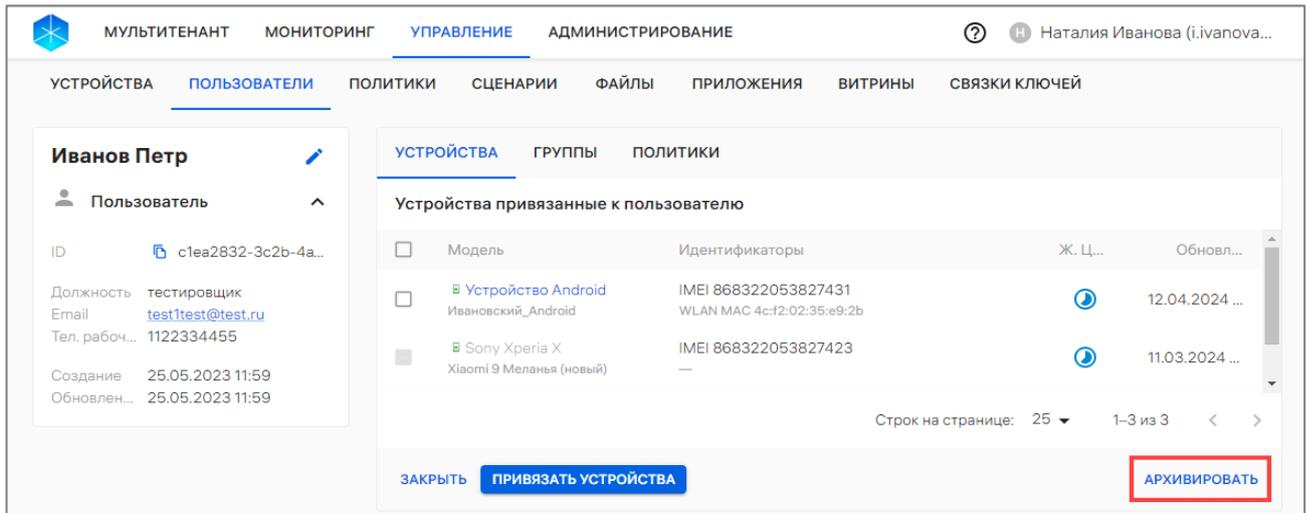


Рисунок 137

- в отобразившемся окне подтвердить либо отменить действия (Рисунок 138);

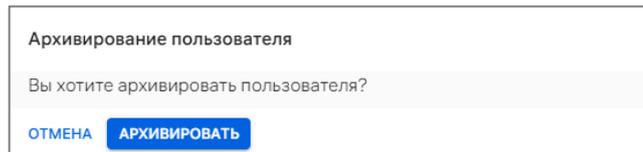


Рисунок 138

2) С помощью списка быстрых действий. Для это необходимо:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по пользователям»;
- выбрать пользователя с типом , установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 139 [1]);
- в списке быстрых действий выбрать значок  «Архивировать пользователя» (Рисунок 139 [2]);

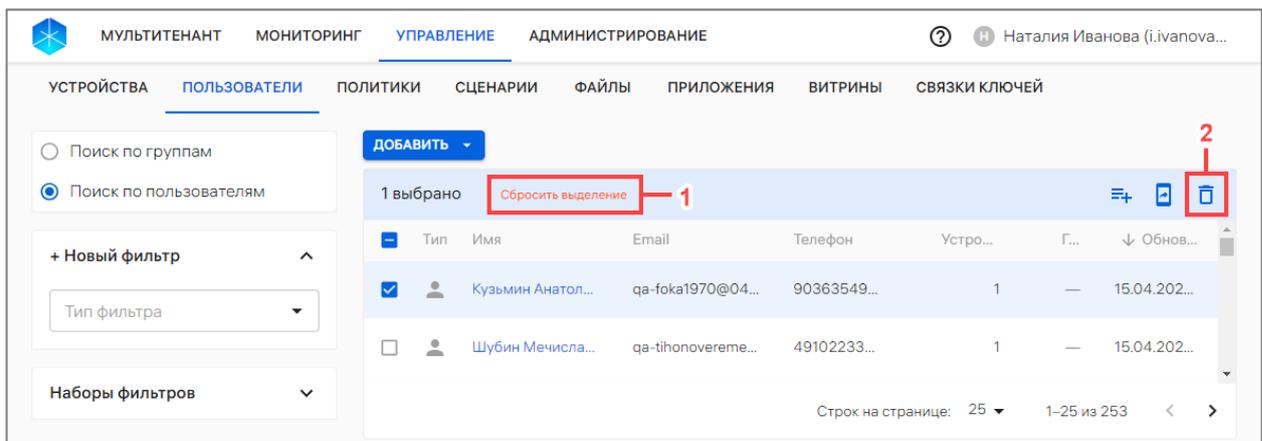


Рисунок 139

- в отобразившемся окне подтвердить либо отменить действия (см. Рисунок 138).

В результате успешного архивирования отобразится соответствующее сообщение. Заархивированные пользователи не будут отображаться в списке пользователей.

2.3.8. Удаление группы пользователей

ВНИМАНИЕ! Удаление группы пользователей с типом  «Организационное подразделение» возможно только через синхронизацию с LDAP-сервером (пп. 4.1.4.3.3).

Удаление группы пользователей с типом «Группа пользователей» и «Динамическая группа» возможно вручную. Для этого необходимо:

- предварительно исключить всех пользователей из группы – для группы с типом «Группа пользователей» (п. 2.3.6);
- отвязать группу пользователей от всех политик (п. 2.4.7) и офлайн-сценариев (п. 2.5.3) – для динамической группы.

После выполнения условий, приведенных выше, группа с типом «Группа пользователей» и «Динамическая группа» может быть удалена из ПУ. Для этого необходимо:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке нажать кнопку «Удалить» (Рисунок 140);

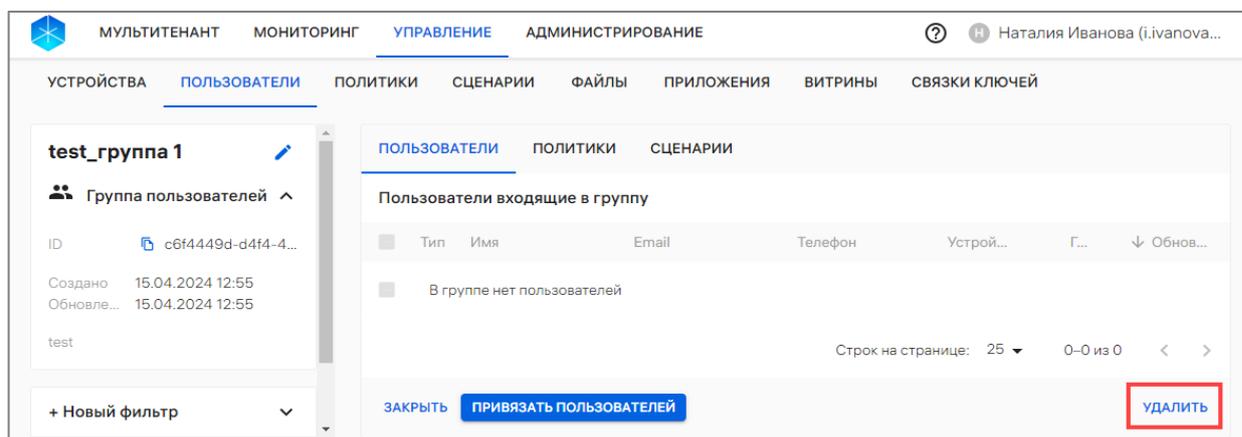


Рисунок 140

- в открывшемся окне (Рисунок 141) подтвердить либо отменить действия.

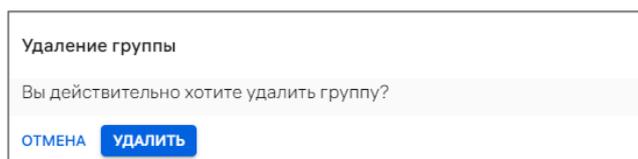


Рисунок 141

В результате успешного удаления отобразится соответствующее сообщение.

2.4. Подраздел «Политики»

Подраздел «Политики» Консоли администратора ПУ предназначен для работы и управления политиками и корпоративным шаблоном политик, которые могут быть назначены на группы устройств или группы пользователей.

ПРИМЕЧАНИЕ. Для корректного управления устройством необходимо, чтобы:

- на устройстве было выставлено корректное время и был задан часовой пояс;
- версия ППО совпадала с версией приложения «Аврора Центр» на устройстве

(важно, после обновления ППО обновить также и версию приложения на устройстве).

Для управления устройством на базе ОС Аврора необходимо перевести устройство в режим администратора.

ПРИМЕЧАНИЕ. Если устройство в режиме пользователя, необходимо назначить и дождаться применения на устройстве политики с правилом «Настройки пользователя/Создать пользователя».

Для перехода в подраздел «Политики» необходимо в верхней панели раздела «Управление» выбрать подраздел «Политики». В результате отобразится список политик, а при их отсутствии отображается сообщение «Нет данных».

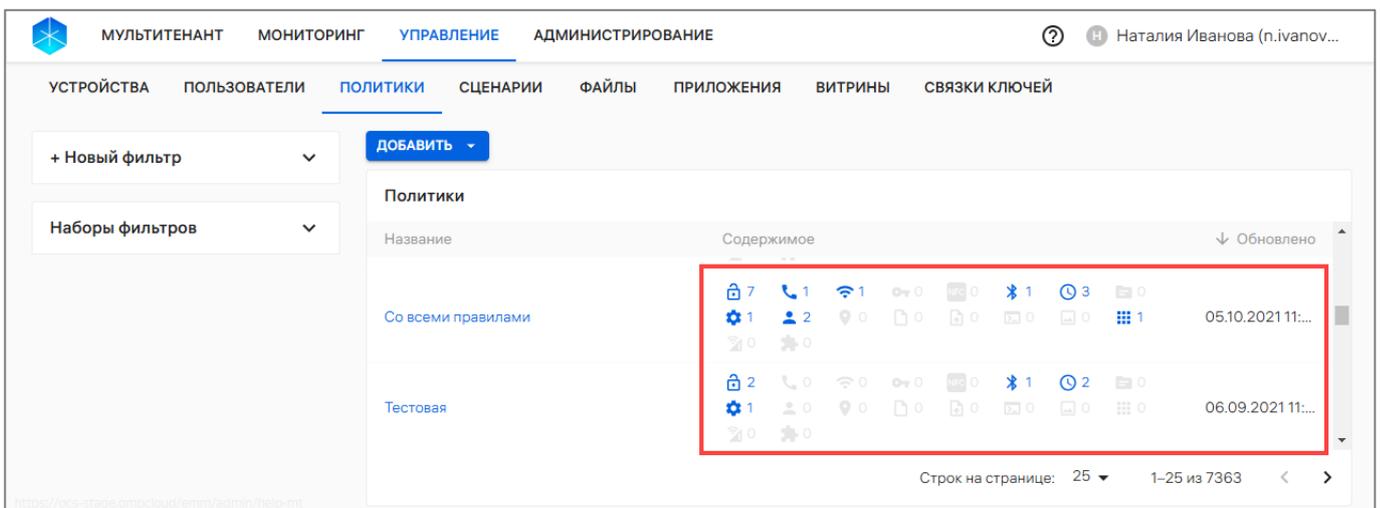


Рисунок 142

В рабочей области подраздела «Политики» (см. Рисунок 142) информация о политике отображается в столбцах, приведенных в таблице (Таблица 38).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 38

Название столбца	Значение	Описание
Название	Название политики	Представляет собой активную ссылку, при нажатии на которую происходит переход к карточке политики
	Комментарий	Дополнительная информация к политике. Заполняется при необходимости
Содержимое	Категория правил в политике	 Ограничение доступа
		 Голосовые вызовы
		 Конфигурация WLAN
		 Конфигурация VPN
		 Конфигурация NFS
		 Конфигурация Bluetooth®
		 Конфигурация
		 Конфигурация репозиториев
		 Система
		 Настройки пользователя
		 Геопозиционирование
		 Файлы
		 Файлы с устройства
		 Скрипты
		 Внешний вид
		 Приложения
 Мобильная сеть		
	Количество правил	Количество правил в категории
Обновлено	Дата и время последнего обновления политики	

Добавление политики возможно одним из следующих способов:

- вручную (п. 2.4.2);
- на основе корпоративного шаблона (п. 2.4.3);
- на основе существующей политики (п. 2.4.4).

Существует возможность добавления в политику правил как во время, так и после ее создания.

Список правил политик, доступных для каждой версии ОС, приведен в таблице (Таблица 39).

Приложение «Аврора Центр» с периодичностью раз в час проверяет, какие политики, офлайн-сценарии и команды оперативного управления назначены на устройство (если политикой не задана другая периодичность). В случае несовпадения текущего и целевого состояния устройства, переприменяет необходимые опции управления.

ПРИМЕЧАНИЕ. В связи с использованием более ранних версий программного интерфейса (API), в управлении устройствами с ОС Android версий 7-8 выделяют следующие особенности:

- пользователь может вручную отключить геолокацию, которая включена перманентно на управляемых устройствах с ОС Android;

- режим киоска, блокировка экрана и установка приложений работают с особенностями (подробное описание приведено в таблице (Таблица 39)).

Таблица 39

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
1	Ограничение доступа/Блокировка экрана	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.1
2	Ограничение доступа/Использование камеры	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.2
3	Ограничение доступа/Снимки экрана	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.3
4	Ограничение доступа/Управление авиарежимом	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.4
5	Ограничение доступа/Управление точкой доступа WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.5
6	Ограничение доступа/Управление Bluetooth	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.6
7	Ограничение доступа/Использование браузера	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.7
8	Ограничение доступа/Управление датой и временем	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.8
9	Ограничение доступа/Передача данных MTP	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.9

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
10	Ограничение доступа/Использование микрофона	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.10
11	Ограничение доступа/Сброс к заводским настройкам	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.11
12	Ограничение доступа/Использование USB-накопителей	4.1.0 и выше	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.12
13	Ограничение доступа/Использование SD-карт	4.1.0 и выше	-	-	-	-	-	пп. 2.4.1.13
14	Ограничение доступа/Отправка и получение SMS	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.14
15	Ограничение доступа/Режим киоска	-	7 и выше	-	-	-	-	пп. 2.4.1.15
16	Голосовые вызовы/Исходящие вызовы	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.16
17	Голосовые вызовы/Входящие вызовы	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.17
18	Конфигурация WLAN/Режим работы WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.18
19	Конфигурация WLAN/Подключения к сети WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.19

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
20	Конфигурация VPN/Подключения VPN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.20
21	Конфигурация NFC/Управление NFC	5 и выше	-	-	-	-	-	пп. 2.4.1.21
22	Конфигурация Bluetooth/Режим работы Bluetooth	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.22
23	Конфигурация/Расписание получения команд	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.23
24	Конфигурация/Расписание отправки состояния	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.24
25	Конфигурация/Расписание отправки событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.25
26	Конфигурация/Исключения событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.26
27	Конфигурация/Хранение логов на устройстве	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.27
28	Конфигурация/Обновление координат в клиенте Аврора Центр	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.28
29	Конфигурация/Создание точек восстановления	-	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.29
30	Конфигурация/Настройка прокси-сервера	-	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.30

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
31	Конфигурация/Таймаут экрана	-	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.31
32	Конфигурация репозитория/Подключение системных репозитория	-	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.32
33	Система/Обновление ОС	4.0.2 и выше	-	p10	-	-	-	пп. 2.4.1.33
34	Настройки пользователя/Требования к паролю	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.34
35	Настройки пользователя/Создать пользователя	4.0.2 и выше	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.35
36	Настройки пользователя/Сертификаты пользователя	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.36
37	Файлы/Доставка на устройство	-	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.37
38	Файлы с устройства/Загрузка файлов с устройств	-	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.38
39	Скрипты/Выполнение на устройстве	-	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.39

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
40	Геопозиционирование/ Настройки режима работы геопозиционирования	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.40
41	Внешний вид/Установка фона рабочего стола	-	7 и выше	-	-	-	-	пп. 2.4.1.41
42	Внешний вид/Отображение идентификаторов в клиенте Аврора Центр	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.42
43	Приложения/Управление приложениями	4.0.2 и выше	7 и выше	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.43
44	Мобильная сеть/Точка доступа	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.44
45	Мобильная сеть/Управление мобильной передачей данных	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.45

2.4.1. Общее описание правил политик

2.4.1.1. Ограничение доступа/Блокировка экрана

Правило позволяет разблокировать или заблокировать экран устройства с выводом сообщения.

Выбор значения из списка:

– «Заблокирован» – данное значение выбрано по умолчанию при добавлении правила, а также доступно поле для ввода сообщения, которое будет отображаться на заблокированном экране. Экстренные вызовы остаются доступны;

– «Разблокирован».

ВНИМАНИЕ! На устройствах на базе ОС Android:

– при блокировке экрана также блокируется передача данных по MTP и исходящие вызовы (кроме экстренных). Поэтому если на устройство назначена политика с разрешением передачи данных по MTP и/или исходящих вызовов, то в карточке устройств будет отображаться статус «Не соответствует политике»;

– в зависимости от производителя и версии ОС Android поведение блокировки экрана может отличаться, например:

- если устройство защищено PIN-кодом, то после перезагрузки на экране ввода PIN-кода может быть доступно верхнее меню;

- перезагрузка устройства касанием соответствующей кнопки в интерфейсе может быть недоступна (например, данное поведение наблюдается на устройстве Samsung). В этом случае осуществлять перезагрузку устройства данного производителя следует с помощью комбинации кнопок на корпусе (в соответствии с документацией производителя);

- на устройствах Huawei на базе ОС Android версии 9 выявлена следующая проблема: если в окне вызова вручную ввести номер, отличный от экстренного, и попытаться совершить вызов, то вызов не произойдет ни в этом случае, ни после изменения номера на экстренный. Для решения проблемы следует вернуться на Экран блокировки и повторить экстренный вызов.

ПРИМЕЧАНИЕ. На устройствах с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0:

– в режиме блокировки необходимо вводить пароль при каждом включении экрана, если устройство защищено паролем;

– при попытке выключить устройство будет отображено окно, в котором возможно не только выключить или перезагрузить устройство, но и включить авиарежим, несмотря на запрещающее правило политики. Если включить авиарежим, то будет отображено окно с уведомлением и инструкцией как отключить авиарежим (Рисунок 143).

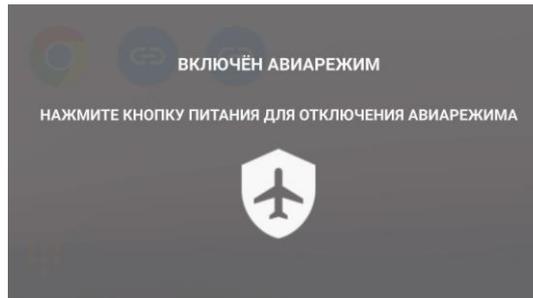


Рисунок 143

2.4.1.2. Ограничение доступа/Использование камеры

Правило разрешает или запрещает использование камеры на устройствах.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.3. Ограничение доступа/Снимки экрана

Правило разрешает или запрещает создание скриншотов с экрана устройства.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.4. Ограничение доступа/Управление авиарежимом

Правило разрешает или запрещает использование авиарежима на устройствах.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.5. Ограничение доступа/Управление точкой доступа WLAN

Правило фиксирует текущее состояние точки доступа WLAN. Разрешает или запрещает вносить изменения в настройки точки доступа WLAN.

ПРИМЕЧАНИЕ. Для устройств Huawei и Honor на базе ОС Android при запрещающем правиле раздача интернета в режиме модема отключается, но пользователь может вручную включить и отключить точку доступа, а также изменить ее настройки.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.6. Ограничение доступа/Управление Bluetooth

Правило фиксирует текущее состояние Bluetooth®. Запрещает или разрешает вносить изменения в настройки Bluetooth®.

ВНИМАНИЕ! Для устройств на базе ОС Android версии 9, если Bluetooth® был включен, то после применения правила он может отображаться как выключенный в настройках, но при этом Bluetooth® продолжит работать.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.7. Ограничение доступа/Использование браузера

Правило разрешает или запрещает использование браузера на устройствах.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.8. Ограничение доступа/Управление датой и временем

Правило фиксирует текущие дату и время на устройствах. Разрешает или запрещает вносить изменения в дату и время.

ПРИМЕЧАНИЯ:

✓ Для устройств на базе ОС Аврора и ОС Android изменение времени в меньшую сторону от реального может привести к тому, что записи о произошедших операциях перестанут отображаться в журнале приложения «Аврора Центр». Поэтому рекомендуется назначить политику с правилом по запрету управления датой и временем;

✓ Для некоторых устройств на базе ОС Android правило по запрету изменения даты и времени может оставлять возможность изменения часового пояса (в частности, на Huawei Y9).

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.9. Ограничение доступа/Передача данных MTP

Правило разрешает или запрещает передачу данных через USB-соединение.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.10. Ограничение доступа/Использование микрофона

Правило запрещает или разрешает использование микрофона для записи звука на устройствах.

Выбор значения из списка:

- «Разрешено»;

– «Запрещено» (микрофон будет недоступен для записи звука во всех приложениях и внешних устройствах, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов). При добавлении правила значение выбрано по умолчанию.

2.4.1.11. Ограничение доступа/Сброс к заводским настройкам

Правило запрещает или разрешает сброс к заводским настройкам.

Выбор значения из списка:

- «Разрешен»;
- «Запрещен» (при добавлении правила значение выбрано по умолчанию).

2.4.1.12. Ограничение доступа/Использование USB-накопителей

Правило запрещает или разрешает использование USB-накопителей.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

Особенности применения политики на устройствах с ОС Аврора:

– если применить запрещающее правило в момент использования подключенного USB-накопителя (например, какой-либо файл с USB-накопителя открыт), то USB-накопитель не отключится. Также на устройстве могут возникнуть ошибки, после которых USB-накопитель останется доступен;

– если после применения запрещающего правила разрешить использование USB-накопителей, то устройство начнет видеть их через 1-2 минуты или после извлечения и повторного подключения USB-кабеля;

– при применении запрещающего правила на устройстве INOI P4903 сообщение о блокировке в пункте меню «Хранилище» в подразделе «Настройки» отображается не полностью.

Особенности применения политики на устройствах с ОС семейства Linux: если в момент применения запрещающего правила политики USB-накопитель подключен к устройству и на нем происходит чтение/запись, то будет производиться попытка размонтировки раз в час USB-накопителя и его блокировки, либо USB-накопитель будет запрещен после перезагрузки устройства.

2.4.1.13. Ограничение доступа/Использование SD-карт

Правило запрещает или разрешает использование SD-карт.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

ПРИМЕЧАНИЯ:

- ✓ В случае применения запрещающего правила в момент просмотра:
 - каталога с SD-карты в приложении «Файлы», данный каталог будет доступен для просмотра до его закрытия;
 - файла с SD-карты, данный файл будет доступен для просмотра до его закрытия;
- ✓ Если после запрета разрешить использование SD-карт, то устройство начнет видеть их после перезагрузки или после ручного включения в пункте меню «Хранилище» в подразделе «Настройки».

2.4.1.14.Ограничение доступа/Отправка и получение SMS

Правило разрешает или запрещает отправку и получение SMS-сообщений на устройстве.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

После назначения политики с правилом по запрету приема и отправки SMS:

- 1) Блокируется отправка сообщений на экстренные номера;
- 2) Стандартное приложение для отправки и получения SMS:
 - на устройствах с **ОС Аврора**:
 - ярлык приложения исчезнет. Если приложение было открыто и в этот момент пришла политика по запрету приема и отправки SMS, то пользователь останется в открытом приложении, но не сможет получать и отправлять новые SMS;
 - если при получении вызова пользователь отвечает отправкой быстрого сообщения, то пользователь в истории сможет увидеть, что сообщение было отправлено, но не доставлено;
 - на устройствах с **ОС Android** будет доступно для открытия, но недоступно для взаимодействия;
 - 3) Только на устройствах с ОС Android при использовании сторонних приложений для SMS либо не будет возможности в него попасть, либо не будет возможности с его помощью отправить SMS;
 - 4) При использовании нецелевых приложений для отправки сообщений (например, через приложение с вызовами, контактами, заметками и т.п.):
 - на устройствах с **ОС Android**:
 - будет неудачная попытка отправки;
 - для некоторых версий ОС при попытке отправить сообщение через нецелевое приложение (например, «Контакты») данное приложение «зависнет» и для восстановления работоспособности необходимо перезапустить приложение;
 - на устройствах **ОС Аврора** ничего не произойдет. Но при этом пользователь сможет ознакомиться с историей сообщений (через приложение «Контакты») и/или

открыть приложение с сообщениями (такое же поведение может произойти после отправки SMS после завершения вызова);

5) В зависимости от ОС и прошивки запрет может распространяться также и на MMS-сообщения.

После снятия политики по запрету отправки и получения SMS в некоторых случаях:

– для **ОС Аврора** может потребоваться перезагрузка устройства для корректной работы с SMS. При этом сообщения, которые пользователь пытался отправить при запрете, невозможно будет отправить после снятия запрета, для их отправки необходимо пересоздать сообщения;

– для некоторых версий **ОС Android** созданные ранее SMS-диалоги могут исчезнуть.

2.4.1.15. Ограничения доступа/Режим киоска

Правило позволяет активировать на устройствах режим киоска, в результате чего будут доступны только указанные в политике приложения, ярлыки веб-страниц и сайты, а также позволяет отключить верхнее меню.

Для создания правила необходимо выполнить следующие действия:

1) В поле «Включен» возможно включить или выключить режим киоска с помощью переключателя (Рисунок 144).

ПРИМЕЧАНИЕ. При добавлении правила переключатель по умолчанию включен;

2) В поле «Отключение панели уведомлений» выключить переключатель, если в режиме киоска требуется отключить верхнее меню.

ПРИМЕЧАНИЕ. При добавлении правила переключатель по умолчанию выключен.

ВНИМАНИЕ! Управление панелью уведомлений возможно для устройств с ОС Android 9 и выше;

3) В поле «Код выхода из режима киоска» ввести код, состоящий из 8 цифр. Также возможно сгенерировать код автоматически, нажав кнопку  «Сгенерировать пароль» в правой части строки.

ПРИМЕЧАНИЕ. Поле обязательно для заполнения, если режим киоска включен;

4) Для параметра «Цвет шрифта» доступен выбор одного из значений:

– «По умолчанию» – цвет шрифта остается тот, который был в системе до назначения и применения политики с правилом режима киоска;

– «Выбор цвета» – при выборе данного значения становится доступным:

- поле для ввода HEX-кода;
- окно с цветовой палитрой для выбора необходимого цвета;

АДМГ.20134-01 90 01-3

5) Для параметра «Фон» доступен выбор одного из значений:

- «Системное изображение» — фон остается системным, который был до назначения и применения политики с правилом режима киоска;
- «Выбор цвета» – при выборе данного значения становится доступным:
 - поле для ввода HEX-кода;
 - окно с цветовой палитрой для выбора необходимого цвета;

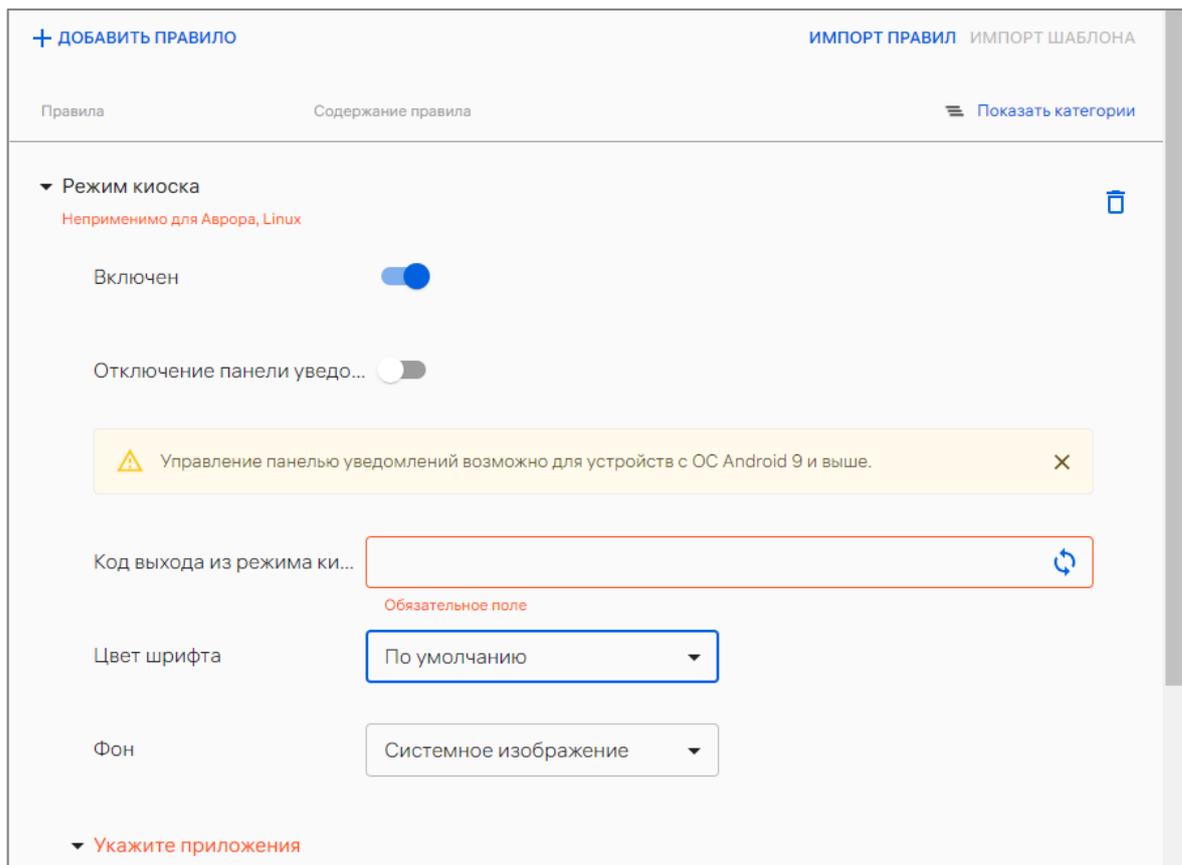


Рисунок 144

6) В блоке «Приложения» указать приложения и их порядок расположения (Рисунок 145), которые будут доступны пользователю в режиме киоска. Для этого следует в поле «Код приложения» ввести название пакета приложения (необходимые данные доступны для просмотра в карточке устройства в столбце «Инфо» (пп. 2.1.1.9).

Если требуется добавить еще одно приложение, то необходимо нажать на значок **+** в левом нижнем углу и повторить действия описанные выше.

Если требуется изменить порядок расположения приложений необходимо воспользоваться кнопками **▲** **▼**.

ПРИМЕЧАНИЕ. Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного ярлыка веб-страницы;

Рисунок 145

7) Добавить ярлыки веб-страниц, позволяющих открыть необходимые сайты (Рисунок 146), выполнив следующие действия:

– в блоке «Ярлыки веб-страниц/Укажите ярлыки веб-страниц» нажать на значок **+**;

– в поле «Название ярлыка» ввести название ярлыка (может содержать от 1 до 20 символов);

– в поле «URL» ввести электронный адрес необходимого сайта/страницы в формате URL. Например: [https:// www.omp.ru/](https://www.omp.ru/).

ПРИМЕЧАНИЯ:

✓ Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного приложения;

✓ Возможно добавление нескольких ярлыков веб-страниц;

Рисунок 146

8) Настроить список разрешенных/запрещенных сайтов. Доступно, если в качестве браузера по умолчанию используется Chrome (Рисунок 147).

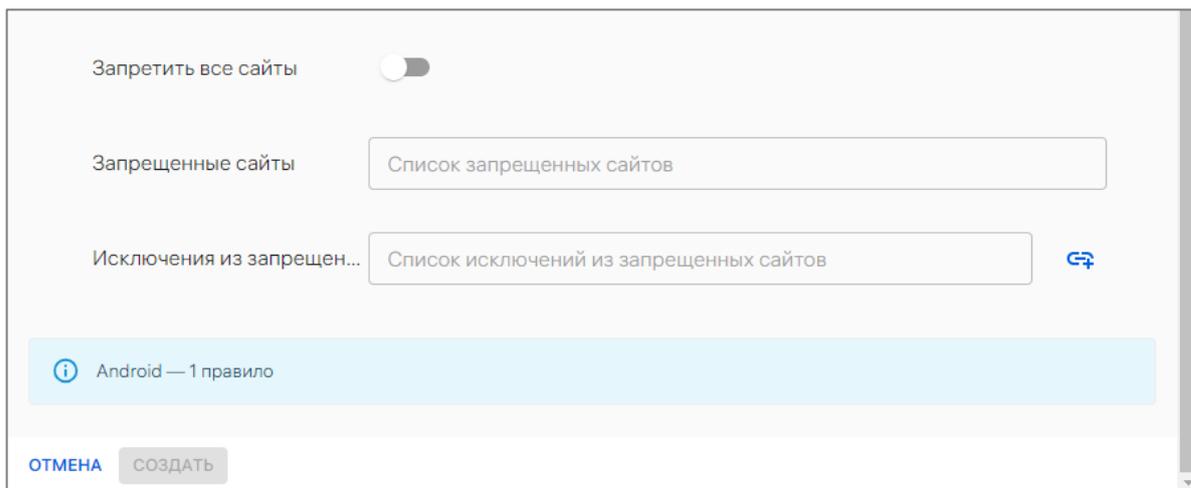


Рисунок 147

Для настройки списка разрешенных сайтов необходимо:

- перевести переключатель «Запретить все сайты» в положение «Включено»;
- в поле «Исключения из запрещенных сайтов» ввести электронный адрес разрешенного сайта в формате URL (например: <https://www.ompr.ru/>) и нажать Enter.

ПРИМЕЧАНИЯ:

✓ С помощью кнопки  «Добавить ярлыки в список исключений». Также возможно добавить в разрешенный список адреса сайтов из ярлыков, которые указаны на шаге 7;

✓ Возможно добавление нескольких разрешенных сайтов.

Для настройки списка запрещенных сайтов необходимо:

- убедиться, что переключатель «Запретить все сайты» находится в положении «Выключено»;

– в поле «Запрещенные сайты» ввести электронный адрес запрещенного сайта в формате URL (например: <https://www.ompr.ru/>) и нажать Enter.

ПРИМЕЧАНИЯ:

✓ Возможно добавление нескольких запрещенных сайтов;

✓ Необходимо добавлять в списки запрещенных/разрешенных сайтов только конечные URL. Например, если заблокировать все сайты, кроме <https://www.ompr.ru/>, то после редиректа он станет <https://ompr.ru/> и разрешение не сработает.

ВНИМАНИЕ! Не рекомендуется выбирать приложение «Аврора Центр» в качестве средства запуска (launcher) как при его установке, так и в дальнейшем. В противном случае выйти из режима киоска будет невозможно.

ПРИМЕЧАНИЯ:

✓ Блокировка экрана имеет приоритет над режимом киоска. При назначении политик с правилами включенной блокировки экрана и включенного режима киоска отобразится Экран блокировки, а в состоянии устройства – информация о включенной блокировке экрана и отключенном режиме киоска, вследствие чего в карточке устройства отобразится статус «Не соответствует политике»;

✓ Если в список разрешенных приложений добавить приложение по работе с файлами, то при открытии файлов будут запускаться обработчики этих файлов, даже если их нет в списке разрешенных приложений. Например, при открытии файла формата .mp3 может запуститься медиаплеер (при его наличии на устройствах);

✓ В целях обеспечения экстренных вызовов в режиме киоска всегда доступно приложение для совершения вызовов. В случае необходимости запретить вызовы следует дополнительно назначить на устройство соответствующую политику;

✓ Ярлыки веб-страниц открываются через браузер, заданный по умолчанию. При этом:

– если заданный по умолчанию браузер выбран, то разрешенным в режиме киоска остается только он. При этом, если заданный по умолчанию браузер не добавлен в список приложений, то его иконка отображаться не будет;

– если заданный по умолчанию браузер не задан, то при открытии ярлыка пользователю будет предложено его выбрать;

✓ Адреса сайтов на кириллице необходимо добавлять в списки разрешенных/запрещенных сайтов в кодировке Punycode;

✓ При первом запуске режима киоска будет запрещен вход в безопасный режим (safeboot) на устройстве;

✓ Если устройство защищено паролем, то в режиме киоска необходимо вводить пароль при каждом включении экрана;

✓ На устройствах с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0, работающих в режиме киоска:

– при попытке выключить устройство будет отображено окно, в котором можно не только выключить или перезагрузить устройство, но и включить авиарежим, даже несмотря на запрещающее правило политики. Если включить авиарежим, то будет отображено окно с уведомлением и инструкцией как отключить авиарежим (см. Рисунок 143);

– переключение между окнами запущенных приложений запрещено;

– системные данные (время, заряд батареи, уровень сигнала WLAN и т.п.) не отображаются в верхней строке состояния;

– панель уведомлений не отображается даже если отображение панели уведомлений разрешено в правиле политики;

✓ На устройствах с ОС Android версии 8.1 при включении режима киоска в момент блокировки экрана стандартным средством ОС, устройство будет не соответствовать политике в Аврора Центр, пока экран не будет разблокирован и устройство не отправит свое актуальное состояние;

✓ Особенности комбинирования политик, которые содержат разные правила режима киоска:

– пересечение приложений, ярлыков: в комбинированном варианте будут приложения и ярлыки из двух политик;

– пересечение запрещенных сайтов: в комбинированном варианте будут запрещенные сайты из двух политик;

– пересечение кодов выхода из киоска: код выхода будет отображен в окне комбинированной политики с перечнем доступных приложений, ярлыков, запрещенных ссылок, выбранного фона. Его необходимо запомнить;

✓ Чтобы отобразить в режиме киоска ярлыки к различным разделам настроек, необходимо в разделе «Приложения» в поле «Код приложения N» указать Activity нужной настройки:

– «Bluetooth»: `com.android.settings/.Settings$BluetoothSettingsActivity`;

– «Wi-Fi»: `com.android.settings/.Settings$WifiSettingsActivity`;

– «Мобильная передача данных»: `com.android.settings/.Settings$WirelessSettingsActivity`;

– «Геолокация»: `com.android.settings/.Settings$LocationSettingsActivity`;

– «Экран и яркость»: `com.android.settings/.Settings$DisplaySettingsActivity`;

– «Звуки и вибрация»: `com.android.settings/.Settings$SoundSettingsActivity`;

– «Настройки SIM», «APN»: `com.android.settings/.Settings$ApnSettingsActivity`.

При этом необходимо учитывать следующие ограничения, которые могут возникнуть на некоторых устройствах и версиях ОС:

– из окна с открытым разделом настроек будет возможность выйти в общие настройки;

– перечисленные выше Activity могут не сработать для открытия разделов настроек. В этом случае необходимо обратиться в техническую поддержку ООО «Открытая мобильная платформа» и в запросе указать проблемное Activity, модель и версию ОС устройства.

2.4.1.16.Голосовые вызовы/Исходящие вызовы

Правило разрешает или запрещает совершение исходящих вызовов с устройства.

Выбор значения из списка:

– «Разрешены»;

– «Запрещены» (при добавлении правила значение выбрано по умолчанию).

2.4.1.17.Голосовые вызовы/Входящие вызовы

Правило разрешает или запрещает входящие вызовы на устройство.

Выбор значения из списка:

– «Разрешены»;

– «Запрещены» (при добавлении правила значение выбрано по умолчанию).

Входящие вызовы не будут отображаться пользователю, а звонящий абонент будет слышать гудки.

2.4.1.18. Конфигурация WLAN/Режим работы WLAN

Правило позволяет:

- отключать или включать адаптер WLAN;
- зафиксировать текущее состояние адаптера WLAN.

Доступные значения для работы WLAN:

- «Не задано» – управление состоянием адаптера WLAN будет разблокировано (раскрывающийся список «Управление WLAN»);
- «Выключено» – адаптер WLAN будет выключен перманентно (включить его будет невозможно). При добавлении правила значение выбрано по умолчанию;
- «Включено» – адаптер WLAN будет включен перманентно (выключить его будет невозможно).

ВНИМАНИЕ! В зависимости от версии и прошивки ОС Android возможно наличие на устройствах пользовательских настроек, способных влиять на назначенную политику:

- журнал управления WLAN (встречается на устройствах Samsung). Позволяет запретить приложению «Аврора Центр» включать/отключать адаптер WLAN;
- автоматическое включение WLAN. Позволяет включать адаптер WLAN, когда устройство обнаружит поблизости одну из сохраненных сетей, и отключать его, если в течение некоторого времени не будет установлено соединение.

Доступные значения для управления состоянием адаптера WLAN:

- «Запрещено» – будет зафиксировано текущее состояние адаптера WLAN. При добавлении правила значение выбрано по умолчанию.

ВНИМАНИЕ! Для устройств на базе ОС Android версии 9 пользователь может вручную включить/отключить WLAN, даже если управление WLAN запрещено;

- «Разрешено» – пользователь может включать или отключать адаптер WLAN и изменять его настройки.

2.4.1.19. Конфигурация WLAN/Подключения к сети WLAN

Правило позволяет создать и настроить на устройствах подключения к сетям WLAN с технологиями безопасности WPA-EAP и WPA2. В результате устройство сможет подключаться к защищенным сетям WLAN без дополнительных действий.

ПРИМЕЧАНИЯ:

- ✓ Правило не сработает, если на устройствах выключен адаптер WLAN;
- ✓ На устройствах, функционирующих под управлением ОС Android, после включения адаптера WLAN и применения правила, момент непосредственного подключения к точке доступа зависит от версии и прошивки ОС. Если подключение к точке доступа не произошло, то следует перезагрузить устройство или выполнить подключение вручную.

Для создания правила необходимо:

1) В поле ввода «Название сети (SSID)» ввести название беспроводной сети (Service Set Identifier) для подключения. Параметр обязателен для заполнения. Название беспроводной сети должно быть уникальным в рамках правила.

ПРИМЕЧАНИЕ. Если разные политики содержат правила с одинаковым названием беспроводной сети, то при их назначении на устройстве будет применено правило с более поздней датой обновления.

ВНИМАНИЕ! Если название подключения WLAN в правиле содержит символ «/» (например, OMP/_test), то:

– на устройстве будет создано подключение WLAN в названии которого не будет указан данный символ (например, OMP_test), в результате чего устройство с символом «/» в названии не сможет подключиться к сети WLAN;

– в карточке устройства на вкладке «Состояние» будут отображены два подключения WLAN – с символом «/» в названии и без него. В результате чего устройство будет в статусе «Не соответствует политике»;

2) В поле «Скрытая сеть» при помощи переключателя возможно включить или отключить трансляцию названия беспроводной сети. При добавлении правила переключатель по умолчанию выключен;

3) В поле «Автоподключение» при помощи переключателя возможно включить или отключить автоподключение устройства к беспроводной сети. При добавлении правила переключатель по умолчанию включен.

ПРИМЕЧАНИЕ. Для устройств на базе ОС Android автоподключение работает следующим образом: в момент создания и настройки подключения будет произведена попытка подключения к точке доступа. В случае неудачи следующая попытка подключения будет произведена в соответствии с особенностями версии и прошивки ОС Android;

4) В поле «Настройка IP-адреса» по умолчанию выставлено значение «Автоматическая». Поле редактированию не подлежит;

5) Если необходимо создать подключение к беспроводной сети с технологией безопасности:

WPA2:

– в раскрывающемся списке «Безопасность» выбрать «WPA2». При добавлении правила значение выбрано по умолчанию;

– в поле «Пароль» ввести пароль беспроводной сети. Параметр не обязателен для заполнения. Если беспроводная сеть не защищена паролем, то необходимо оставить поле пустым.

ПРИМЕЧАНИЯ:

✓ Если пароль не задан, то на устройствах с ОС Android подключение не будет создано и в журнале приложения «Аврора Центр» отобразится запись об ошибке создания подключения, а на устройствах на базе ОС Аврора необходимо будет вручную ввести пароль для подключения к защищенной беспроводной сети;

✓ Пароль хранится в системе в нешифрованном виде. Просмотр пароля возможен:

- в карточке политики во вкладке «Правила» (пп. 2.1.5.1);
- в карточке устройства во вкладке «Политики» (пп. 2.1.1.5).

WPA-EAP:

Создать подключение к беспроводной сети с технологией безопасности WPA-EAP возможно по протоколу:

1. **TLS** (в дополнение к созданию подключения через протокол TLS будет выпущен и доставлен на устройства пользовательский сертификат для подключения к беспроводной сети).

Для подключения к беспроводной сети с технологией безопасности **WPA-EAP** по протоколу **TLS** необходимо:

- в раскрываемом списке «Безопасность» выбрать «WPA-EAP»;
- в раскрываемом списке «Протокол» выбрать «TLS»;
- в раскрываемом списке «Категория сертификата» выбрать категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии требуемой категории в списке необходимо добавить ее в настройках администрирования Аврора Центр (п. 4.1.2);
- в раскрываемом списке «Идентификатор» выбрать динамическую переменную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

- {{UserEmail}} – email из карточки пользователя;
- {{UserPrincipalName}} – значение параметра «userPrincipalName» из LDAP-данных о пользователе.

2. PEAP.

Для подключения к беспроводной сети с технологией безопасности **WPA-EAP** по протоколу **PEAP** необходимо:

- в раскрываемом списке «Безопасность» выбрать «WPA-EAP»;
- в раскрываемом списке «Протокол» выбрать «PEAP»;
- в поле «2-й этап аутентификации» по умолчанию установлено значение «MSCHAPv2». Поле недоступно для редактирования;
- в раскрываемом списке «Тип идентификации» выбрать, какой тип идентификации необходимо использовать:
 - «Шаблон» – значение выбрано по умолчанию. Далее в поле «Идентификатор» в раскрываемом списке выбрать динамическую переменную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

АДМГ.20134-01 90 01-3

- ◆ {{UserEmail}} – email из карточки пользователя;
- ◆ {{UserPrincipalName}} – значение параметра «userPrincipalName» из LDAP-данных о пользователе;
- ◆ {{sAMAccountName}} – значение параметра «sAMAccountName» из LDAP-данных о пользователе.

ПРИМЕЧАНИЕ. Подключение к сети **WPA-EAP PEAP** будет создано с паролем по умолчанию (12345678). После создания подключения необходимо зайти в его настройки и вручную изменить пароль на корректное значение;

- «Логин и пароль». Далее для подключения ввести логин и пароль пользователя в соответствующих полях. В случае незаданного пароля пользователь устройства должен будет ввести его самостоятельно.

ПРИМЕЧАНИЕ. Если требуется сменить пароль в режиме киоска (при отсутствии прав на редактирование подключения), необходимо обратиться к администратору.

ВНИМАНИЕ!

- ✓ Для выпуска сертификата и корректной подстановки значения в динамическую переменную необходимо, чтобы устройство было привязано к пользователю;

- ✓ Если в ПУ к устройствам привязано несколько пользователей, то при создании подключения будут использоваться учетные данные пользователя, который был привязан к устройствам последним или который был получен из интеграции с LDAP. Если из LDAP получены данные нескольких пользователей, то будет выбран тот, который привязан к устройствам последним;

б) Если требуется создать подключение к сети WLAN, настроенной на прокси-сервер, необходимо перевести переключатель «Прокси-сервер» в положение  «Включено» и заполнить следующие поля:

- «Хост» – хост прокси-сервера. Поле обязательно для заполнения;
- «Порт» – по умолчанию задано значение 80. При необходимости доступно ввести другой номер порта. Поле обязательно для заполнения;
- «Исключения из проксирования» – при необходимости ввести через запятую хосты, которые будут исключениями из проксирования. Поле необязательно для заполнения.

ПРИМЕЧАНИЕ. Необходимо учитывать следующие особенности использования прокси-сервера в подключении:

- для устройств с ОС Android настроить прокси-сервер можно только в версиях 8 и выше;
- для устройств с ОС Аврора можно задавать более одного прокси-сервера на подключение. При получении настроек прокси-сервера от ОС, приложение «Аврора Центр» будет работать с прокси-сервером, который будет первым в списке серверов, полученных от ОС;

– если переключатель «Прокси-сервер» в правиле политики выключен, то это не влияет на соответствие устройства политике. После применения политики имеющиеся на устройстве настройки прокси-сервера будут удалены.

Если необходимо создать на устройствах еще одно подключение к сети WLAN, то необходимо нажать значок **+** внизу правила и повторить шаги, приведенные выше.

2.4.1.20. Конфигурация VPN/Подключения VPN

Правило позволяет создать подключение VPN в приложениях:

- Cisco AnyConnect для устройств ОС Android;
- КриптоПро NGate R2 для устройств на базе ОС Android и ОС Аврора.

Для создания правила необходимо:

1) В поле «Название» ввести название подключения VPN, которое должно быть уникальным в рамках правила. Параметр обязателен для заполнения.

ПРИМЕЧАНИЕ. Если разные политики содержат правила с одинаковым названием подключения VPN, то при их назначении на устройство будет применено правило с более поздней датой обновления;

2) В поле «Адрес сервера» ввести адрес сервера VPN. Параметр обязателен для заполнения;

3) В поле «Тип» выбрать одно из приложений, для которого необходимо создать подключение VPN:

– **Cisco AnyConnect** (при добавлении правила значение выбрано по умолчанию):

- в поле «Протокол» по умолчанию указан протокол безопасности SSL. Поле недоступно для редактирования;

- если требуется, чтобы вместе с созданием подключения VPN был выпущен и доставлен на устройство необходимый пользовательский сертификат, то в раскрывающемся списке «Категория сертификата» необходимо выбрать необходимую категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии необходимой категории в списке, требуется добавить ее в подразделе «Настройки» раздела «Администрирование» (п. 4.1.2). Параметр не обязателен для заполнения;

– **КриптоПро NGate R2:**

- в поле «Тип аутентификации» указан тип «По логину и паролю». Поле заполнено по умолчанию и недоступно для редактирования;

- в раскрывающемся списке «Логин» необходимо выбрать динамическую переменную, которая будет автоматически подставлять нужный логин пользователя в подключение:

- ◆ `{{sAMAccountName}}` – логин пользователя (значение параметра «sAMAccountName» из LDAP о пользователе). Пример значения: ivanivanov. При добавлении правила значение выбрано по умолчанию;

◆ {{UserEmail}} – email из карточки пользователя. Пример значения: ivanov@mail.ru;

◆ {{UserPrincipalName}} – логин пользователя (значение параметра «userPrincipalName» из LDAP о пользователе). Пример значения: ivanivanov@mail.ru.

ВНИМАНИЕ! Если в ПУ к устройству привязано несколько пользователей, то при создании подключения будут использоваться учетные данные того пользователя, который был привязан к устройству позднее всех или данные пользователя, которые были получены из интеграции с LDAP. Если из LDAP получены данные нескольких пользователей, то будет выбран пользователь, который привязан к устройству позднее всех;

• в поле «Автозапуск VPN» при помощи переключателя возможно включить или отключить автоподключение устройства к VPN. При добавлении правила переключатель по умолчанию включен.

ПРИМЕЧАНИЕ. Настройка автозапуска действует только для ОС Android;

• поле «Серийный номер лицензии» заполняется, если требуется передать в подключение VPN серийный номер лицензии. Параметр не обязателен для заполнения.

ПРИМЕЧАНИЕ. Передача серийного номера лицензии действует только для ОС Android.

Если необходимо создать еще одно подключение VPN в приложении Cisco AnyConnect для ОС Android, необходимо нажать на значок + внизу правила и повторить шаги, приведенные выше.

ВНИМАНИЕ! Для приложения КриптоПро NGate R2 можно создать только одно подключение VPN.

2.4.1.21. Конфигурация NFC/Управление NFC

Правило фиксирует текущее состояние NFC. Запрещает или разрешает вносить изменения в настройки NFC.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.22. Конфигурация Bluetooth/Режим работы Bluetooth

Правило разрешает или запрещает возможность использовать Bluetooth®.

Выбор значения из списка:

- «Выключен»;
- «Включен» (при добавлении правила значение выбрано по умолчанию).

2.4.1.23. Конфигурация/Расписание получения команд

Правило задает расписание на получение оперативных команд и политик.

Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.24. Конфигурация/Расписание отправки состояния

Правило задает расписание отправки состояния устройства на ПУ. Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.25. Конфигурация/Расписание отправки событий безопасности

Правило задает расписание отправки в ПУ сообщений о событиях безопасности (`security.d journaling daemon`), произошедших на устройстве.

Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.»

2.4.1.26. Конфигурация/Исключения событий безопасности

Правило позволяет исключить отправку определенных событий безопасности с устройств, фильтруя их по процессам и/или уровням.

Для фильтрации:

- по типу события безопасности всех процессов необходимо выбрать «Все процессы» и указать уровень событий, который следует исключить;
- по определенному событию безопасности необходимо ввести ручную путь к исполняемому файлу процесса отправителя события. Также представлена возможность дополнительно указать уровень события, которое следует исключить;
- по второму событию безопасности необходимо нажать на значок **+** внизу фильтра и также ввести ручную путь к исполняемому файлу процесса отправителя события. При необходимости дополнительно указать уровень события, которое следует исключить. Аналогично возможно сделать и для последующих событий безопасности, которые следует исключить.

2.4.1.27. Конфигурация/Хранение логов на устройстве

Правило позволяет задать способ хранения системных сообщений на устройствах.

Выбор значения из списка:

- «Постоянное» (значение выбрано по умолчанию) – системные сообщения хранятся в локальном хранилище устройства и сохраняются после перезагрузки устройства. Правило имеет приоритет в комбинированных политиках;
- «Временное» – системные сообщения хранятся в оперативной памяти устройства и удаляются при перезагрузке устройства.

2.4.1.28. Конфигурация/Обновление координат в клиенте Аврора Центр

Правило задает частоту обновления координат в приложении «Аврора Центр».

ВНИМАНИЕ! Обновление координат в приложении «Аврора Центр» не влияет на частоту актуализации координат самим устройством. Устройство актуализирует свои координаты независимо от того, как часто приложение «Аврора Центр» запрашивает координаты. На частоту актуализации координат устройства влияет режим работы геопозиционирования.

Ввод значения с клавиатуры в формате: «Каждые [чч] ч. [мм] м [сс] с».

ПРИМЕЧАНИЕ. При добавлении правила по умолчанию установлена частота 10 минут (значение: «Каждые [0] ч. [10] м [0] с»).

2.4.1.29. Конфигурация/Создание точек восстановления

ПРИМЕЧАНИЕ. Правило применимо только для устройств с ОС семейства Linux. ОС должна быть установлена на раздел BTRFS с разбивкой на подразделы @ и @home. Другие виды разделов не поддерживаются.

Правило регулирует создание точек восстановления при применении политик и автоматический возврат устройства на ранее созданные точки восстановления.

Для создания правила необходимо:

1) В поле «Исключаемые директории» (определяет директории, которые не будут включены в точку восстановления) в раскрывающемся списке выбрать необходимое значение:

– /home - данные из раздела /home, которые будут исключены только в случае, если для него выделен отдельный раздел на диске. Если раздел не выделен, исключение не произойдет, но работа системы не нарушится;

– пустое значение (выбрано по умолчанию) - исключаемые директории не будут заданы;

2) Если требуется, чтобы происходило автоматическое возвращение устройства на ранее созданные точки восстановления при отсутствии связи приложения «Аврора Центр» с сервером, необходимо перевести переключатель «Автоматическое восстановление» в положение  «Включено» и дополнительно в поле «Интервал» указать нужный временной интервал. По умолчанию переключатель выключен.

ПРИМЕЧАНИЕ. Если после применения политики, соответствующей режиму работы, связь с ПУ оборвется более чем на указанный интервал, произойдет автоматическое возвращение изменений на последнюю точку восстановления.

ВНИМАНИЕ!

✓ Крайне не рекомендуется выставлять значение интервала менее одного часа. В данный интервал входит не только время отсутствия связи при штатной работе, но и время перезагрузки устройства, установки обновлений и т.д.;

✓ По умолчанию проверка выполняется по доступности адреса <http://ipv4.omprussia.ru/>. Однако ПУ может быть недоступен во время аварий и/или проведения технических работ. Для более безопасной работы автовосстановления требуется в конфигурационном файле `config/subsystems/emm/config.yml` найти параметр `networkCheckSettings` и указать в нем стабильный внутренний URL, который будет использоваться для проверки доступности сети. После этого связь будет проверяться по двум адресам, и если хотя бы один из них доступен, то автовосстановления не произойдет;

3) В раскрывающемся списке «Режим работы» выбрать необходимое значение:
– «Только при применении правил, изменяющих файловую систему» (выбрано по умолчанию). Точка восстановления будет создаваться только при применении хотя бы одного из следующих правил политики:

- «Конфигурация репозиториев /Подключение системных репозиториев»;
- «Система/Обновление ОС»;
- «Файлы/Доставка на устройство»;
- «Скрипты/Выполнение на устройстве»;
- «Приложения/Управление приложениями»;

– «Всегда». Точка восстановления будет создаваться при каждом пересчете политик в приложении «Аврора Центр» (1 раз в час).

ВНИМАНИЕ! Точка восстановления будет создаваться только при наличии доступа к сети Интернет. Проверка выполняется по доступности адреса <http://ipv4.omprussia.ru/>. Для более безопасной проверки требуется в конфигурационном файле `/var/ocs/config/subsystems/emm/config.yml` найти параметр `networkCheckSettings` и указать в нем стабильный внутренний URL, который тоже будет использоваться для проверки доступности сети. После этого связь будет проверяться по двум адресам, и если хотя бы один из них доступен, то точка восстановления будет создана.

ПРИМЕЧАНИЕ. При создании точки восстановления система автоматически записывает локальные дату и время устройства. Если на момент создания точки восстановления дата и время устройства были изменены вручную, в дальнейшем это может привести к некорректному возвращению на такие точки. Это связано с тем, что при формировании оперативной команды система «вписывает» значение серверного времени, но точка создается по локальному времени устройства. Например, если на устройстве вручную выставлено 17.03.2024, а серверная дата 17.03.2025, то это резервное копирование данных станет «актуальным» через год.

2.4.1.30. Конфигурация/Настройка прокси-сервера

Правило позволяет настроить подключение к прокси-серверу.

Для создания правила необходимо заполнить следующие поля:

- «Хост» – ввести хост прокси-сервера. Поле обязательно для заполнения;
- «Порт» – по умолчанию задано значение 80. При необходимости ввести другой номер порта. Поле обязательно для заполнения;
- «Имя пользователя» – при необходимости ввести имя пользователя. Поле необязательно для заполнения;
- «Пароль» – ввести пароль пользователя. Поле обязательно для заполнения, если было введено имя пользователя.

ПРИМЕЧАНИЕ. Пароль хранится на сервере в незашифрованном виде;

– «Исключения из проксирования» – при необходимости ввести через запятую хосты, которые будут исключены из проксирования. Поле необязательно для заполнения.

После доставки политики для применения настроек прокси-сервера необходимо произвести повторную авторизацию на устройстве или перезагрузить устройство.

При назначении политики необходимо учитывать следующие особенности:

– пароль хранится на сервере в незашифрованном виде. При этом приложение «Аврора Центр» передает с устройства в «Текущее состояние» и ожидаемом состоянии пароль в виде хэша (sha256);

– для логина и пароля нельзя использовать специальные символы, т.к. устройство не сможет правильно прочитать настройки прокси-сервера из файла;

– если будет использоваться прокси-сервер с протоколами HTTPS или FTP, то сначала нужно настроить переадресацию на этом прокси-сервере, поскольку на устройство автоматически подставляется адрес прокси-сервера с использованием протокола HTTP.

2.4.1.31. Конфигурация/Таймаут экрана

Правило позволяет установить время бездействия пользователя, по истечении которого экран устройства будет заблокирован.

Для создания правила необходимо указать время таймаута в минутах.

При добавлении правила в политику по умолчанию установлено время – 1 минута.

Если требуется отключить блокировку устройства, указать в правиле – 0 минут.

2.4.1.32. Конфигурация репозитория/Подключение системных репозитория

Правило позволяет подключить корпоративные репозитории на платформе Linux, чтобы пользователь мог устанавливать/обновлять ПО из этих репозитория.

Для создания правила необходимо заполнить следующие поля (Рисунок 148):

1) «Параметры подключения» – поле обязательно для заполнения. Ввести параметры подключения к системному репозиторию. Формат параметров зависит от ОС.

Примеры:

– ОС Альт Linux:

```
rpm https://repo.drweb.com/drweb/altlinux 11.0/x86_64 drweb
```

– ОС Astra Linux и ОС Ubuntu:

```
deb http://repo.drweb.com/drweb/debian 10.0.0 non-free
```

– РЕД ОС:

```
[drweb] name=DrWeb - 11.0
baseurl=https://repo.drweb.com/drweb/e15/11.0/$basearch/gpgcheck=1
enabled=1 gpgkey=https://repo.drweb.com/drweb/drweb.key
```

АДМГ.20134-01 90 01-3

В параметрах подключения возможно использовать:

- любой протокол, который поддерживает система, если настраивается подключение к незащищенному репозиторию;
- только протоколы http и https, если настраивается подключение к защищенному репозиторию. Подробная информация о защищенных репозиториях приведена ниже;

2) «Безопасное подключение». Настройка отвечает за подключение к защищенному репозиторию.

Защищенные репозитории - корпоративные репозитории, доступ к которым необходимо обеспечить для устройств компании, которые находятся вне корпоративной сети, при этом возможность использовать их какими-либо другими внешними устройствами должна отсутствовать.

Если репозиторий:

- **Не является защищенным**, необходимо перевести переключатель «Безопасное подключение» в положение «Выключен».

Пример настройки незащищенного репозитория drweb для ОС Альт Linux: в «Параметры подключения» ввести строку (с учетом формата, требуемого для данного дистрибутива ОС) `rpm https://repo.drweb.com/ drweb/altlinux 11.0/x86_64 drweb`, переключатель «Безопасное подключение» должен быть в положении «Выключен»;

- **Защищенный**, перевести переключатель «Безопасное подключение» в положение «Включен».

Правило «Подключение системных репозиторияев» для защищенных репозиторияев предполагает использование контент-серверов. Адрес проксируемого репозитория должен быть указан в конфигурационном файле ППО при развертывании (переменная `linuxRepoAddress`, подробнее о подключении репозитория для ОС семейства Linux через контент-сервер ППО приведено в документе «Руководство администратора» АДМГ.20134-01 91 01).

Пример настройки репозитория drweb для ОС Альт Linux (как защищенного): в «Параметры подключения» ввести строку (с учетом формата, требуемого для данного дистрибутива ОС) `rpm http://content01.ocs-content.ompccloud.ru/pkgrepo/linux/drweb/altlinux 11.0/x86_64 drweb`, где:

- `content01.ocs-content.ompccloud.ru` - адрес контент-сервера (адрес самого проксируемого репозитория drweb указывается в конфигурационном файле ППО при развертывании, переменная `linuxRepoAddress`);
- `pkgrepo/linux` - обязательный base path для репозиторияев.

Переключатель «Безопасное подключение» должен быть в положении «Включен».

Если требуется:

- добавить еще один репозиторий в политику, необходимо нажать на значок **+** и повторить шаги, приведенные выше;

– удалить репозиторий из правила, нажать на значок  «Удалить» справа от названия репозитория.

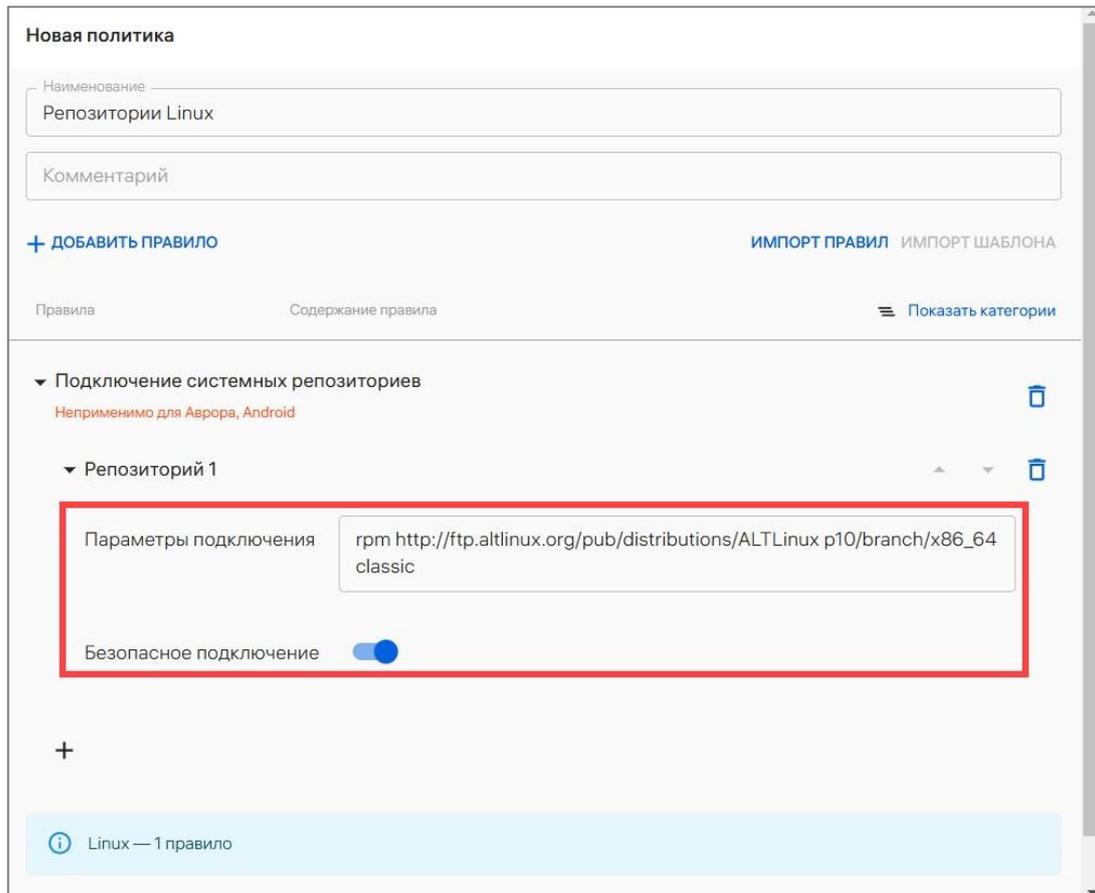


Рисунок 148

2.4.1.33. Система/Обновление ОС

Правило предназначено для обновления ОС на устройствах.

Создание правила по установке версии ОС Аврора (Рисунок 149):

– в поле «Платформа» в раскрывающемся списке выбрать «Аврора». При добавлении правила это значение выбрано по умолчанию;

– в поле «Установить версию ОС» задать версию ОС, которая будет установлена на устройствах. Список версий ОС заполняется в соответствии с версиями дистрибутивов в файловом хранилище ПООС. Описание ПООС приведено в документе «Руководство администратора» АДМГ.20134-01 91 01;

– задать временной интервал, в течение которого на устройствах будет установлена указанная версия ОС. Выбор времени старта и завершения обновления в формате: «Установка с» [чч:мм] и «Установка до» [чч:мм]».

Если текущая версия ОС Аврора выше или соответствует версии из политики, обновление ОС Аврора не выполняется.

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

Рисунок 149

Создание правила по установке версии ОС Альт Linux (Рисунок 150):

ВНИМАНИЕ! Не рекомендуется прерывать процесс установки обновления, особенно это важно при обновлении ядра и его модулей. Это может вызвать сбой ОС.

- в поле «Платформа» в раскрывающемся списке выбрать «Linux»;
- в поле «Установить версию ОС» задать временной интервал, в течение которого на устройство будут установлены обновления ОС (Рисунок 150 [1]). Выбор времени старта и завершения обновления в формате: «Установка с» [чч:мм] и «Установка до» [чч:мм]».

ПРИМЕЧАНИЕ. В поле «Версия ОС» будет установлено значение «latest», которое нельзя изменить. Это означает, что будут установлены последние доступные версии пакетов и/или ядра. В рамках правила политики можно обновить ОС только до более высокой доступной минорной версии (например, с 10.2 до 10.4);

- перевести переключатели, отвечающие за объекты обновления (Рисунок 150 [2]), в положение «Включен» (по умолчанию они выключены):

- «Обновить пакеты» - будут обновлены пакеты, для которых в подключенных репозиториях есть доступные новые версии;
- «Обновить ядро» - будет обновлено ядро и его модули, если в подключенных репозиториях есть доступные новые версии;

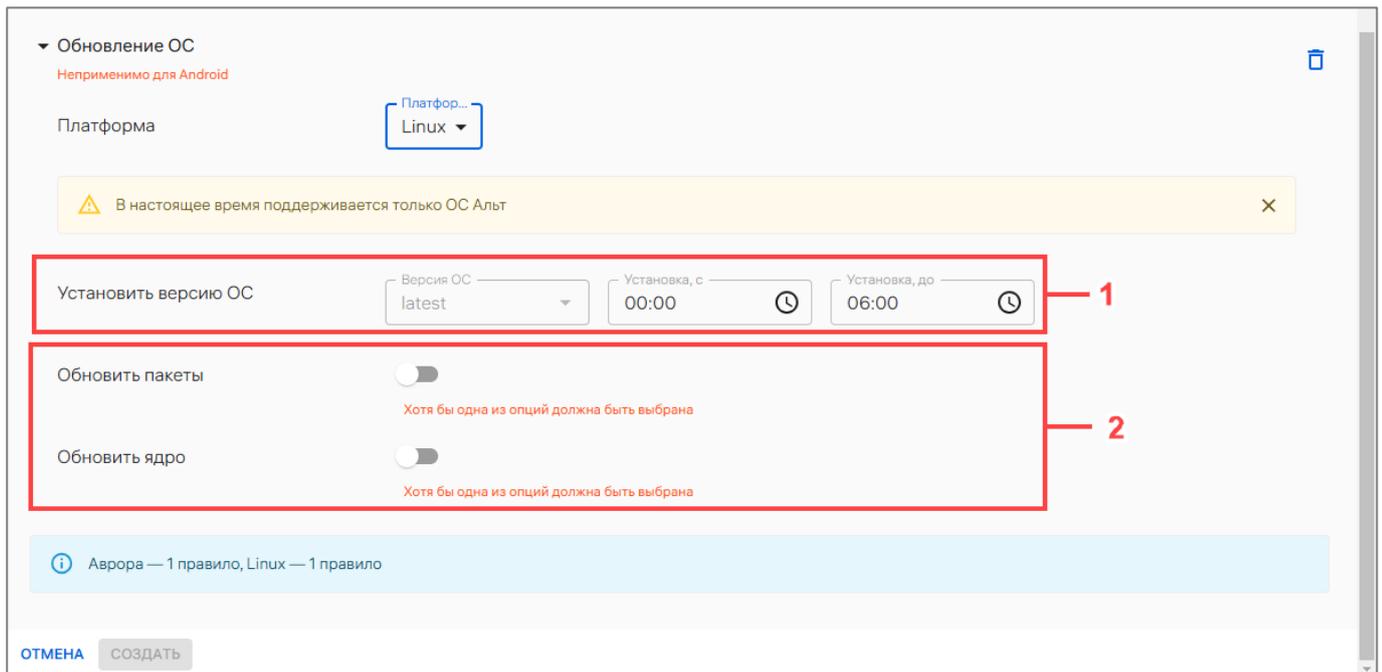


Рисунок 150

– остановка обновления ядра при удалении модуля. При обновлении ядра может произойти ситуация, когда один или несколько его модулей будут удалены. Если в этом случае необходимо остановить обновление ядра, то перевести переключатель «Остановить обновления ядра, если хотя бы 1 модуль удаляется» в положение «Включен» (по умолчанию он выключен и отображается, если «Обновить ядро» включено (Рисунок 151 [1]);

– в разделе «Обслуживание ОС» перевести нужные переключатели, отвечающие за объекты обновления, в положение «Включен» (по умолчанию они выключены и отображаются, если «Обновить пакеты» или «Обновить ядро» включено):

- «Удаление ранее скачанных пакетов»;
- «Удаление неиспользуемых пакетов»;
- «Удаление дубликатов пакетов»;

ПРИМЕЧАНИЕ. Наличие на устройстве повторов пакетов может быть причиной сбоя обновления ОС. Для их удаления возможно использовать опцию «Удаление дубликатов пакетов». Если она активирована в правиле политики, то попытка удаления повторов будет выполняться перед установкой обновлений. Если попытка удаления дубликатов прошла неуспешно, то обновление ОС не будет запущено. В этом случае необходимо удалить повторы пакетов вручную и затем повторить попытку обновления ОС;

- «Удаление старых ядер»;
- «Перезагрузка ОС».

ПРИМЕЧАНИЕ. Включенные опции обслуживания ОС будут выполнены только после успешной установки обновлений ОС.

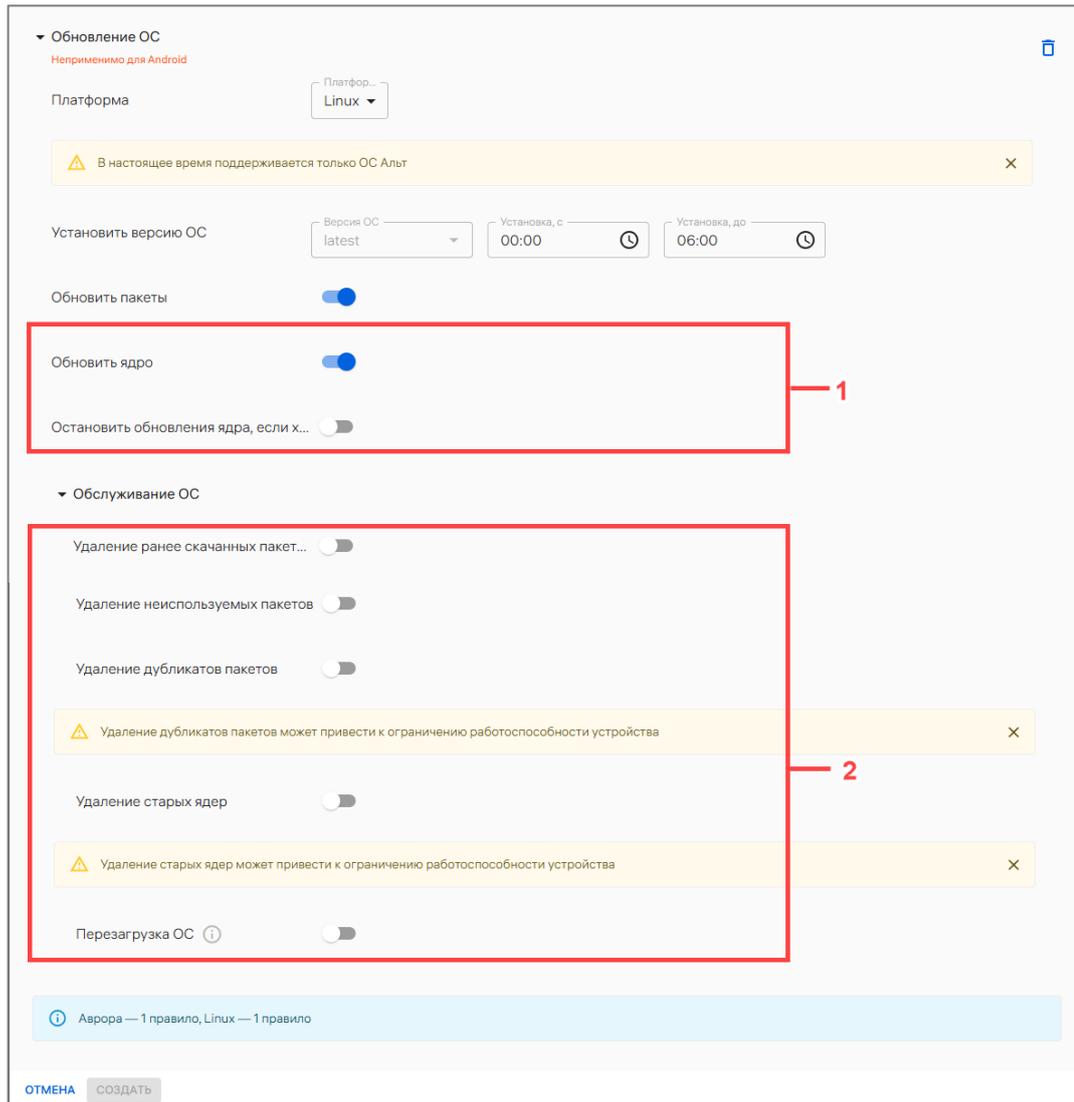


Рисунок 151

Особенности установки обновлений ОС Альт Linux:

1) Приложение «Аврора Центр» каждые три часа выполняет поиск доступных обновлений для пакетов и ядра ОС и передает результат вместе с состоянием устройства. Правило политики запланирует обновление только, если будут найдены доступные обновления пакетов и/или ядра;

2) В запланированный интервал перед установкой обновления выполняется проверка доступности свободного места:

– если места недостаточно, то установка обновлений будет отменена. Приложение «Аврора Центр» передаст информацию о неуспешном обновлении в следующем отправленном состоянии;

– если места достаточно, то будет запущено обновление;

3) При комбинировании политик с правилами, где в одном выбран тип ОС Аврора, а в другом Linux, в результате будет назначено правило и политика с более свежей датой изменения (updatedAt);

4) На соответствие устройства политике влияет параметр «Статус обновления». Возможны следующие случаи, когда устройство будет не соответствовать назначенной политике:

– устройству по какой-то причине не удастся получить информацию по доступным обновлениям (статус обновления в карточке: текущее состояние - «Нет данных», целевое - «Выполнено»);

– устройство получило информацию по доступным обновлениям и передало ее в своем состоянии, но не успело применить назначенную политику (статус обновления в карточке: текущее состояние - «Нет данных», целевое - «Выполнено»);

– устройство применило политику и ей соответствует. Устройство получило информацию по доступным обновлениям и передало ее в своем состоянии, но до передачи состояния устройство не успело запланировать обновление (или не успело передать информацию о запланированном обновлении в состоянии). Статус обновления в карточке: текущее состояние - «Нет данных», целевое - «Выполнено»;

– устройство получило информацию по доступным обновлениям, запланировало обновление в интервал и передало информацию в своем состоянии, но по какой-либо причине устройство не смогло обновиться в запланированный интервал (ошибка, было выключено и т.п.). Статус обновления в карточке: текущее состояние - «Не выполнено», целевое - «Выполнено».

При этом, если на устройство назначена политика, но устройство только запланировало обновление (и еще не имело возможности его выполнить, поскольку запланировало на какой-то момент в будущем), то устройство будет соответствовать политике (несмотря на то, что фактически есть необновленные компоненты). Статус обновления в карточке: текущее состояние - «Запланировано», целевое - «Выполнено».

2.4.1.34. Настройки пользователя/Требования к паролю

Правило задает следующие параметры:

- сложность пароля для разблокировки устройства;
- срок действия пароля.

Для создания правила необходимо выбрать значения из раскрывающегося списка:

– «Сложность»:

- «Обычная» – позволяет задать пароль длиной от 7 до 10 символов. Может состоять только из цифр либо включать цифры, буквы и спецсимволы. При добавлении правила значение устанавливается по умолчанию;

- «Высокая» – позволяет задать пароль длиной от 8 до 12 символов. Может включать цифры, буквы и спецсимволы;

АДМГ.20134-01 90 01-3

- «Символов» (доступные значения зависят от выбранной сложности);
- «Срок, дней» (доступные значения: 30, 60, 90, 120, 150, 180 дней).

ВНИМАНИЕ! При назначении политики устанавливается запрет на изменение требований к паролю. Если после этого будет удалена политика «Требования к паролю», то запрет на изменения все еще будет действовать на устройстве.

ПРИМЕЧАНИЯ:✓ **Для ОС Аврора:**

- в версии 4.0.2 и выше правило для пароля действует для учетной записи как пользователя, так и администратора устройства;
- за 6 дней до окончания срока действия пароля приходит уведомление о необходимости сменить пароль;

✓ **Для ОС Android:**

- не отображается уведомление с напоминанием о смене пароля;
- по истечении срока действия пароля отобразится уведомление о необходимости сменить пароль. При касании уведомления осуществляется переход в настройки ОС для смены пароля;
- если на устройстве были применены более строгие требования к паролю, то отобразится уведомление о необходимости сменить пароль. При нажатии на уведомление осуществляется переход в настройки ОС для смены пароля.

2.4.1.35.Настройки пользователя/Создать пользователя

Правило разрешает или запрещает создание пользователя при активации устройства.

Выбор значения из списка:

- «Создавать» (при добавлении правила значение выбрано по умолчанию);
- «Не создавать».

2.4.1.36.Настройки пользователя/Сертификаты пользователя

Правило позволяет создать и передать на устройство сертификаты пользователя, необходимые для подключения к защищенным сетям WLAN.

Выбрать из раскрывающегося списка категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии необходимой категории в списке, требуется добавить ее в подразделе «Настройки» раздела «Администрирование» (п. 4.1.2).

Для выпуска и доставки сертификата необходимо:

- привязать активированное устройство к пользователю (п. 2.2.7);
- выполнить одно из действий:
 - привязать устройство к группе устройств (п. 2.2.8);
 - привязать пользователя, к которому привязано устройство, к группе пользователей (п. 2.3.4);

– назначить политику с правилом «Настройки пользователя/Сертификаты пользователя» на группу устройств или пользователей, в которую входит устройство.

ПРИМЕЧАНИЯ:

✓ Если у устройств изменится пользователь, то сертификат не будет перевыпущен. Для выпуска сертификата другому пользователю необходимо создать новую категорию пользовательских сертификатов и применить ее в правиле;

✓ Если у пользователя изменились данные, используемые в сертификате, то сертификат не будет перевыпущен. Для выпуска нового сертификата необходимо пользователю создать новую категорию пользовательских сертификатов и применить ее в правиле;

✓ Если пользователь был отвязан от устройства, то пользовательский сертификат не удалится с устройства. Чтобы удалить сертификат с устройства, следует удалить правило из политики.

2.4.1.37.Файлы/Доставка на устройство

Правило позволяет выбрать один или несколько файлов, которые необходимо доставить на устройство.

Для создания правила необходимо (Рисунок 152):

– в раскрывающемся списке «Файл» выбрать файл, который необходимо доставить на устройство, при необходимости воспользовавшись фильтром (подраздел 1.5).

ПРИМЕЧАНИЕ. Если необходимого файла в списке нет, то следует добавить его, выполнив действия описанные в п. 2.6.1;

– в раскрывающемся списке «Версия» выбрать версию файла, которую необходимо доставить на устройство;

ПРИМЕЧАНИЕ. Если необходимой версии файла нет в списке, то следует добавить ее, выполнив действия описанные в п. 2.6.2;

– в поле «Директория» ввести путь к папке на устройстве, в которую необходимо разместить файл.

Если необходимо добавить в правило еще один файл, то необходимо нажать на значок  в левом нижнем углу и повторить действия описанные выше.

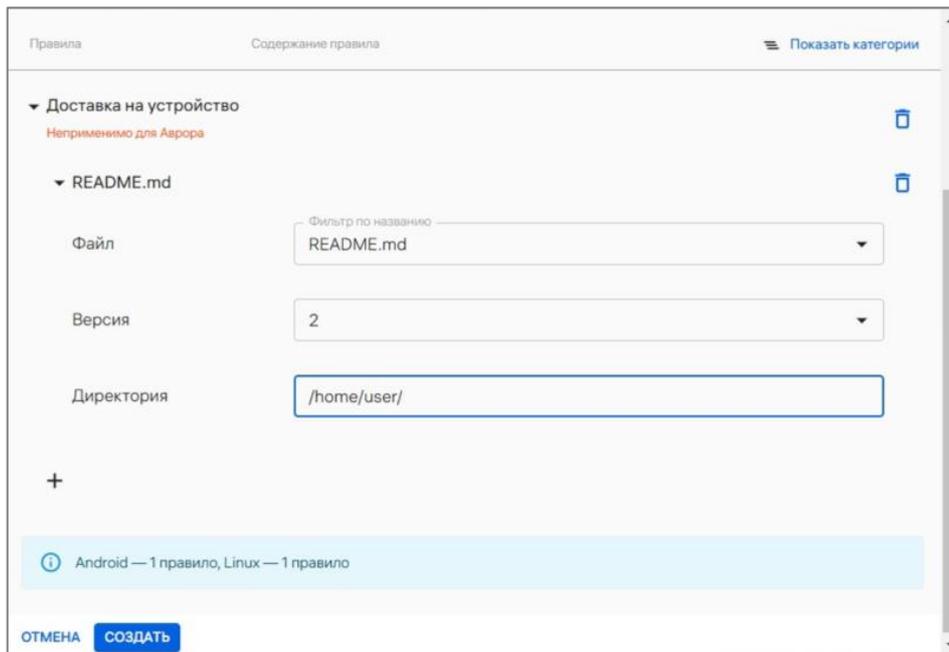


Рисунок 152

2.4.1.38. Файлы с устройства/Загрузка файлов с устройств

Правило позволяет указать папку на устройстве, из которой файлы будут загружаться на сервер Аврора Центр.

Для создания правила необходимо (Рисунок 153):

- в поле «Папка на устройстве» ввести путь до папки на устройстве, файлы из которой необходимо передавать на сервер Аврора Центр (поле обязательно для заполнения);
- в поле «Проверять каждые» ввести периодичность проверки новых файлов в папке в формате [дн:чч:мм] (по умолчанию установлена периодичность проверки в 1 час);
- перевести переключатель «Удалять на устройстве после отправки» в положение «Включено», если требуется, чтобы файлы после передачи на сервер Аврора Центр удалялись с устройства (по умолчанию переключатель установлен в положении «Включено»).

Если требуется:

- добавить еще одну папку в политику, нажать на значок **+** и повторить шаги, приведенные выше;
- удалить папку из правила, нажать на значок **🗑** «Удалить» справа от названия папки.

Для сохранения файлов на сервер будет использоваться папка Uploads (например, /ocs/emm/uploads/default/). Каждый загруженный файл будет в качестве названия использовать свой идентификатор, который ему присвоил Аврора Центр при сохранении на сервере. При этом каждый файл будет загружен в отдельную папку. Имя файла в папке будет совпадать с именем этого файла на устройстве.

Пример: при загрузке с устройства на сервер файлу был присвоен идентификатор 683bba5f-81c3-44e8-bac7-cb4bf021a284. Этот же идентификатор будет именем файла на сервере. Загруженный файл будет расположен на сервере по пути /ocs/emm/uploads/default/68/3b/ba/5f/683bba5f-81c3-44e8-bac7-cb4bf021a284.

ПРИМЕЧАНИЕ. Система размещения в 4-х подпапках, название каждой из которых - это разбитые по 2 первые 8 символов идентификатора файла (/68/3b/ba/5f/), необходима для успешного сохранения файла на сервере.

Если требуется открыть файл, необходимо скачать его с сервера и переименовать так, как он назывался на устройстве с указанием расширения (например, в test.txt). Затем открыть его подходящей программой.

ПРИМЕЧАНИЕ. Оригинальное название файла вместе с расширением доступно в базе данных emm.applications.uploaded_files в столбце source_urn.

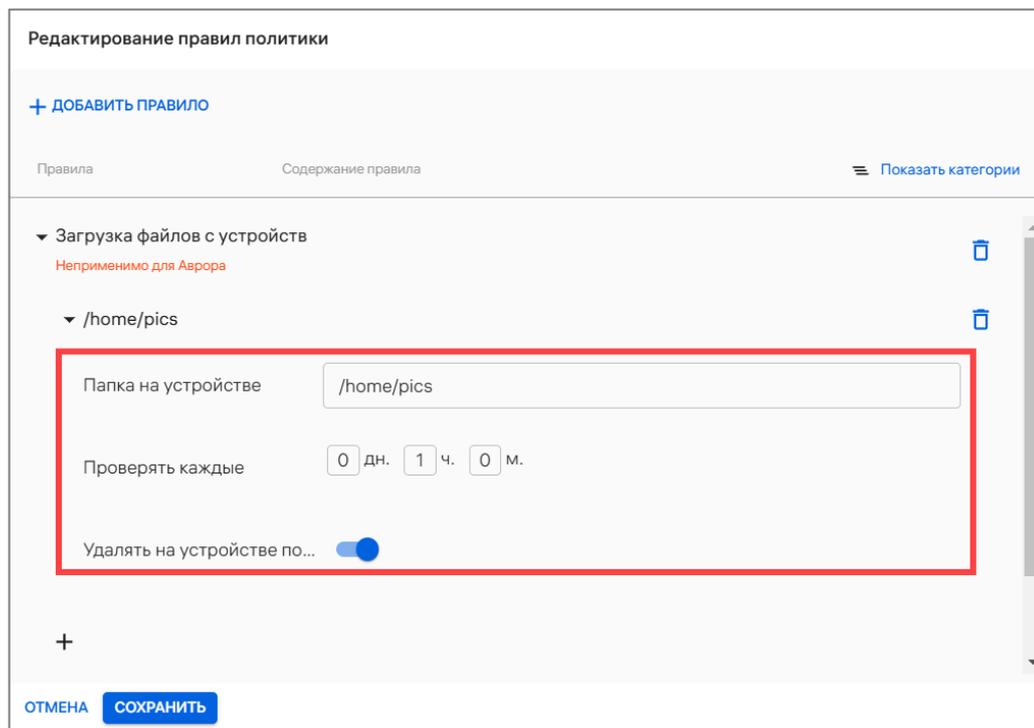


Рисунок 153

2.4.1.39.Скрипты/Выполнение на устройстве

Правило позволяет доставить и выполнить скрипт на устройстве.

Для создания правила необходимо:

1) В раскрывающемся списке «Путь к файлу» (Рисунок 154 [1]) выбрать путь к скрипту, который необходимо выполнить на устройстве после доставки.

ПРИМЕЧАНИЕ. Успешное создание правила по выполнению скриптов возможно только при наличии правила по доставке файлов в политике. Если в раскрывающемся списке «Путь к файлу» нет нужного скрипта, следует нажать на «добавить доставку файлов» (Рисунок 155) и заполнить параметры правила по доставке файлов (пп. 2.4.1.37);

2) В поле «Таймаут» (Рисунок 154 [2]) необходимо ввести максимальное время в формате [мм:сс], в течение которого скрипт должен выполняться на устройстве после доставки. По умолчанию установлено время в 1 минуту;



Рисунок 154

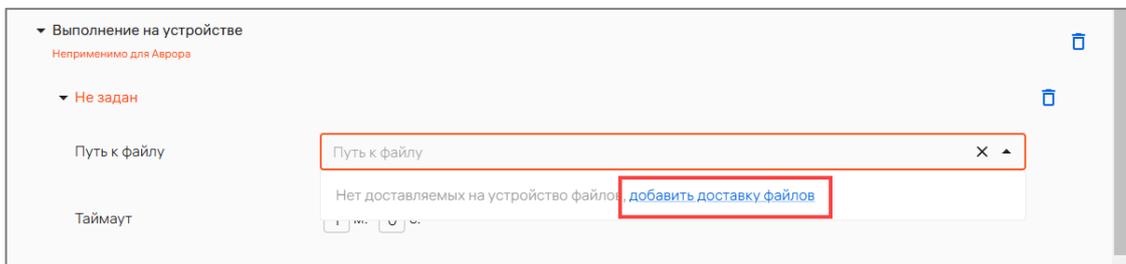


Рисунок 155

3) Нажать кнопку «Добавить переменную» (см. Рисунок 154 [3]), если необходимо добавить в правило управляемые переменные для скрипта (являются переменными окружения, которые будут использованы в изолированной среде при выполнении скрипта), и заполнить следующие параметры (Рисунок 156):

- «Переменная в скрипте» - ввести идентичное название переменной из выбранного скрипта;
- «Переменная к подстановке» - выбрать в раскрывающемся списке нужную управляемую переменную для скрипта.

ПРИМЕЧАНИЯ:

- ✓ Если необходимой управляемой переменной нет в списке, необходимо добавить ее (п. 4.1.8);
- ✓ Если требуется добавить еще одну переменную для подстановки в скрипт, необходимо нажать на кнопку «Добавить переменную» и повторить шаги, приведенные выше.

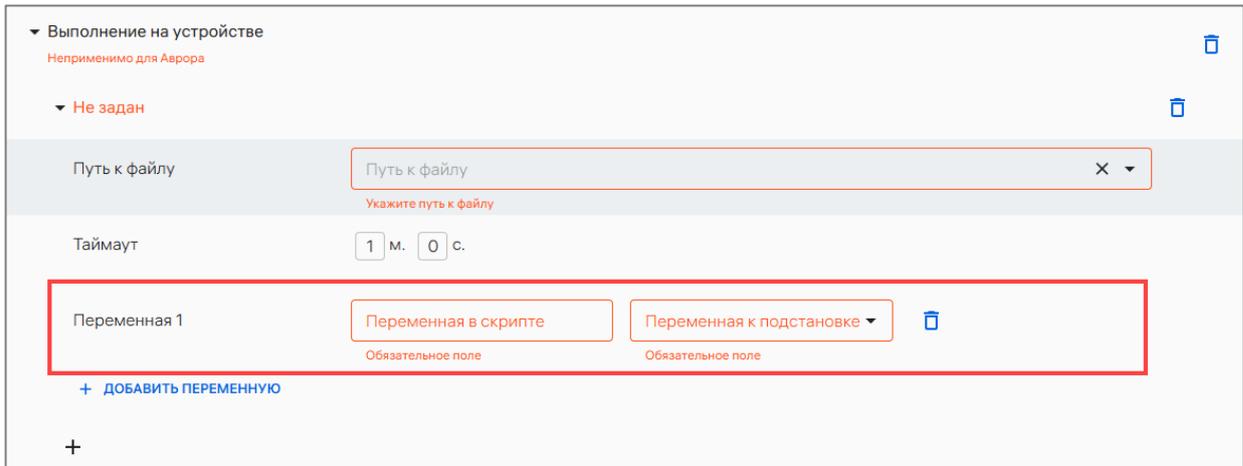


Рисунок 156

Если необходимо добавить в правило еще один выполняемый скрипт, то необходимо нажать на значок **+** (см. Рисунок 154 [4]) в левом нижнем углу и повторить действия, описанные выше.

ПРИМЕЧАНИЯ:

✓ Скрипт будет переприменяться на устройстве каждый час, а также при применении новой или редактировании текущей политики. Если необходимо, чтобы скрипт выполнялся на устройстве однократно, то следует это учитывать при создании скрипта (например, создавать `.lock` файлы). Также при создании скрипта необходимо учитывать другие особенности выполнения скриптов на устройстве (Приложение 3);

✓ Перед выполнением скрипта приложение «Аврора Центр» выполняет сверку хэш-сумм файла скрипта, добавленного в ПУ, и файла скрипта, доставленного на устройство. При несовпадении хэш-сумм скрипт не будет выполнен.

Подробное описание о выполнении скриптов на устройстве приведено в п. 2.6.2.

Примеры выполняемых скриптов с переменными окружения:

– BASH-скрипт на ОС Android:

```
#!/usr/bin/env sh
echo $LOGIN > /storage/emulated/0/Documents/test.txt echo $PASSWORD >>
/storage/emulated/0/Documents/test.txt
```

– BASH-скрипт на ОС семейства Linux:

```
#!/usr/bin/env sh
echo $LOGIN > test.txt echo $PASSWORD >> test.txt
```

2.4.1.40. Геопозиционирование/Настройки геопозиционирования

режима работы

Правило задает следующие параметры:

– выключает или включает геопозиционирование;

– задает режим работы геопозиционирования;
– запрещает или разрешает вносить изменения в настройки геопозиционирования.

Доступные значения (для раскрывающегося списка «Режим работы»):

– «Не задано». Режим работы геопозиционирования не управляется ПУ. Если режим работы не задан, то запрет или разрешение изменения настроек задается вручную. Для этого необходимо выбрать необходимое значение из раскрывающегося списка «Изменение настроек»:

- «Запрещено» (при добавлении правила значение выбрано по умолчанию);

- «Разрешено»;

– «Выключено» (при добавлении правила значение выбрано по умолчанию):

- отключает геопозиционирование;

- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его;

– «Сохранение заряда аккумулятора»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются поставщики сетевого местоположения и аппаратное позиционирование (например, с помощью триангуляции базовых станций), но не GPS;

- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его;

– «Только спутники»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются GPS (Глобальная система позиционирования) и aGPS (Assisted GPS – технология, ускоряющая «холодный старт» GPS-приемника за счет предварительной загрузки в него необходимой информации не со спутников, а через более быстрые каналы связи, такие как WLAN, Bluetooth® и другие), а также аппаратное позиционирование (например, с помощью триангуляции базовых станций), но не поставщики местоположения;

- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его;

– «Высокая точность»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются GPS, а также aGPS или какой-либо поставщик сетевого местоположения;

- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его.

2.4.1.41. Внешний вид/Установка фона рабочего стола

Правило позволяет доставить файл изображения и установить на фон рабочего стола устройства.

ПРИМЕЧАНИЯ:

- ✓ Правило не действует для устройств на базе с ОС Аврора и ОС семейства Linux;
- ✓ Правило поддерживает только файлы формата `.jpeg/.jpg/.png`;
- ✓ Для корректной установки и отображения обоев рабочего стола следует выбирать изображение с разрешением, аналогичным разрешению экрана используемого устройства, или остановиться на изображении с разрешением, значительно превосходящим разрешение экрана устройства.

Для создания правила необходимо в раскрывающемся списке «Путь к файлу» выбрать путь к файлу изображения, который необходимо установить фоном рабочего стола на устройстве после доставки.

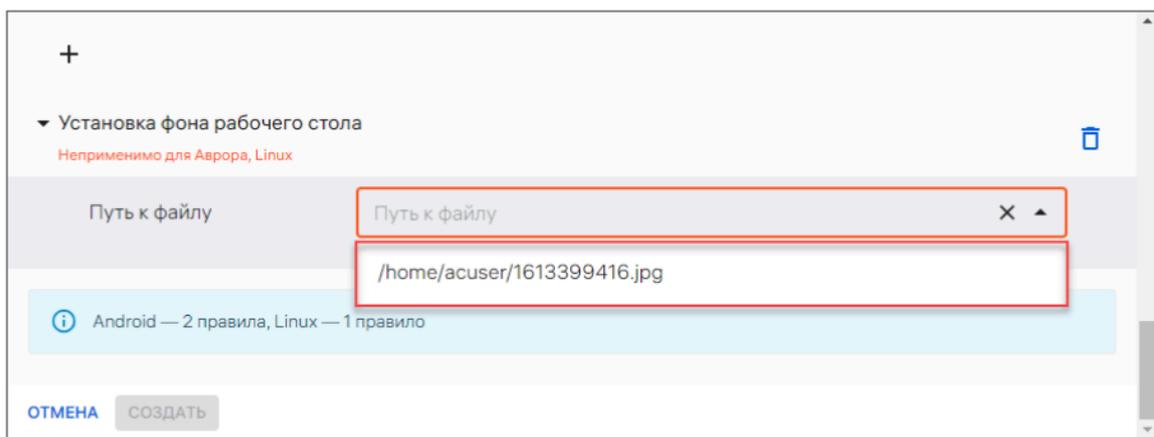


Рисунок 157

Успешное создание правила по установке фона рабочего стола возможно только при наличии правила по доставке файлов в политике с файлом в формате `.jpeg/.jpg/.png`.

Если в раскрывающемся списке «Путь к файлу» нет нужного файла изображения, то необходимо нажать «добавить доставку файлов» и заполнить параметры правила по доставке файлов (Рисунок 158).

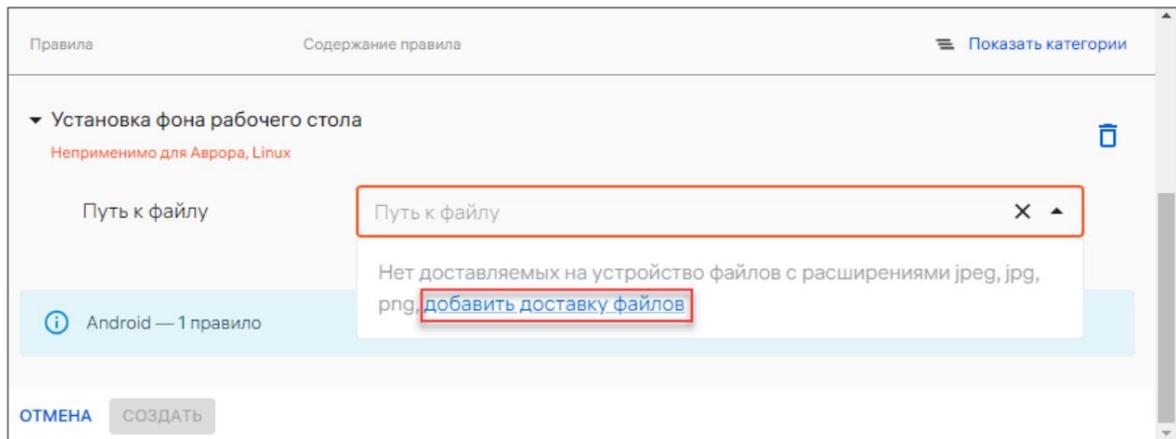


Рисунок 158

2.4.1.42. Внешний вид/Отображение идентификаторов в клиенте Аврора Центр

Правило позволяет задать порядок отображения идентификаторов в приложении «Аврора Центр».

Чтобы создать правило, в блоке «Порядок» необходимо расположить идентификаторы устройства в порядке уменьшения их значимости (Рисунок 159).

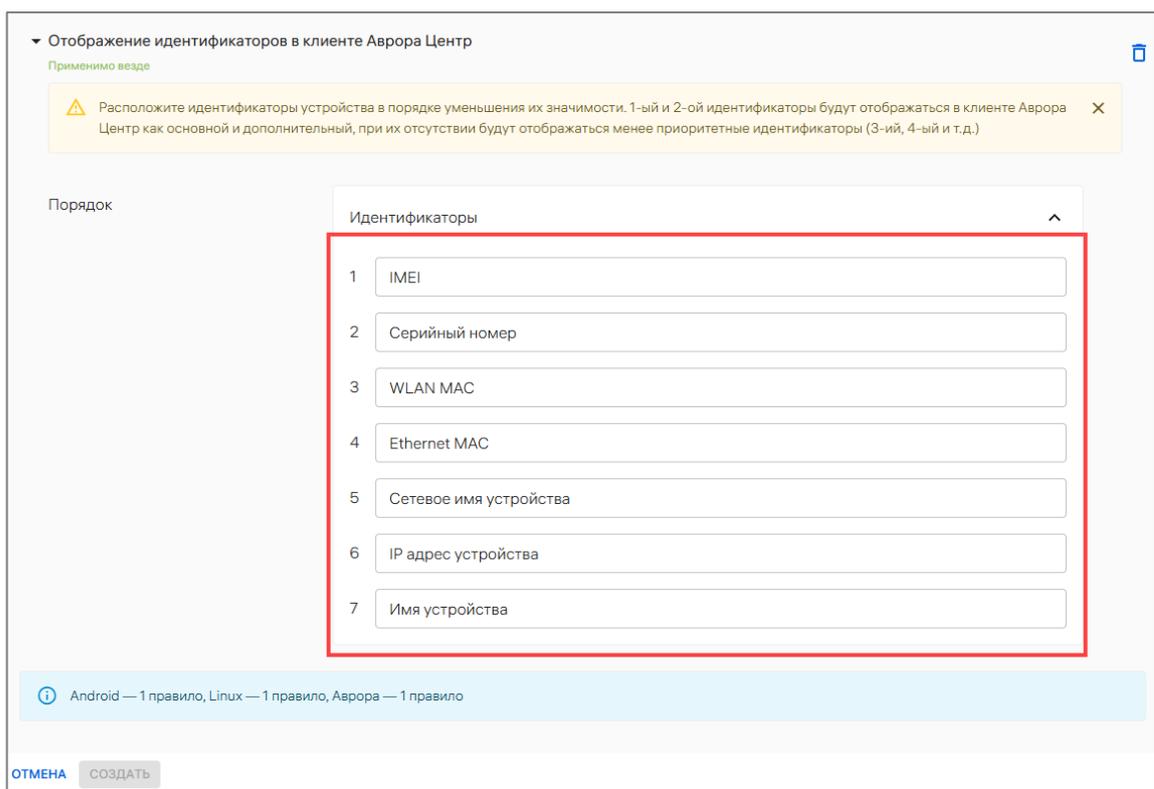


Рисунок 159

Первый и второй идентификаторы будут отображаться в приложении «Аврора Центр» для ОС Аврора и ОС Android (в том числе в режиме киоска) как основной и дополнительный (Рисунок 160, Рисунок 161), при их отсутствии будут отображаться менее приоритетные идентификаторы (третий, четвертый и т.д.).

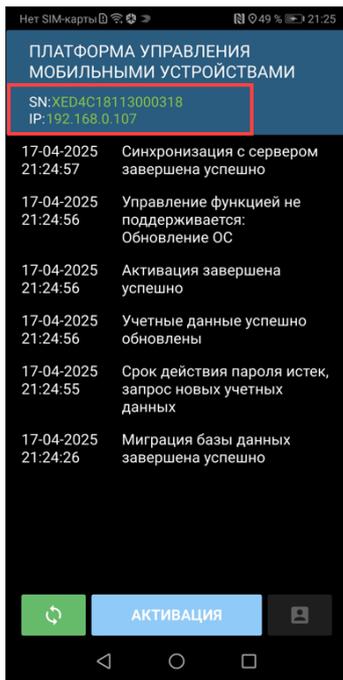


Рисунок 160

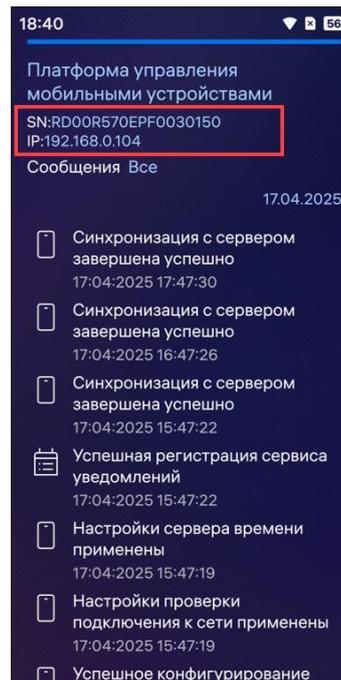


Рисунок 161

Правило также задаст порядок отображения идентификаторов в приложении «Аврора Центр» для ОС семейства Linux. Посмотреть идентификаторы в заданном порядке можно с помощью команды:

```
omp-uem-ctl get-device-identifiers
```

2.4.1.43. Приложения/Управление приложениями

Правило позволяет:

- задать установки приложения выбранной витрины и версии на устройствах, а также позволяет обновлять и удалять установленные приложения. Приложений в политике может быть задано несколько;
- задать список запрещенных приложений (черный список), которых на устройстве быть не должно, вне зависимости от того, каким образом производилась установка на устройство (через ПУ или вручную).

ПРИМЕЧАНИЕ. Предусмотрена возможность задать дополнительные правила по добавлению нескольких приложений в политику, выполнив действия, описанные в п. 2.4.6.

Чтобы приложение было доступно для выбора, необходимо выполнение следующих условий:

- приложение должно быть добавлено и опубликовано в Подсистеме «Маркет» (ПМ) (подробная информация приведена в документе «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2);

– видимость витрины с приложением включена в настройках интеграции с Сервером приложений (п. 4.1.4.1);

– приложения для ОС Аврора, ОС Android, ОС Альт Linux (и РЕД ОС) и ОС Astra Linux (и ОС Ubuntu) должны находиться в отдельных витринах (описание процесса создания витрины с приложением приведено в документе «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2).

ПРИМЕЧАНИЯ:

✓ После установки, с помощью политики, приложению для ОС Android будут автоматически выданы все необходимые разрешения, которые пользователь не сможет отозвать;

✓ Приложение, которое подписано подписью разработчика, клиента и связкой ключей из ППО, невозможно установить через политику;

✓ Перед установкой приложения выполняется сверка хэш-сумм билда приложением «Аврора Центр», вычисленного в ПМ, и билда, полученного на устройстве для установки. При несовпадении хэш-сумм приложение не будет установлено;

✓ Для успешной установки snap-пакетов, требующих опцию `--classic`, на ОС Альт Linux и РЕД ОС необходимо сделать дополнительный симлинк с помощью команды:

```
n -s /var/lib/snapd/snap /snap
```

Приложение будет удалено с устройства, если после установки оно удаляется из правила, заменяется другим приложением или устройство будет удалено из группы, на которую назначена политика.

2.4.1.43.1. Приложения к установке

Для добавления в правило приложения для установки необходимо:

1) В разделе «Укажите приложения к установке» нажать на значок **+** (Рисунок 162 [1]);

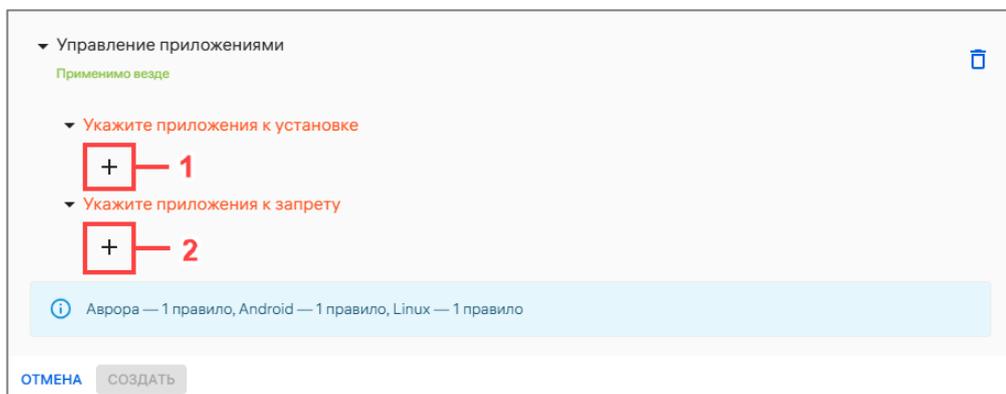


Рисунок 162

2) Если требуется, чтобы все приложения из правила установились на устройстве сразу после получения политики устройством, убедиться что:

- переключатель «Общее время установки» находится в положении «Включен» (Рисунок 163);
- в раскрывающемся списке «Время установки» выбрано значение «Моментально»;

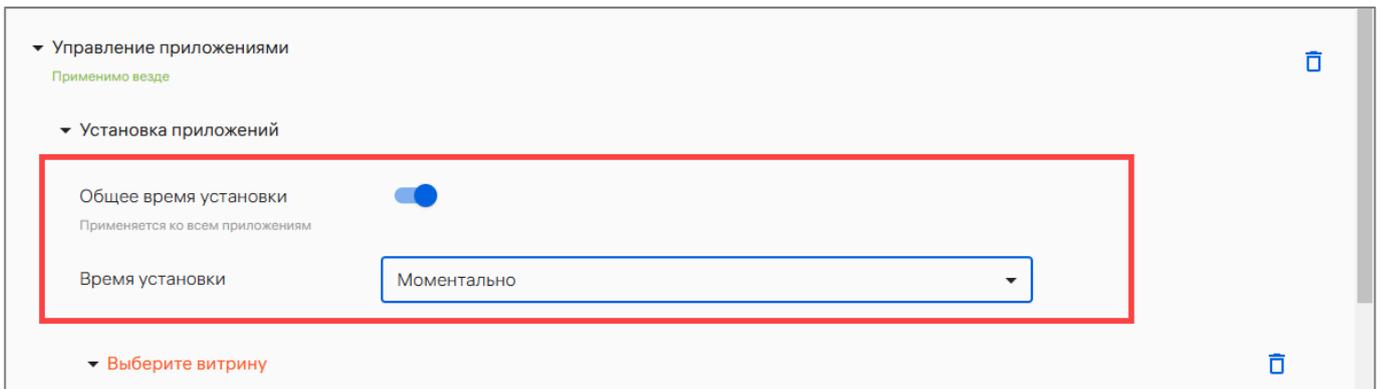


Рисунок 163

3) Если требуется, чтобы все приложения из правила установились на устройстве в заданный интервал времени, необходимо:

- убедиться, что переключатель «Общее время установки» находится в положении «Включен» (Рисунок 164);
- в раскрывающемся списке «Время установки» выбрано значение «Интервал»;
- в поле «Интервал установки» указать начало и конец временного интервала, в течение которого можно установить приложения;

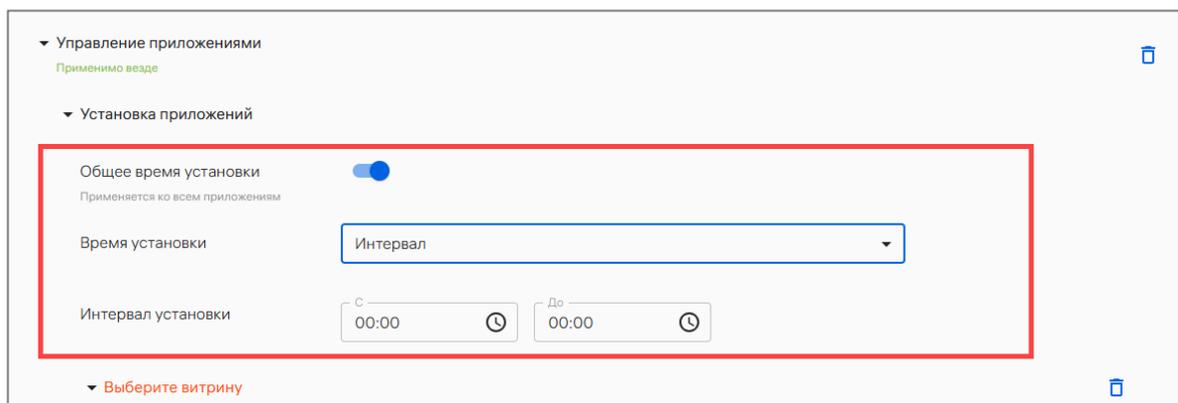


Рисунок 164

4) В полях с раскрывающимися списками выбрать (Рисунок 165 [1]):

- витрину, в которой размещено приложение;
- приложение, которое необходимо установить на устройства;
- номер версии приложения;

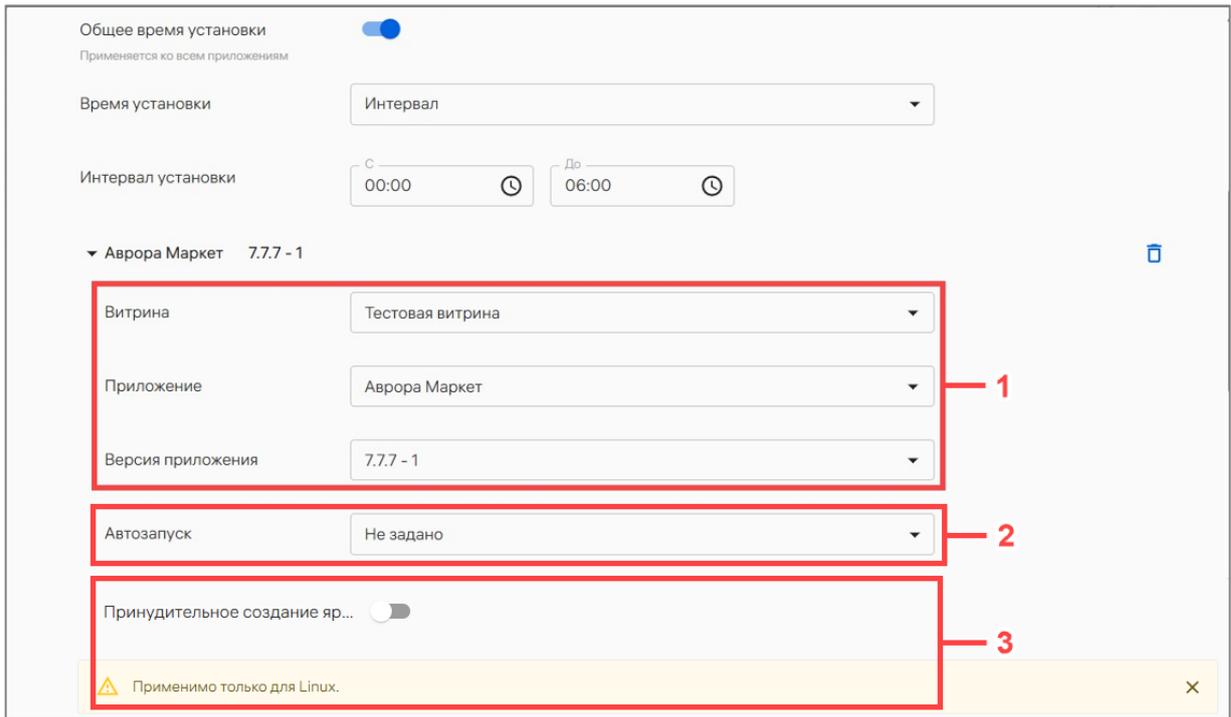


Рисунок 165

5) Для устройств, функционирующих на базе ОС Аврора, доступно задать автозапуск приложения. Для этого в раскрывающемся списке «Автозапуск» (см. Рисунок 165 [2]) выбрать необходимое значение:

- «Не задано» – пользователь может установить автозапуск приложения вручную. При добавлении правила значение выбрано по умолчанию;
- «Да» – приложение будет запускаться автоматически после загрузки ОС. Пользователь не сможет отменить автозапуск приложения;
- «Нет» – приложение не будет запускаться автоматически после загрузки ОС. Пользователь не сможет установить автозапуск приложения;

6) Если требуется, чтобы desktop-файлы устанавливаемого приложения были вынесены на рабочий стол, перевести переключатель «Принудительное создание ярлыка» в положение «Включен» (см. Рисунок 165 [3]). По умолчанию он выключен.

ПРИМЕЧАНИЯ:

- ✓ Параметр доступен только на устройствах с ОС семейства Linux;
- ✓ Если в пакете приложения нет desktop-файлов, то ярлык не будет создан. При этом в карточке устройства будет статус политики «Не соответствует», пока в правиле не будет отключена опция «Принудительное создание ярлыка»;
- ✓ Если в пакете приложения несколько desktop-файлов, то они все будут вынесены на рабочий стол;

7) Если требуется задать индивидуальное время установки приложения на устройстве, необходимо:

- перевести переключатель «Общее время установки» в положение «Выключен»;

- в раскрывающемся списке «Время установки» выбрать:
 - пункт «Моментально» (Рисунок 166), если необходимо, чтобы приложение установилось сразу после получения политики устройством;

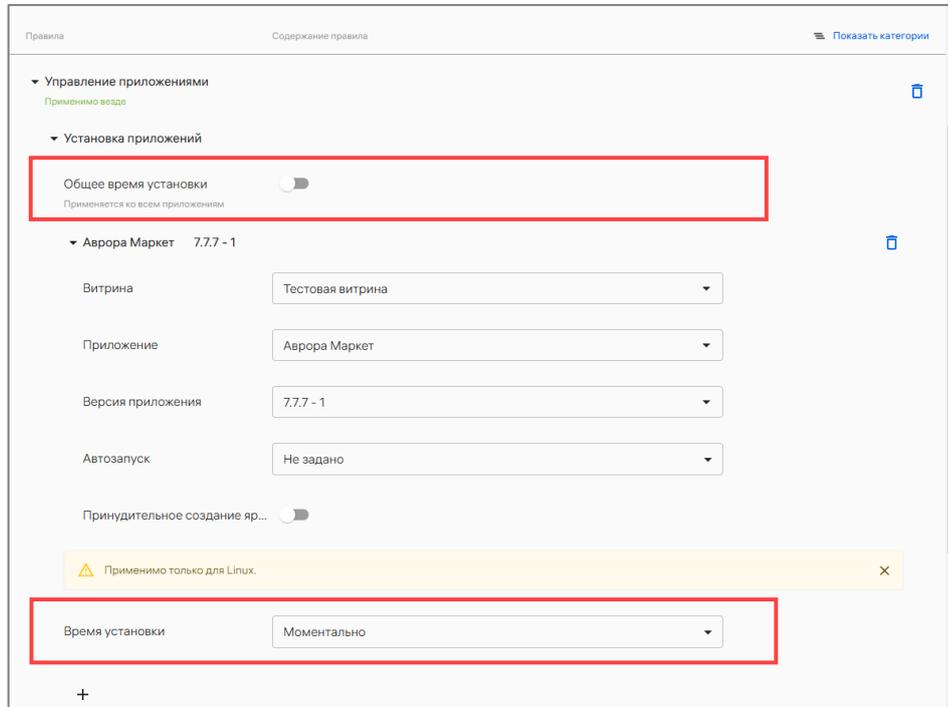


Рисунок 166

- пункт «Интервал» (Рисунок 167), если необходимо, чтобы приложение установилось на устройстве в заданный интервал времени. И затем в поле «Интервал установки» указать начало и конец временного интервала.

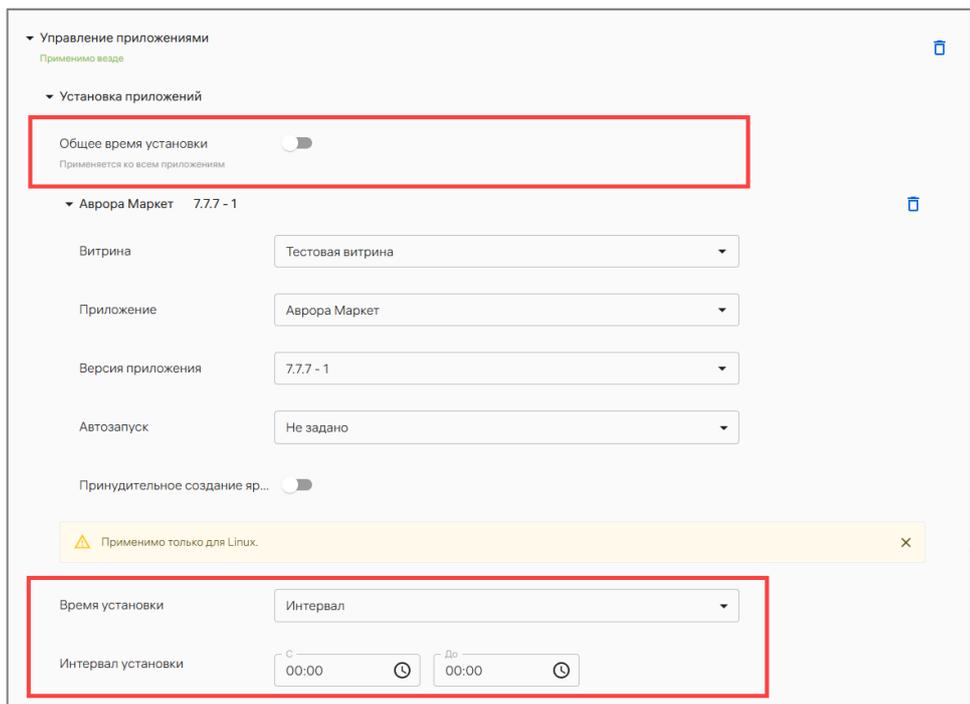


Рисунок 167

2.4.1.43.2. Приложения к запрету

Для добавления в правило запрещенных приложений необходимо:

1) В разделе «Укажите приложения к запрету» нажать на значок **+** (см. Рисунок 162 [2]);

2) В раскрывающемся списке «Название пакета» (Рисунок 168 [1]) выбрать название пакета запрещенного приложения. В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ПУ. При необходимости воспользоваться фильтром по названию пакета, для этого в поле «Название пакета» ввести полное или частичное название пакета;

Рисунок 168

3) Если необходимо задать диапазон запрещенных версий приложения (по умолчанию запрещены все версии приложения):

– перевести переключатель «Диапазон версий» в положение «Включен» (см. Рисунок 168 [2]);

– в поле «Диапазон 1» ввести начало (поле «С») и конец (поле «До») нужного диапазона (см. Рисунок 168 [3]). Верхняя граница «До» не включается в интервал;

– нажать кнопку «Диапазон» (см. Рисунок 168 [4]), если требуется добавить еще один диапазон, и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Для создания правила необходимо настроить хотя бы один список (устанавливаемых или запрещенных приложений).

Когда устройство успешно применит политику с запрещенным списком приложений, то запрещенные версии приложений будут удалены с устройства (если были установлены). Если на устройство назначена политика, которая содержит правило по установке приложения, но при этом это приложение в запрещенном списке, то такое приложение не будет установлено на устройство.

ПРИМЕЧАНИЕ. Если на устройстве с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0 установлен Google Play, то при первой установке приложения через политику может появиться окно с подтверждением (Рисунок 169).

После выдачи разрешения это окно не будет отображаться при последующих установках приложений с помощью политики.

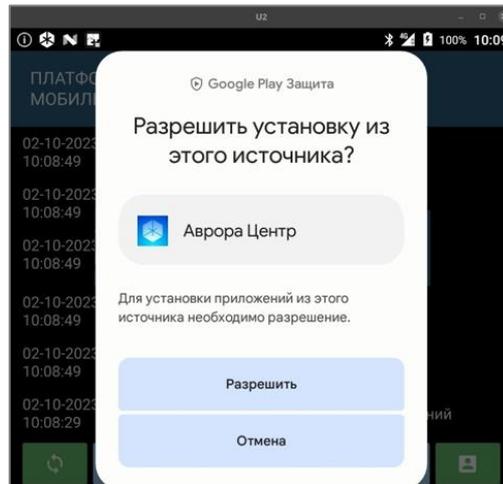


Рисунок 169

ПРИМЕЧАНИЯ:

✓ Начиная с версии ОС Аврора 5.1.0:

– поддерживается установка приложения с учетом архитектуры ОС: 32бита/64 бита (при условии, что сборка соответствующей архитектуры была загружена в ПМ);

– приложения, подписанные публичными/общедоступными ключами разработчика, можно устанавливать только при включенном режиме разработчика на устройстве;

– для успешной установки приложений через приложение «Аврора Маркет» необходимо его установить/обновить с помощью политики через ПУ, при этом приложение «Аврора Маркет» должно быть подписано подписью источника;

✓ На устройства с ОС семейства Linux возможно установить два приложения разных форматов, но с одинаковым именем;

✓ Установка на устройство:

– snap-пакетов – установить snap-менеджер при отсутствии его на устройстве. Обновить приложение со snap-пакетом с помощью политики можно только, если оно не запущено на устройстве;

– appimage-пакетов – после успешной установки appimage-приложение не имеет ярлыка на рабочем столе. Чтобы открыть приложение, необходимо зайти в папку установки /opt/omp-uem-agent/appimages;

– flatpak-пакетов – установить flatpak-менеджера при отсутствии его на устройстве. При установке flatpak-пакета может быть запрошена установка пакетов из общих репозиторийев (необходимо настроить репозиторий).

2.4.1.44. Мобильная сеть/Точка доступа

Правило позволяет создать и настроить на устройстве точку доступа мобильной сети (APN).

Для создания правила необходимо заполнить поля, приведенные в таблице (Таблица 40).

Таблица 40

Наименование полей	Описание
Имя	Ввести имя точки доступа мобильной сети. Поле обязательно для заполнения. Может содержать от 1 до 256 символов
APN	Ввести хост точки доступа мобильной сети. Поле обязательно для заполнения. Требования к заполнению: – длина строки от 1 до 253 символов; – длина каждого сегмента (если разрезать строку по точкам) от 1 до 63 символов; – каждый сегмент содержит только латинские буквы, цифры, тире, при этом первый знак каждого сегмента не может быть тире либо нижнее подчеркивание
Тип APN	При добавлении правила значение по умолчанию «Интернет». Поле недоступно для редактирования
Тип аутентификации	При добавлении правила значение по умолчанию «Нет». Поле недоступно для редактирования
MCC	Ввести мобильный код страны. Поле обязательно для заполнения. Может содержать номер от 001 до 999
MNC	Ввести код мобильной сети. Поле обязательно для заполнения. Может содержать код от 01 до 999

ПРИМЕЧАНИЕ. При назначении политики следует учитывать следующие особенности:

– ОС Аврора и ОС Android:

- нет методов получения данных об MCC и MNC. Поэтому эти данные берутся из OperatorNumeric (для ОС Android) и IMSI (для ОС Аврора) по следующему принципу: MCC – первые 3 символа, MNC – 4 и 5 символ. Поскольку MNC в России двузначный – для других стран MNC может быть трехзначным и это надо учитывать, если SIM-карта и оператор сотовой связи будет из других стран;

– ОС Android:

- создание точки доступа мобильной сети возможно на ОС Android с версией 9 и выше;

- настройки точки доступа мобильной сети, выставленные через приложение «Аврора Центр», нельзя посмотреть и/или изменить на устройстве вручную;

- создание точки доступа мобильной сети работает некорректно на устройстве Huawei POT-LX1 с ОС Android версии 10;

– ОС Аврора:

- из-за ограничений MDM API нельзя выставить MCC и MNC;

- выставлять настройки точки доступа мобильной сети можно только применительно к конкретной SIM-карте, при этом, после выставления настроек эта SIM-карта становится картой по умолчанию для интернет-соединения (ограничение MDM API);
- выставлять настройки точки доступа мобильной сети можно только применительно к конкретной SIM-карте, соответственно, поддерживаются устройства, в которых вставлена одна SIM-карта. Если на устройстве более одной SIM-карты, то поведение будет неопределенным, поскольку настройки будут выставлены на ту SIM-карту, значение IMSI которой меньше в результате лексикографической сортировки;
- после удаления правила политики для настройки параметров точки доступа к мобильной сети эти значения не удаляются с устройства – значения по умолчанию не сбрасываются до первоначальных (ограничение MDM API). Как следствие этого поведения, если на устройство назначить правило политики с точно такими же настройками, какие уже выставлены в ОС, то в журнале приложения «Аврора Центр» не будет сообщения о создании точки доступа мобильной сети, поскольку она уже создана на устройстве.

2.4.1.45. Мобильная сеть/Управление мобильной передачей данных

Правило фиксирует текущее состояние мобильной передачи данных. Запрещает или разрешает вносить изменения в настройки мобильной передачи данных.

Выбор значения из списка:

- «Разрешено»;
- «Запрещено». При добавлении правила значение выбрано по умолчанию.

2.4.2. Добавление политики вручную

Для добавления политики вручную необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать кнопку «Добавить» и выбрать из раскрывающегося списка «Добавить политику» (Рисунок 170);

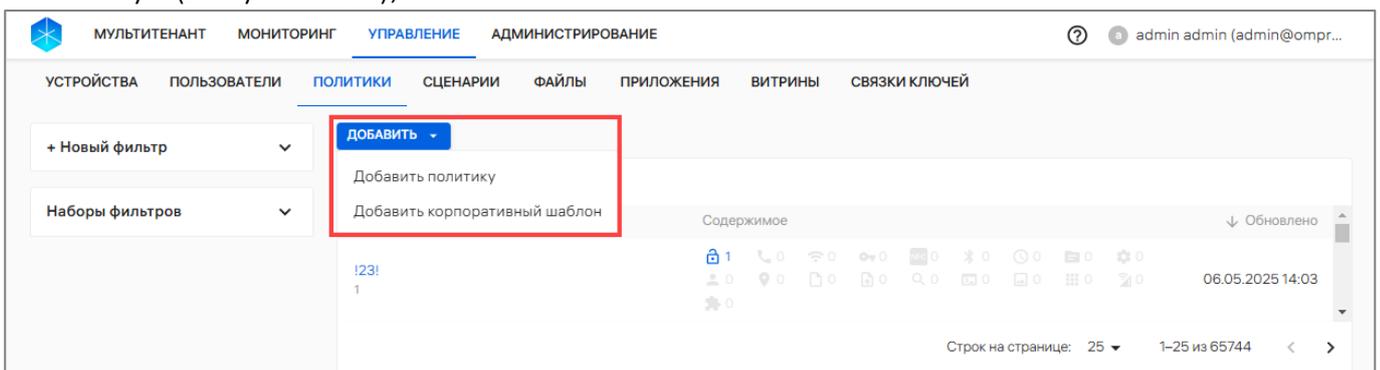


Рисунок 170

– в открывшемся окне:

- ввести название политики – название политики должно быть уникальным. Поле обязательно для заполнения (Рисунок 171 [1]);
- ввести комментарий – при необходимости ввести дополнительную информацию к политике (Рисунок 171 [2]);
- нажать кнопку «Добавить правило» (Рисунок 171 [3]) и выбрать правило политики из раскрывающегося списка;
- задать параметры правила (Рисунок 171 [4]). Описание правил для политик приведено в таблице (см. Таблица 39).

Новая политика

Наименование
test_политика_1

Комментарий
test

+ ДОБАВИТЬ ПРАВИЛО

ИМПОРТ ПРАВИЛ ИМПОРТ ШАБЛОНА

Правила Содержание правила

Показать категории

Снимки экрана
Неприменимо для Linux

Запрещено

Аврора — 1 правило, Android — 1 правило

ОТМЕНА СОЗДАТЬ

Рисунок 171

В случае необходимости создать политику из нескольких правил следует повторить действия, описанные выше.

В случае необходимости удалить правило следует нажать значок  «Удалить» (см. Рисунок 171 [5]) справа от правила.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного сохранения политики отобразится соответствующее сообщение и откроется карточка добавленной политики (п. 2.4.6).

2.4.3. Добавление политики на основе корпоративного шаблона

При необходимости на этапе добавления политики вручную возможно воспользоваться функционалом импорта шаблона.

ПРИМЕЧАНИЕ. Импорт шаблона возможно выполнить при условии, что корпоративный шаблон политик уже создан (пп. 2.4.3.1).

Для добавления политики на основе корпоративного шаблона необходимо в окне ввести:

- название политики (название политики должно быть уникальным. Поле обязательно для заполнения);
- комментарий (при необходимости ввести дополнительную информацию к политике);
- нажать кнопку «Импорт шаблона» (Рисунок 172), в результате чего правила из корпоративного шаблона будут импортированы в новую политику.

Новая политика

Наименование
test_политика

Комментарий
test

+ ДОБАВИТЬ ПРАВИЛО ИМПОРТ ПРАВИЛ **ИМПОРТ ШАБЛОНА**

Правила Содержание правила

Данная политика не содержит ни одного правила

ОТМЕНА СОЗДАТЬ

Рисунок 172

При необходимости, в соответствии с п. 2.4.1, импортированные правила возможно:

- изменить (см. Рисунок 171 [4]). Описание правил для политик приведено в таблице (см. Таблица 39);
- добавить правило в политику (см. Рисунок 171 [3]);
- удалить правило (см. Рисунок 171 [5]).

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного добавления политики отобразится соответствующее сообщение и откроется карточка добавленной политики.

2.4.3.1. Добавление корпоративного шаблона

Корпоративный шаблон политик содержит стандартный для организации набор правил. Указанные значения будут использованы для последующего применения на устройствах, если они не определены создаваемой политикой. Шаблон политики освобождает Администратора Платформы управления от манипуляций с повторяемыми опциями на этапе создания новых политик.

Корпоративный шаблон политик включает в себя все опции, доступные для управления в момент создания шаблона. При создании корпоративного шаблона Администратор Платформы управления указывает значения опций «по умолчанию» и получает возможность создавать политики на основе этого шаблона.

Для добавления корпоративного шаблона необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать кнопку «Добавить»;
- выбрать из раскрывающегося списка пункт «Добавить корпоративный шаблон» (см. Рисунок 170).

ВНИМАНИЕ! Предусмотрена возможность создания только одного корпоративного шаблона. Пункт меню «Добавить корпоративный шаблон» отсутствует, если корпоративный шаблон политик уже создан. Вместо него отображается пункт меню «Редактировать корпоративный шаблон» (Рисунок 174);

- в открывшемся окне возможно выполнить следующие действия:

- при необходимости изменить комментарий к корпоративному шаблону (наименование корпоративного шаблона проставляется автоматически) (Рисунок 173 [1]);

- добавить правила в корпоративный шаблон, нажав на кнопку «Добавить правило» (Рисунок 173 [2]). Добавление правила выполняется в соответствии с п. 2.4.1.

ПРИМЕЧАНИЕ. По умолчанию корпоративный шаблон не содержит ни одного правила;

Рисунок 173

- подтвердить либо отменить действия.

В результате успешного создания корпоративного шаблона политики отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если корпоративный шаблон политик не создан, то в подразделе «Аудит» раздела «Мониторинг» отобразится ошибка «404» для следующих событий:

- переход в подраздел «Политики»;
- комбинирование политик.

2.4.3.2. Редактирование корпоративного шаблона

Созданный шаблон политики доступен для редактирования.

Редактирование предполагает изменение (в том числе удаление или дополнение) существующих правил шаблона.

Для редактирования корпоративного шаблона необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать кнопку «Добавить»;
- выбрать из раскрывающегося списка пункт «Редактировать корпоративный шаблон» (Рисунок 174);
- в открывшемся окне (см. Рисунок 173) внести изменения, выполнив действия, приведенные в пп. 2.4.3.1.

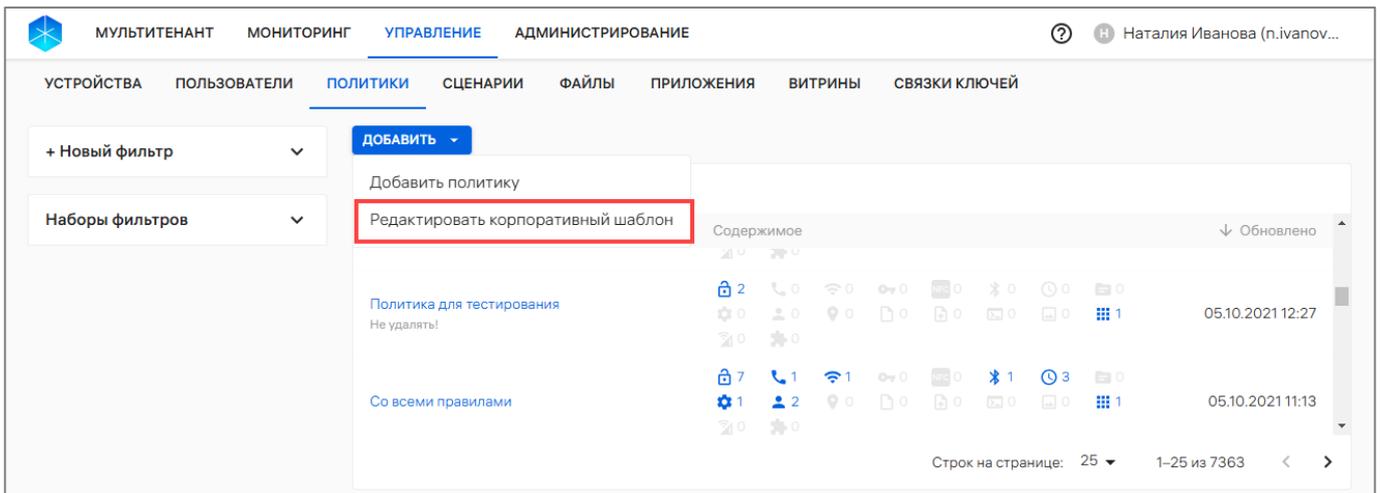


Рисунок 174

В результате успешного сохранения внесенных в корпоративный шаблон изменений отобразится соответствующее сообщение.

ВНИМАНИЕ! После редактирования корпоративного шаблона для его вступления в силу необходимо отредактировать и применить текущую политику либо отвязать ее и снова применить.

2.4.4. Назначение политики на группы устройств или группы пользователей

Назначить политику на группу устройств и/или группу пользователей возможно через:

- карточку политики (пп. 2.4.4.1);
- карточку группы устройств (пп. 2.4.4.2);
- карточку группы пользователей (пп. 2.4.4.3).

2.4.4.1. Назначение политики на группы устройств и/или группы пользователей через карточку политики

Для назначения политики на группы устройств и/или группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать на название политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке политики перейти во вкладку «Группы»;
- нажать кнопку «Редактировать группы» (см. Рисунок 45 [2]);
- в открывшемся окне нажать кнопку «Добавить» (Рисунок 175 [1]);

- в раскрывающемся списке выбрать тип группы (Рисунок 175 [2]):
 - «Группу устройств»;
 - «Группу пользователей»;



Рисунок 175

– выбрать необходимую группу из раскрывающегося списка или воспользоваться фильтром по названию группы.

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешного назначения политики на группы устройств и/или группы пользователей отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. При наличии нескольких изменений политик, например: редактирование политик, назначение политик на группы устройств или группы пользователей, добавление устройств в группы устройств и т.д., на устройство будет назначена последняя скомбинированная политика.

2.4.4.2. Назначение политики на группу устройств через карточку группы

В Консоли администратора ПУ предусмотрена возможность контроля и отслеживания политик, назначенных на группу устройств. Политики содержат набор правил для применения на устройства.

ПРИМЕЧАНИЕ. Перед назначением политики на группу устройств необходимо убедиться, что добавлена хотя бы 1 политика. Добавление политик описано в п. 2.4.1 – 2.4.4.

Для назначения политик на группу устройств необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в открывшейся карточке группы устройств перейти во вкладку «Политики»;
- нажать кнопку «Назначить политики» (см. Рисунок 32 [2]);

– в отобразившемся окне выбрать необходимую политику из раскрывающегося списка или воспользоваться фильтром (Рисунок 176 [1]). Далее при необходимости возможно добавить дополнительную политику, выбрав ее из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранную политику, нажав значок  «Убрать из списка» (Рисунок 176 [3]);

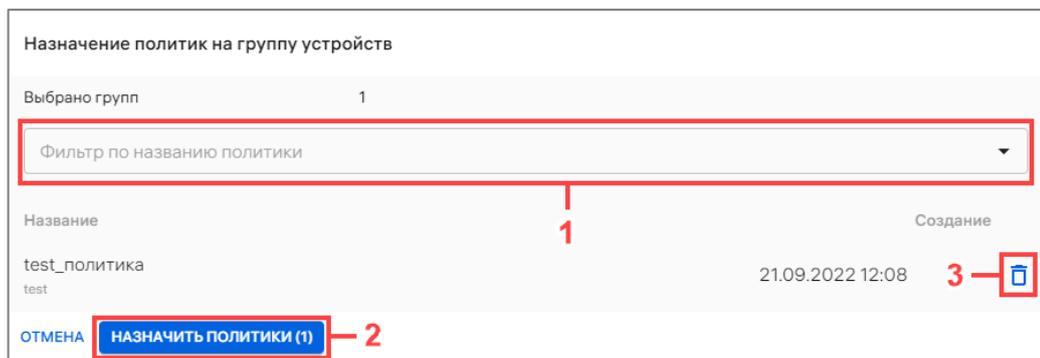


Рисунок 176

– нажать кнопку «Назначить политики» (см. Рисунок 176 [2]).

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешного назначения политики на группу устройств отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если устройство, входящее в группу, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.4.3. Назначение политики на группу пользователей через карточку группы

Для назначения политик на группу пользователей через карточку группы необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в открывшейся карточке группы пользователей перейти во вкладку «Политики»;
- нажать кнопку «Назначить политики» (см. Рисунок 40 [2]);
- в открывшемся окне (см. Рисунок 176) выполнить действия, приведенные в пп. 2.4.4.2.

В результате успешного назначения политики на группу пользователей отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если устройство, привязанное к пользователю из группы, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.5. Добавление политики на основе существующей

ПРИМЕЧАНИЕ. Добавление политики на основе существующей возможно только при условии, что добавлена хотя бы 1 политика (п. 2.4.2, 2.4.3).

Для добавления политики на основе существующей необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- скопировать правила интересующей политики одним из следующих способов:

- выбрать политику в списке, при необходимости воспользовавшись фильтром, перейти в карточку выбранной политики и нажать кнопку «Создать политику на основе существующей» (Рисунок 177);

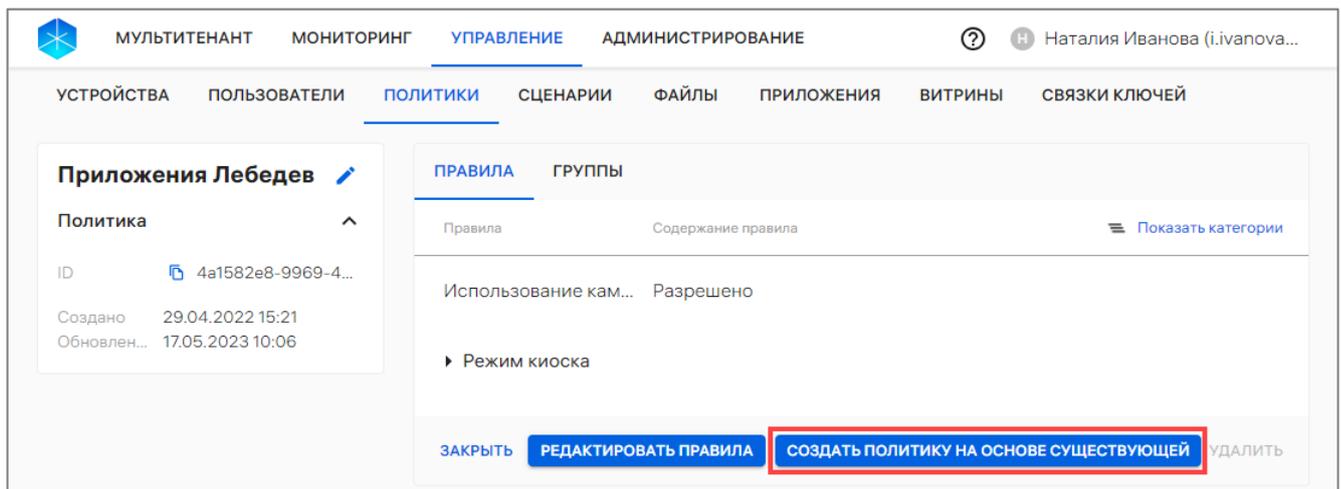


Рисунок 177

– в списке политик нажать кнопку «Добавить» или выбрать из раскрывающегося списка «Добавить политику» (см. Рисунок 170), а затем нажать кнопку «Импорт правил» (Рисунок 178 [1]). Из раскрывающегося списка выбрать правило политики, которое необходимо скопировать (при необходимости воспользоваться фильтром по названию политики) (Рисунок 178 [2]). В результате правила из выбранной политики будут импортированы в новую политику;

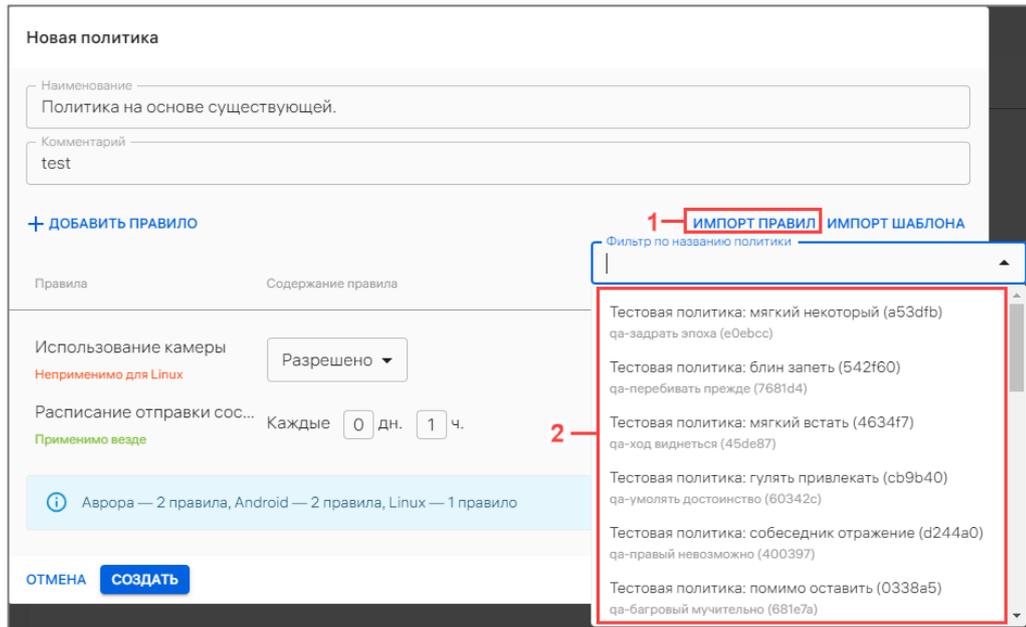


Рисунок 178

– в открывшемся окне:

- ввести название политики (название политики должно быть уникальным). Поле обязательно для заполнения;
- ввести комментарий (при необходимости ввести дополнительную информацию к политике);
- при необходимости изменить параметры импортированных правил (см. Таблица 39).

Если необходимо добавить правило в политику или удалить правило, следует выполнить действия, описанные в п. 2.4.2.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

2.4.6. Редактирование правила политики

ВНИМАНИЕ! Удаление запрещающего правила из политики, отвязка политики от группы или исключение устройства из группы не приведет к изменению состояния самого устройства (например, если правило политики запрещало использование камеры, то после снятия такой политики камера останется не доступной на устройстве). Для изменения состояния необходимо явно в политике установить целевое состояние. Также можно использовать корпоративный шаблон политики (пп. 2.4.3.1). Например, если в корпоративном шаблоне политики будет задано разрешающее правило политики на использование камеры, и при этом на устройстве будет назначена любая политика (даже пустая), тогда устройство приведется в состояние, указанное в корпоративном шаблоне. Важно понимать, что корпоративный шаблон действует на всех устройствах, на которых действует хотя бы одна политика, и регулирует только те правила, которые явно не заданы в политиках.

Набор правил политики возможно отредактировать, выполнив следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- выбрать политику из списка, при необходимости воспользовавшись фильтром (подраздел 1.5);
- перейти в карточку политики;
- во вкладке «Правила» нажать кнопку «Редактировать правила» (Рисунок 179);

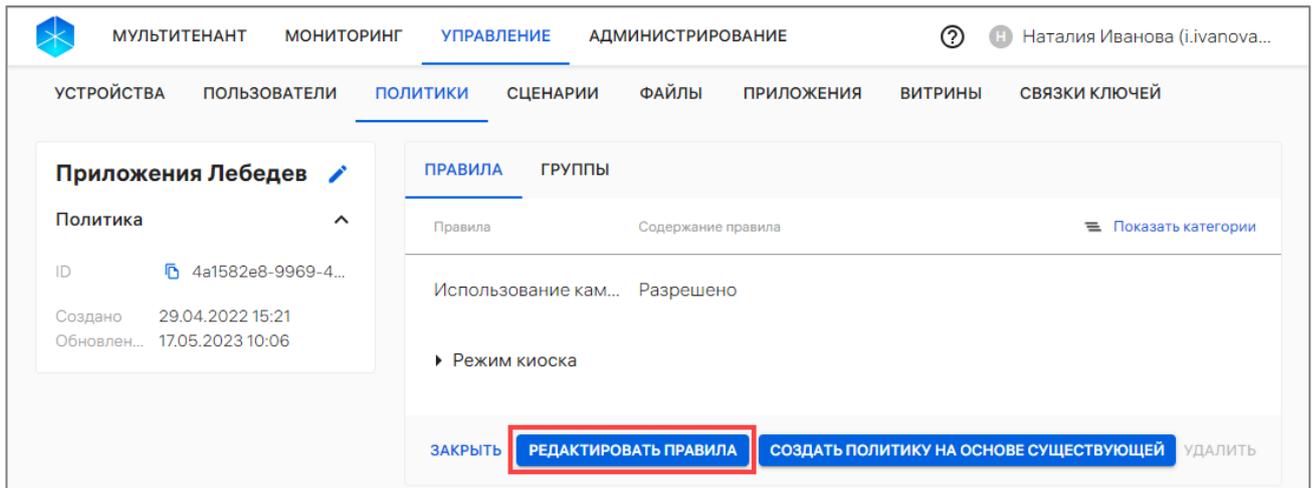


Рисунок 179

- в открывшемся окне внести изменения в правила политики (Рисунок 180 [2]) в соответствии с таблицей (см. Таблица 39);
- для добавления дополнительных правил нажать кнопку «Добавить правило» (Рисунок 180 [1]) и выбрать правило политики из раскрывающегося списка и задать его параметры (при необходимости);
- для удаления правил из политики нажать значок  «Удалить» (Рисунок 180 [3]) справа от правила (при необходимости);

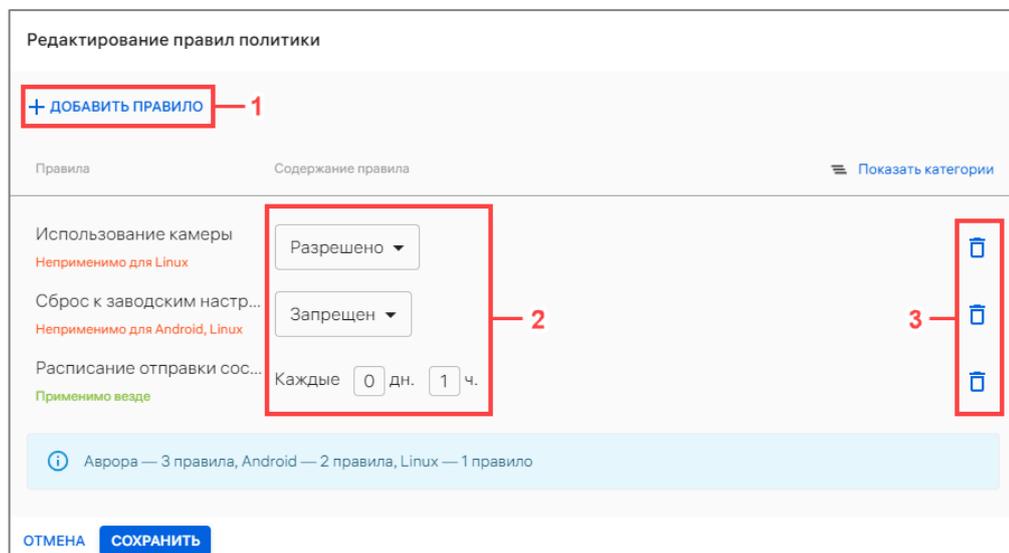


Рисунок 180

– сохранить изменения либо отменить действия.

При успешном сохранении изменений начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Отобразится предупреждение о том, что это может занять некоторое время (Рисунок 181 [1]).

Для автоматического применения политики следует нажать кнопку «Подтвердить» (Рисунок 181 [2]), не дожидаясь результата проверки, в результате политика с обновленными правилами будет назначена на все устройства.

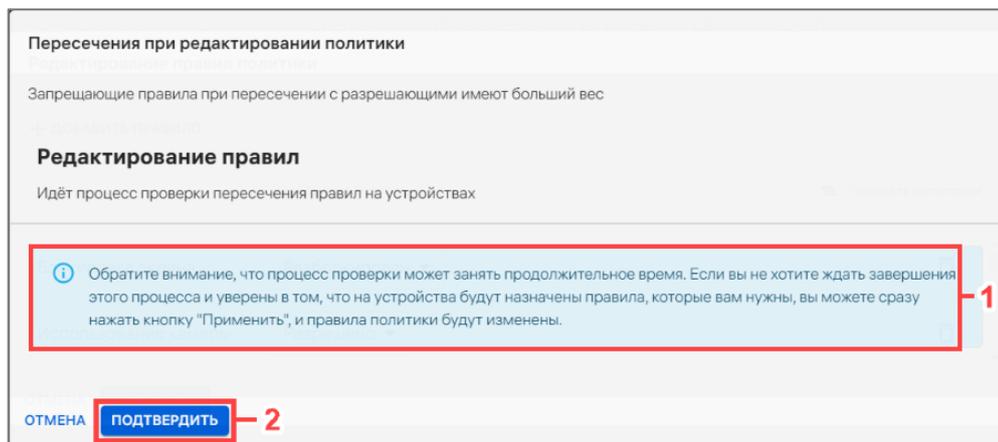


Рисунок 181

Для просмотра пересечения политики с другими политиками и правилами из корпоративного шаблона необходимо дождаться завершения проверки. В результате будет отображен список названий пересекающихся групп и устройств, на которых пересекается политика, а также скомбинированная политика.

Для применения политики на все устройства необходимо нажать кнопку «Подтвердить» (Рисунок 182), в результате чего отобразится сообщение «Политика обновлена». Новые правила начнут действовать для всех активированных устройств, входящих в группы устройств или пользователей, на которые была назначена политика.

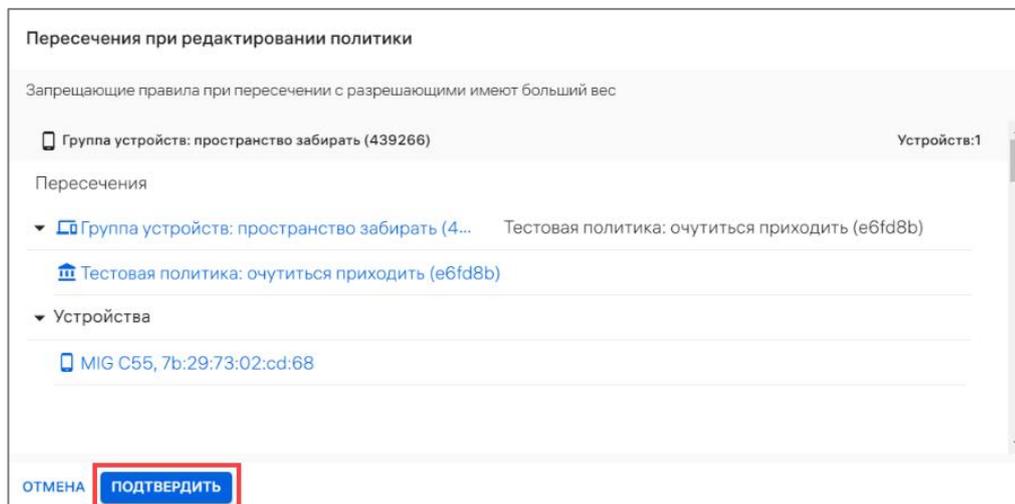


Рисунок 182

ПРИМЕЧАНИЕ. Перед применением скомбинированной политики следует учитывать следующее:

- приоритет имеют запрещающие правила;
- для правил с датами в приоритете правило с более поздней датой создания;
- для периодов – у наименьшего периода действия;
- для правил с версиями (обновление ОС и установка приложения) приоритет у последней версии (например, если версии 1.0.0 и 1.0.1 – будет установлена 1.0.1);
- для правила хранения системных сообщений приоритет у постоянного;
- корпоративный шаблон дополняет скомбинированную политику правилами, которые указаны в нем, но не указаны в скомбинированной политике.

2.4.7. Отвязка политики от группы устройств или группы пользователей

ВНИМАНИЕ! Удаление запрещающего правила из политики, отвязка политики от группы или исключение устройства из группы не приведет к изменению состояния самого устройства. (например, если правило политики запрещало использование камеры, то после снятия такой политики камера останется не доступной на устройстве). Для изменения состояния необходимо явно в политике установить целевое состояние. Также можно использовать корпоративный шаблон политики (пп. 2.4.3.1). Например, если в корпоративном шаблоне политики будет задано разрешающее правило политики на использование камеры, и при этом на устройстве будет назначена любая политика (даже пустая), тогда устройство приведет в состояние, указанное в корпоративный шаблон. Важно понимать, что корпоративный шаблон действует на все устройствах, на которых действует хотя бы одна политика и регулирует только те правила, которые явно не заданы в политиках.

Отвязать политики от группы устройств и/или группу пользователей возможно через:

- карточку политики (пп. 2.4.7.1);
- карточку группы устройств (пп. 2.4.7.2);
- карточку группы пользователей (пп. 2.4.7.3).

2.4.7.1. Отвязка политики от группы устройств и/или группы пользователей через карточку политики

Для отвязки политики от группы устройств и/или группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать на название политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в открывшейся карточке политики перейти во вкладку «Группы»;
- нажать кнопку «Редактировать группы» (см. Рисунок 45 [2]);
- в открывшемся окне нажать значок  «Отвязать политику от группы» (Рисунок 183).

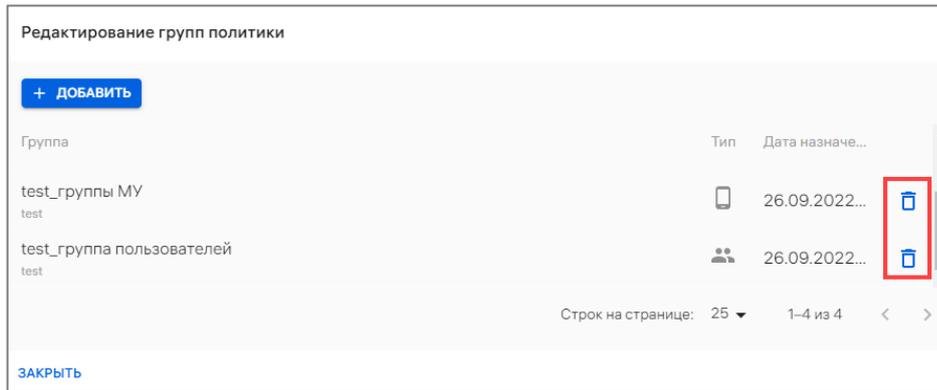


Рисунок 183

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки, политика будет отвязана от группы устройств или групп пользователей.

2.4.7.2. Отвязка политики от группы устройств через карточку группы

Для отвязки политики от группы устройств необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в открывшейся карточке группы устройств перейти во вкладку «Политики»;
- выбрать политику, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 184 [1]);
- в списке быстрых действий выбрать значок  «Отвязать политики от группы» (Рисунок 184 [2]).

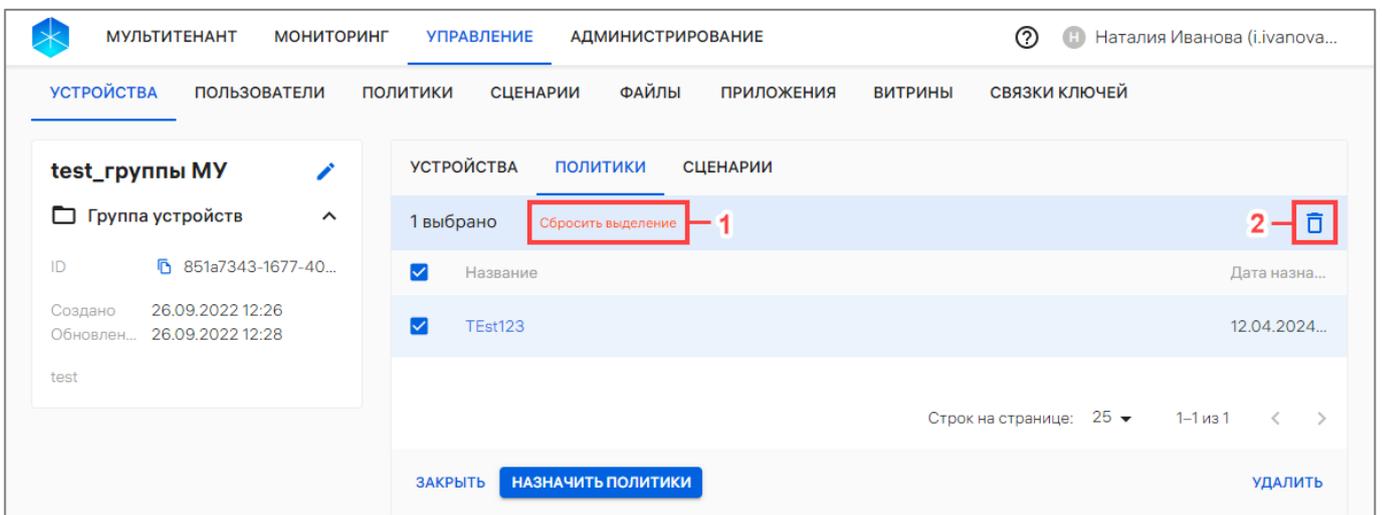


Рисунок 184

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки политики от группы устройств отобразится соответствующее сообщение.

2.4.7.3. Отвязка политики от группы пользователей через карточку группы

Для отвязки политик от группы пользователей через карточку группы необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в открывшейся карточке группы пользователей перейти во вкладку «Политики»;
- выбрать политику, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 185 [1]);
- в списке быстрых действий выбрать значок  «Отвязать политики от группы» (Рисунок 185 [2]).

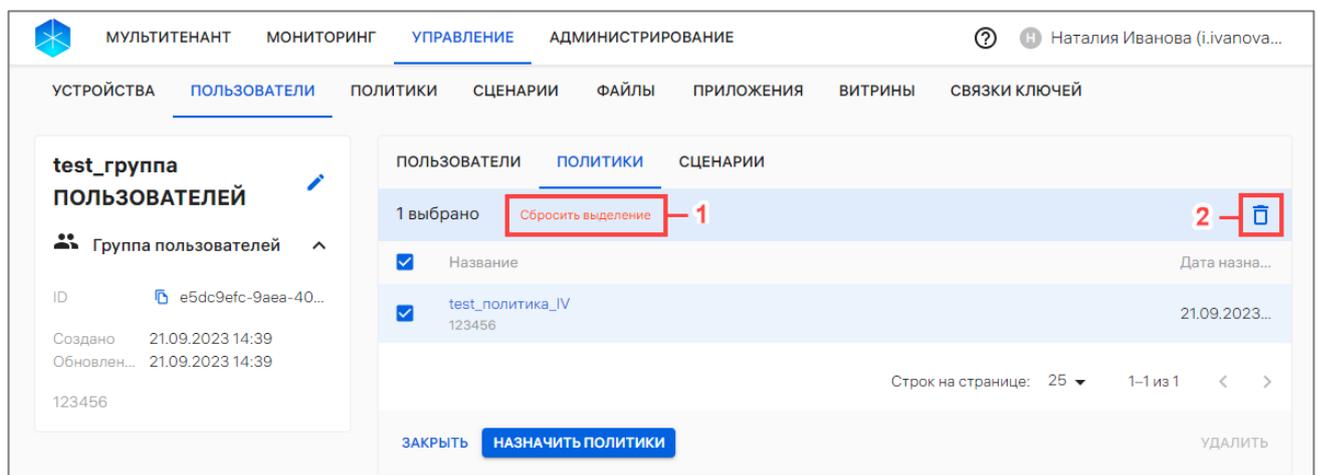


Рисунок 185

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки политики от группы пользователей отобразится соответствующее сообщение.

2.4.8. Удаление политики

ПРИМЕЧАНИЕ. Перед удалением политики необходимо предварительно отвязать ее от всех групп устройств или групп пользователей в соответствии с п. 2.4.7.

Для удаления политики из ПУ необходимо выполнить следующие действия:

- перейти в подраздел «Политики» раздела «Управление»;
- нажать на название необходимой политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
- в карточке политики нажать кнопку «Удалить» (Рисунок 186);

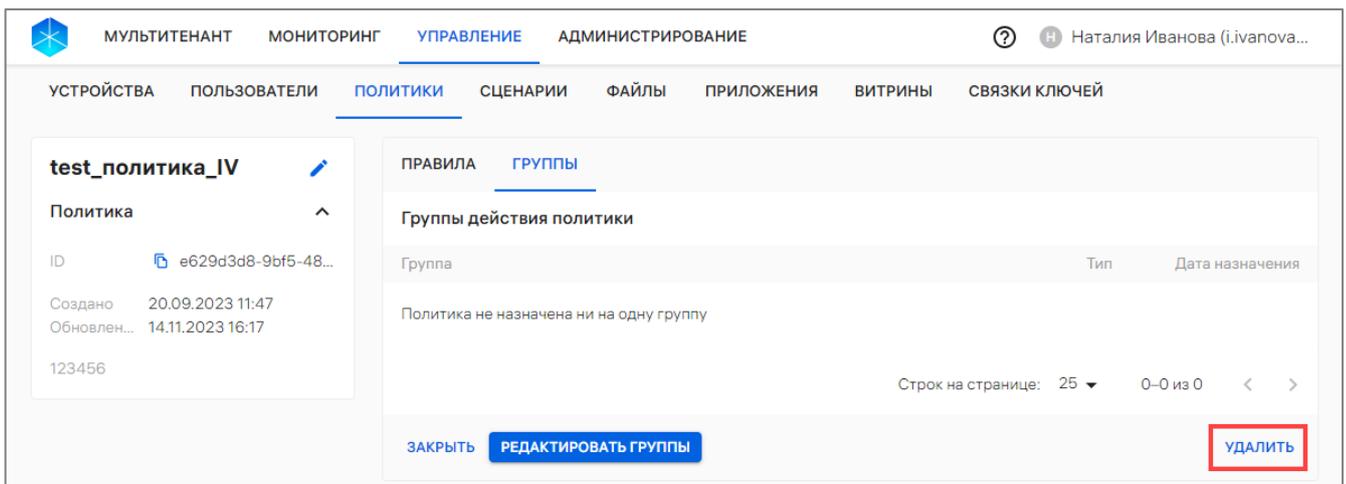


Рисунок 186

- в отобразившемся окне подтвердить либо отменить действия (Рисунок 187).



Рисунок 187

В результате политика будет успешно удалена.

2.5. Подраздел «Сценарии»

Подраздел «Сценарии» Консоли администратора ПУ предназначен для создания офлайн-сценариев и применения их на устройствах.

Офлайн-сценарии – правила, которые отправляются на устройства с указанием действия (события) по срабатыванию. Правила должны мгновенно примениться на устройстве по указанному событию, даже в случае, если в этот момент нет связи с сервером.

ПРИМЕЧАНИЯ:

- ✓ Для корректного управления устройством необходимо, чтобы на устройстве было выставлено корректное время и был задан часовой пояс;
- ✓ На группу устройств или группу пользователей может быть одновременно назначено несколько офлайн-сценариев.

Доступность событий и реакций офлайн-сценариев для разных версий ОС приведена в таблице (Таблица 41).

Таблица 41

Событие	Реакция					
	Заблокировать/ разблокировать устройство	Очистка устройства	Задать одноразовый пароль пользователя/ администратора	Задать период отправки событий безопасности	Разрешить/ запретить использование камеры	Разрешить/ запретить использование микрофона
Смена SIM-карты	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше
Отсутствие связи с сервером	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше
Вне зоны действия WLAN	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше
Нахождение в зоне WLAN	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше
Нахождение на территории, определяемой NFC-метками	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше
Нахождение вне территорий, определяемых координатами	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше
Нахождение на территориях, определяемых координатами	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7 и выше	ОС Аврора 4.0.2 и выше

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Управление», подраздел «Сценарии». В результате отобразится список сценариев (Рисунок 188 [1]).

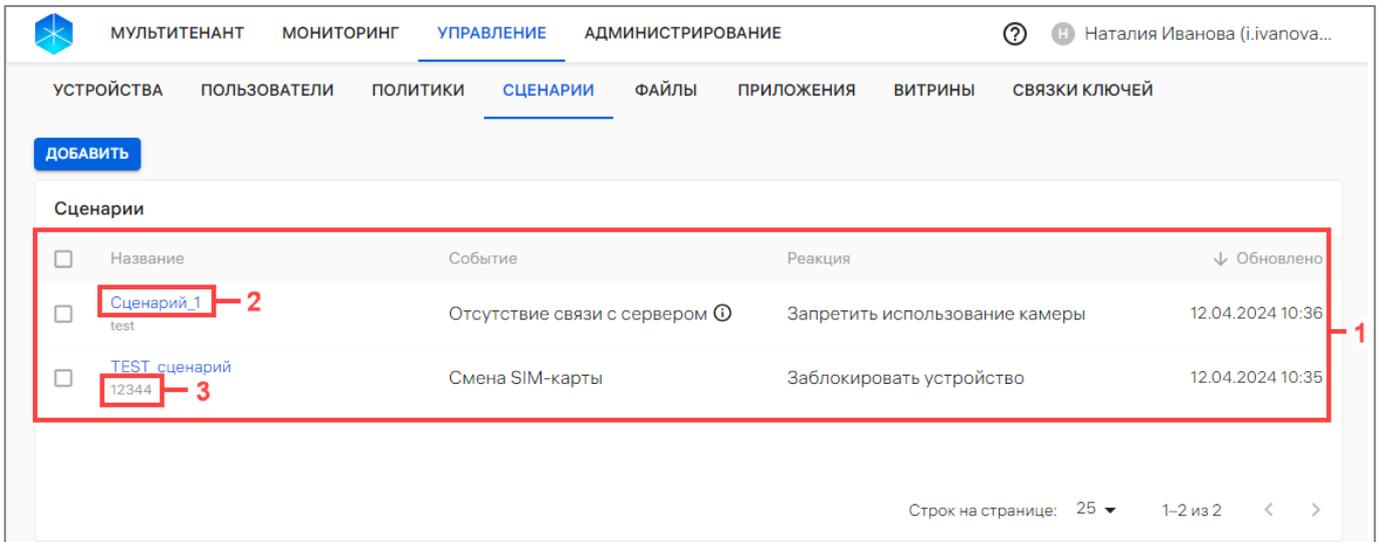


Рисунок 188

В рабочей области подраздела «Сценарии» информация отображается в столбцах, приведенных в таблице (Таблица 42), а при их отсутствии отображается сообщение «Нет данных».

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 42

Название столбца	Описание
Название	– название офлайн-сценария – представляет собой активную ссылку (см. Рисунок 188 [2]), при нажатии на которую осуществляется переход в карточку офлайн-сценария; – комментарий (см. Рисунок 188 [3]) – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 43). В поле содержится подсказка, доступная для просмотра при наведении курсора на значок ⓘ
Реакция	Действие, которое должно произойти с группой в результате назначения данного офлайн-сценария (доступные значения описаны в таблице (Таблица 43)
Обновлено	Дата и время последнего обновления офлайн-сценария

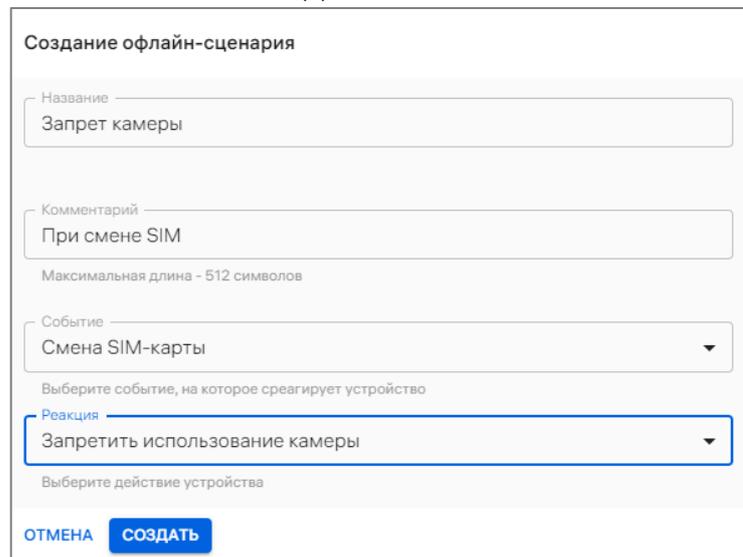
2.5.1. Добавление офлайн-сценария

ПРИМЕЧАНИЕ. Доступно добавление офлайн-сценариев со следующими параметрами:

- с разными событиями;
- с одним событием, но с разными реакциями (правилами);
- с одним событием («Нахождение в зоне WLAN» или «Вне зоны действия WLAN») и с одной реакцией, но с разными MAC-адресами (BSSID) точки доступа WLAN;
- с одним событием «Нахождение на территории, определяемой NFC-метками», при этом:
 - одновременно один и тот же ID метки не может быть на входе и выходе;
 - два офлайн-сценария с одинаковым ID метки входа или выхода не могут иметь одинаковую реакцию.

Для создания офлайн-сценария необходимо выполнить следующие действия:

- перейти в подраздел «Сценарии» раздела «Управление»;
- нажать кнопку «Добавить»;
- в открывшемся окне (Рисунок 189) заполнить поля, приведенные в таблице (Таблица 43);
- подтвердить либо отменить действия.



Создание офлайн-сценария

Название
Запрет камеры

Комментарий
При смене SIM
Максимальная длина - 512 символов

Событие
Смена SIM-карты
Выберите событие, на которое среагирует устройство

Реакция
Запретить использование камеры
Выберите действие устройства

ОТМЕНА СОЗДАТЬ

Рисунок 189

При успешном создании офлайн-сценария отобразится соответствующее сообщение.

Таблица 43

Параметр	Значения
Название	Название офлайн-сценария. Поле обязательно для заполнения
Комментарий	Дополнительная информация к офлайн-сценарию. Поле необязательно для заполнения
Событие	<p>Выбор значения из раскрывающегося списка. Событие, на которое среагирует устройство:</p> <ul style="list-style-type: none"> – Смена SIM-карты – при смене SIM-карты на устройстве сработает реакция, выбранная из раскрывающегося списка «Реакция»; – Отсутствие связи с сервером – при отсутствии связи с сервером Аврора Центр на устройстве сработает реакция, выбранная из раскрывающегося списка «Реакция». Дополнительно необходимо указать временной интервал (формат: [ДД] : [ЧЧ] : [ММ]) отсутствия связи с сервером, после наступления которого устройство среагирует; – Вне зоны действия WLAN – если устройство не обнаружит определенную сеть WLAN в доступных для подключения, то сработает реакция, выбранная из раскрывающегося списка «Реакция». <p>ПРИМЕЧАНИЕ. При выборе события «Вне зоны действия WLAN» отображается дополнительное поле, в котором необходимо указать BSSID (Basic Service Set Identification или идентификатор) точки доступа WLAN;</p> <ul style="list-style-type: none"> – Нахождение в зоне WLAN – если устройство обнаружит определенную сеть WLAN в доступных для подключения, то сработает реакция, выбранная из раскрывающегося списка «Реакция». <p>ПРИМЕЧАНИЕ. При выборе события «Нахождение в зоне WLAN» отображается дополнительное поле, в котором необходимо указать BSSID (Basic Service Set Identification или идентификатор) точки доступа WLAN;</p> <ul style="list-style-type: none"> – Нахождение на территории, определяемой NFC-метками (применение офлайн-сценария на состояние устройства определяется по NFC-метке) – при сканировании метки входа сработает реакция, выбранная из раскрывающегося списка «Реакция», и, наоборот, при сканировании метки выхода применение офлайн-сценария прекратится. <p>ВНИМАНИЕ! После сканирования NFC-метки выхода на устройстве применяется правило из политики, похожее на реакцию офлайн-сценария. Если такое правило отсутствует в политике, то состояние устройства не изменится. Необходимо назначить на устройство политику с похожим правилом, чтобы состояние устройства изменялось после сканирования метки выхода.</p>

Параметр	Значения
	<p>Пример: Задана реакция «Запретить использование камеры» с помощью офлайн-сценария с NFC-метками. При сканировании метки входа использование камеры будет недоступным. После сканирования метки выхода офлайн-сценарий прекратит действие на состояние устройства. При этом, если на устройство не была назначена политика с разрешением камеры, то запрет камеры на устройстве будет сохранен. Для разблокировки камеры необходимо назначить на устройство политику или отправить команду оперативного управления с разблокировкой камеры.</p> <p>При выборе события «Нахождение на территории, определяемой NFC-метками» дополнительно отображаются поля «ID меток входа» и «ID меток выхода», где необходимо указать уникальные идентификаторы меток входа и выхода, состоящие из 4, 7 или 8 пар символов, разделенных двоеточием. Доступно добавление нескольких идентификаторов меток.</p> <p>ВНИМАНИЕ! NFC-метка сканируется на устройствах:</p> <ul style="list-style-type: none"> – на базе ОС Аврора при заблокированном/разблокированном телефоне и при включенном экране; – на базе ОС Android при разблокированном устройстве и при включенном экране. На некоторых устройствах при включенной камере не срабатывает сканирование NFC; – Нахождение вне территорий, определяемых координатами – если местоположение устройства окажется вне заданной территории, то на состояние устройства начнет действовать офлайн-сценарий с реакцией, выбранной из раскрывающегося списка «Реакция». Дополнительно в раскрывающемся списке «Территория» необходимо выбрать требуемую территорию; – Нахождение на территориях, определяемых координатами – если местоположение устройства окажется внутри заданной территории, то на состояние устройства начнет действовать офлайн-сценарий с реакцией, выбранной из раскрывающегося списка «Реакция». Дополнительно в раскрывающемся списке «Территория» необходимо выбрать требуемую территорию. <p>ПРИМЕЧАНИЯ:</p> <ul style="list-style-type: none"> ✓ Если необходимой территории нет в списке, то требуется добавить ее (п. 4.1.5);

Параметр	Значения
	<ul style="list-style-type: none"> ✓ Точность определения координат устройства зависит от многих факторов, а именно: тип устройства, состояние сети, скорость, нахождение в здании или около высоких объектов, покрытие спутников, аппаратные и программные характеристики, уровень шума/помех и т.д; ✓ Приложение «Аврора Центр» получает координаты устройства из ОС каждые 10 минут (ОС Аврора и ОС Android) или каждые 50 метров (ОС Android). При необходимости доступно изменение частоты обновления координат в приложении «Аврора Центр» с помощью правила политики «Конфигурация/Обновление координат в клиенте Аврора Центр» (пп. 2.4.1.28)
Реакция	<p>Выбор значения из раскрывающегося списка:</p> <ul style="list-style-type: none"> – Заблокировать устройство – устройство будет заблокировано; – Разблокировать устройство – устройство будет разблокировано; – Очистка устройства – устройство будет очищено (до заводских настроек); – Задать одноразовый пароль пользователя – необходимо ввести пароль (от 7 до 12 символов), который пользователь сможет использовать для разблокировки устройства. Пароль должен соответствовать требованиям парольной политики; – Задать одноразовый пароль администратора – необходимо ввести пароль (от 7 до 12 символов), который администратор сможет использовать для разблокировки устройства. Пароль должен соответствовать требованиям парольной политики; – Задать период отправки событий безопасности – необходимо задать расписание отправки сообщений о событиях безопасности (security.d journaling daemon), произошедших на устройстве, в формате: [ДД] : [ЧЧ] : [ММ]; – Разрешить использование камеры – использование камеры на устройствах будет разрешено; – Запретить использование камеры – использование камеры на устройствах будет запрещено; – Разрешить использование микрофона – использование микрофона на устройствах будет разрешено; – Запретить использование микрофона – микрофон будет недоступен для записи звука во всех приложениях и внешних устройств, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов

2.5.2. Назначение офлайн-сценария на группы устройств или группы пользователей

Назначить офлайн-сценарии на группы устройств или пользователей возможно следующими способами:

- через карточку офлайн-сценария (пп. 2.5.2.1);
- с помощью списка быстрых действий (пп. 2.5.2.2);
- через карточку группы устройств (пп. 2.5.2.3);
- через карточку группы пользователей (пп. 2.5.2.4).

2.5.2.1. Назначение офлайн-сценария на группы устройств или группы пользователей через карточку офлайн-сценария

Для назначения офлайн-сценария на группы устройств или пользователей через карточку офлайн-сценария необходимо выполнить следующие действия:

- перейти в подраздел «Сценарии» раздела «Управление»;
- перейти в карточку офлайн-сценария (п. 2.1.6);
- для добавления группы устройств или пользователей в раскрывающемся списке выбрать «Добавить группы устройств» или «Добавить группы пользователей» (Рисунок 190);

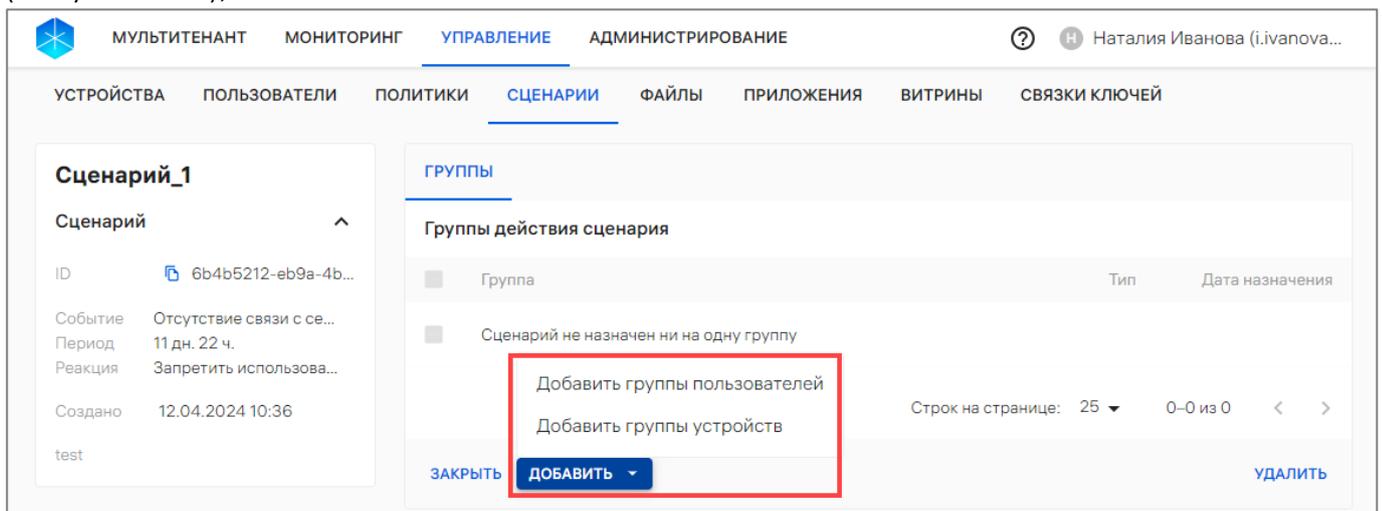


Рисунок 190

- в открывшемся окне выбрать группу из списка, при необходимости воспользовавшись фильтром по названию группы (Рисунок 191 [1]);

- добавленная группа отобразится в списке. При необходимости возможно удалить добавленную группу из списка, нажав значок  (Рисунок 191 [2]). Также доступна возможность отвязки офлайн-сценария от группы, описание которой приведено в п. 2.5.3;

- далее, для назначения офлайн-сценария на добавленные группы, нажать кнопку «Назначить на группы» либо отменить все последние действия нажатием кнопки «Отмена» (Рисунок 191 [3]).

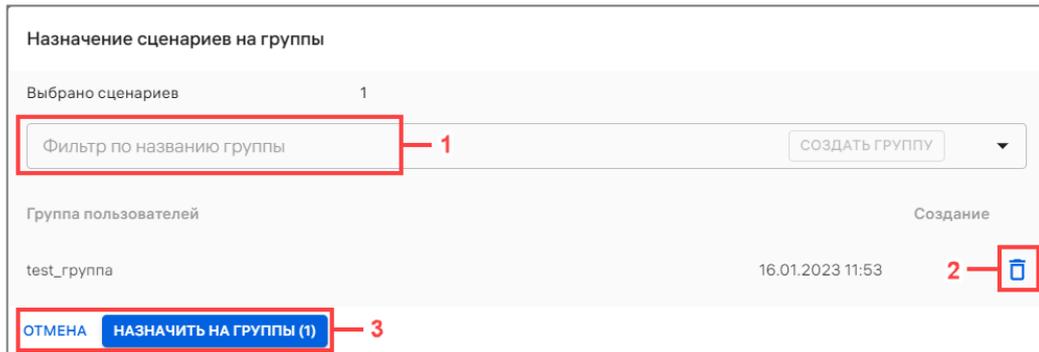


Рисунок 191

В результате применения офлайн-сценария отобразится соответствующее сообщение.

2.5.2.2. Назначение офлайн-сценария на группы устройств/группы пользователей с помощью списка быстрых действий

Для назначения офлайн-сценария на группы устройств/пользователей с помощью списка быстрых действий необходимо выполнить следующие действия:

- перейти в подраздел «Сценарии» раздела «Управление»;
- выбрать офлайн-сценарии, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 192 [1]);
- в списке быстрых действий выбрать:
 - значок  (Рисунок 192 [2]) для назначения офлайн-сценария на группу пользователей;
 - значок  (Рисунок 192 [3]) для назначения офлайн-сценария на группу устройств;
- в открывшемся окне выполнить действия, приведенные в пп. 2.5.2.1.

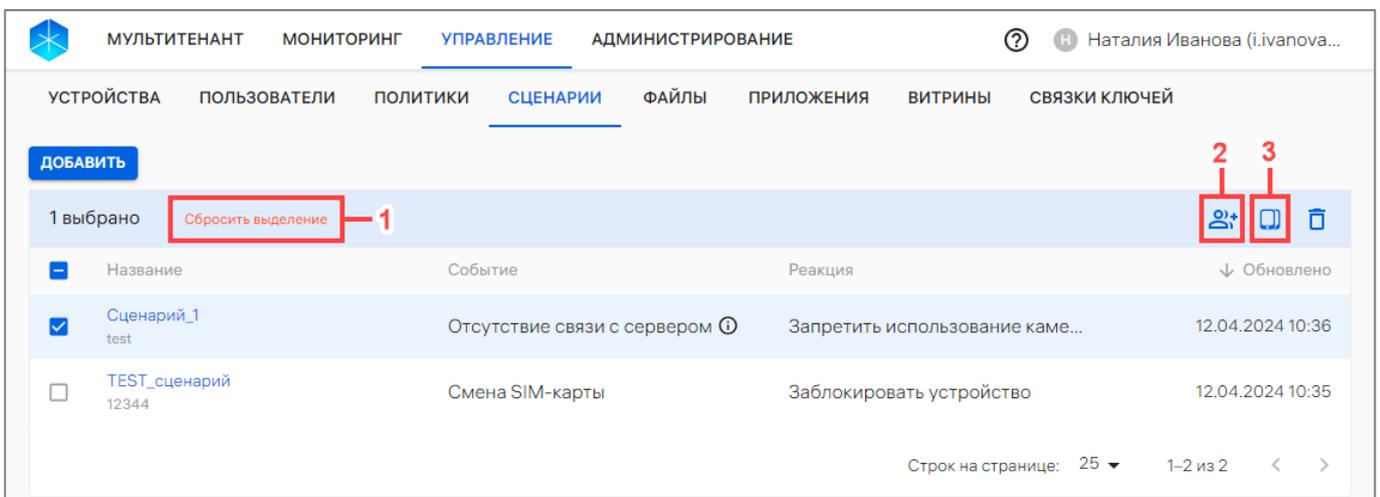


Рисунок 192

2.5.2.3. Назначение офлайн-сценария на группы устройств через карточку группы

Для назначения офлайн-сценария на группу устройств через карточку группы необходимо выполнить следующие действия:

- перейти в подраздел «Устройства» раздела «Управление»;
- в области фильтров выбрать «Поиск по группам»;
- нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));
- в открывшейся карточке перейти во вкладку «Сценарии»;
- нажать кнопку «Назначить сценарии» (Рисунок 193);

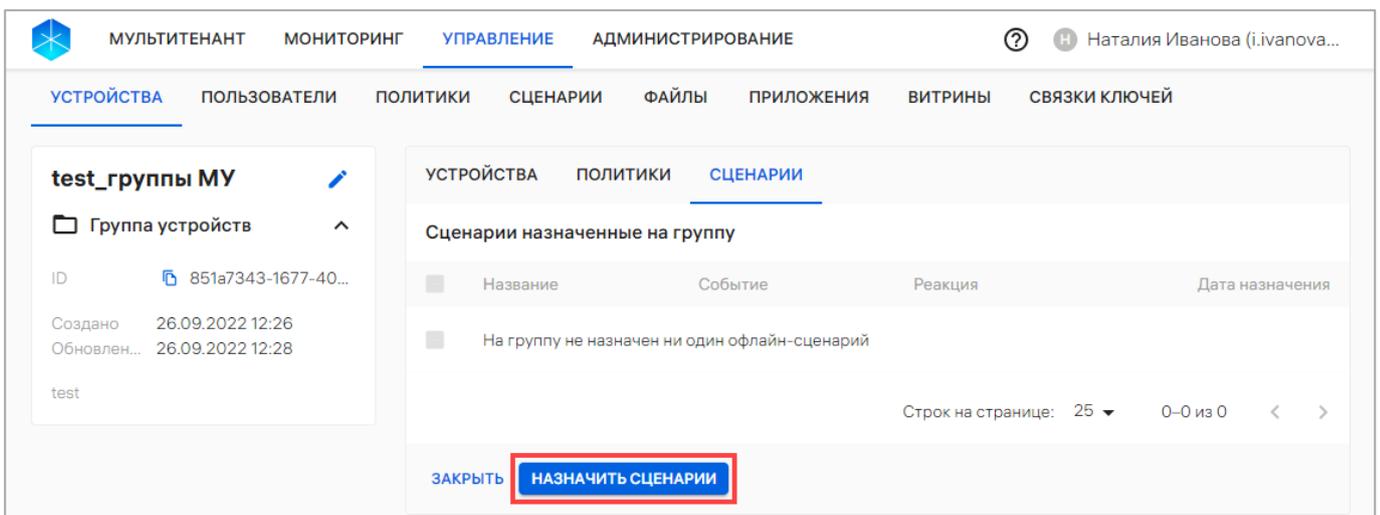


Рисунок 193

– в отобразившемся окне выбрать офлайн-сценарий из раскрывающегося списка или воспользоваться фильтром (Рисунок 194 [1]). Далее, при необходимости, возможно добавить дополнительный сценарий, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранные сценарии, нажав значок  «Убрать из списка» (Рисунок 194 [3]);



Рисунок 194

– нажать кнопку «Назначить сценарии» (см. Рисунок 194 [2]) либо кнопку «Отмена» для отмены действий.

В результате офлайн-сценарий будет назначен на группу устройств.

2.5.2.4. Назначение офлайн-сценария группы пользователей через карточку группы

Для назначения офлайн-сценария на группу пользователей через карточку группы необходимо выполнить следующие действия:

- перейти в подраздел «Пользователи» раздела «Управление»;
 - выбрать в области фильтров «Поиск по группам»;
 - нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);
 - в открывшейся карточке перейти во вкладку «Сценарии»;
 - нажать кнопку «Назначить сценарии» (см. Рисунок 41 [2]);
 - в отобразившемся окне выполнить действия, описанные в пп. 2.5.2.3.
- В результате офлайн-сценарий будет назначен на группу пользователей.

2.5.3. Отвязка офлайн-сценарий от группы устройств/группы пользователей

Отвязать офлайн-сценарии от группы устройств или группы пользователей возможно следующими способами:

- через карточку офлайн-сценария (пп. 2.5.3.1);
- через карточку группы устройств/группы пользователей (пп. 2.5.3.2).

2.5.3.1. Отвязка офлайн-сценария от группы устройств/группы пользователей через карточку офлайн-сценария

Для отвязки офлайн-сценарий от группы устройств/группы пользователей необходимо выполнить следующие действия:

- перейти в подраздел «Сценарии» раздела «Управление»;
- перейти в карточку офлайн-сценария;
- выбрать группу, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 195 [1]);
- в списке быстрых действий выбрать значок  «Отвязать сценарий от группы» (Рисунок 195 [2]);

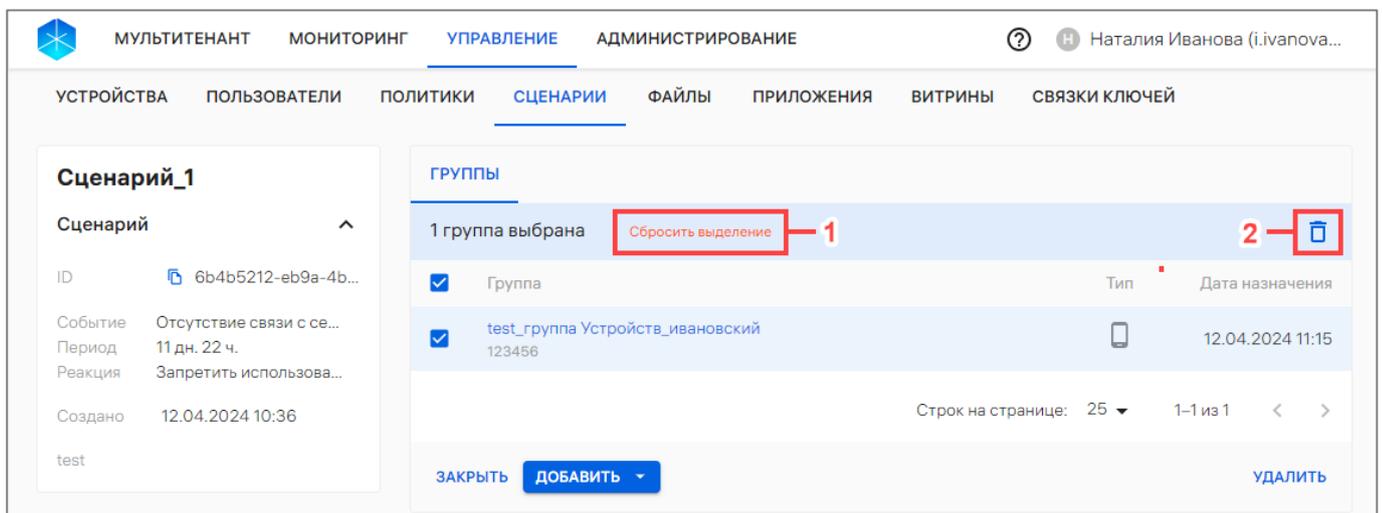


Рисунок 195

– в отобразившемся окне подтвердить либо отменить действие (Рисунок 196).

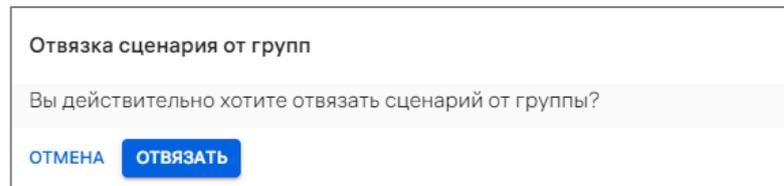


Рисунок 196

В результате отвязки офлайн-сценарий будет удален со всех устройств группы.

ВНИМАНИЕ! Если результат данного офлайн-сценария уже применен на устройствах и при этом на устройствах не назначена политика с иным действием, после отвязки офлайн-сценария его результат не будет отменен.

2.5.3.2. Отвязка офлайн-сценария от группы устройств/группы пользователей через карточку группы

Для отвязки офлайн-сценария от группы устройств/группы пользователей через карточку группы необходимо выполнить следующие действия:

– перейти:

- в подраздел «Устройства» раздела «Управление» – для отвязки группы устройств;

- в подраздел «Пользователи» раздела «Управление» – для отвязки группы пользователей;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название необходимой группы для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5));

– в открывшейся карточке группы перейти во вкладку «Сценарии»;

– выбрать офлайн-сценарий, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения следует нажать кнопку «Сбросить выделение» (Рисунок 197 [1]);

– в списке быстрых действий выбрать значок  «Отвязать сценарии от группы» (Рисунок 197 [2]);

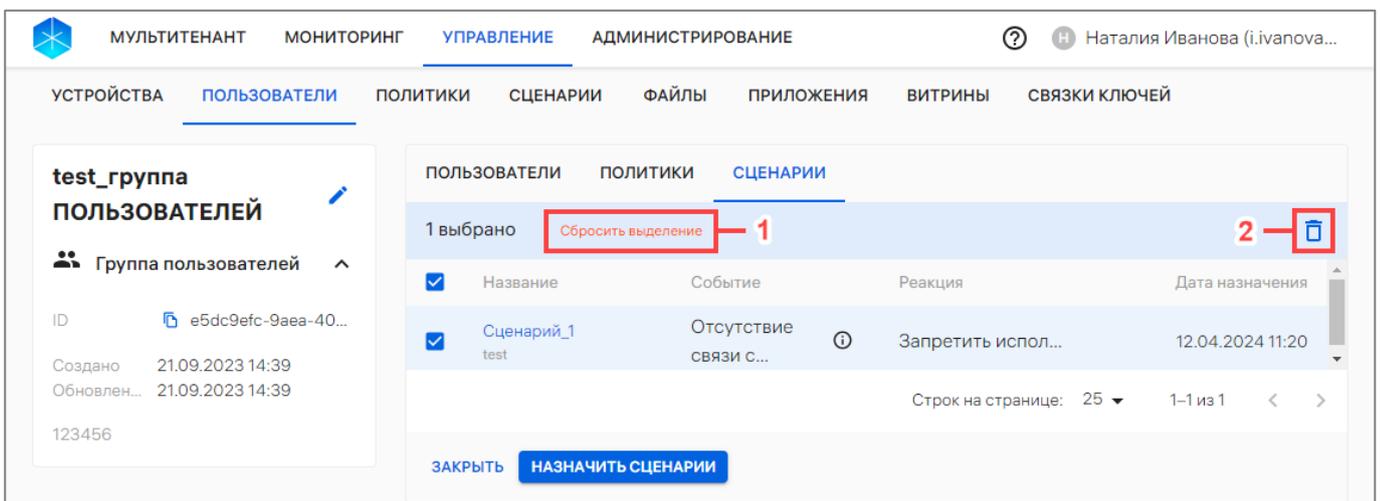


Рисунок 197

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 198).

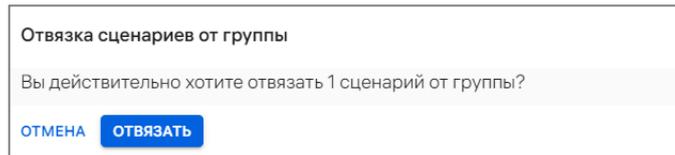


Рисунок 198

В результате успешной отвязки офлайн-сценарий будет удален со всех устройств группы пользователей/устройств.

ВНИМАНИЕ! Если действие данного офлайн-сценария уже применено на устройствах и при этом на них не назначена политика с противоположным действием, после отвязки офлайн-сценария его действие не будет отменено.

2.5.4. Удаление офлайн-сценария

Удалить офлайн-сценарий возможно одним из следующих способов:

1) С помощью списка быстрых действий. Для этого необходимо:

- перейти в подраздел «Сценарии» раздела «Управление»;
- выбрать офлайн-сценарии, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 199 [1]);
- в списке быстрых действий выбрать значок  (Рисунок 199 [2]);

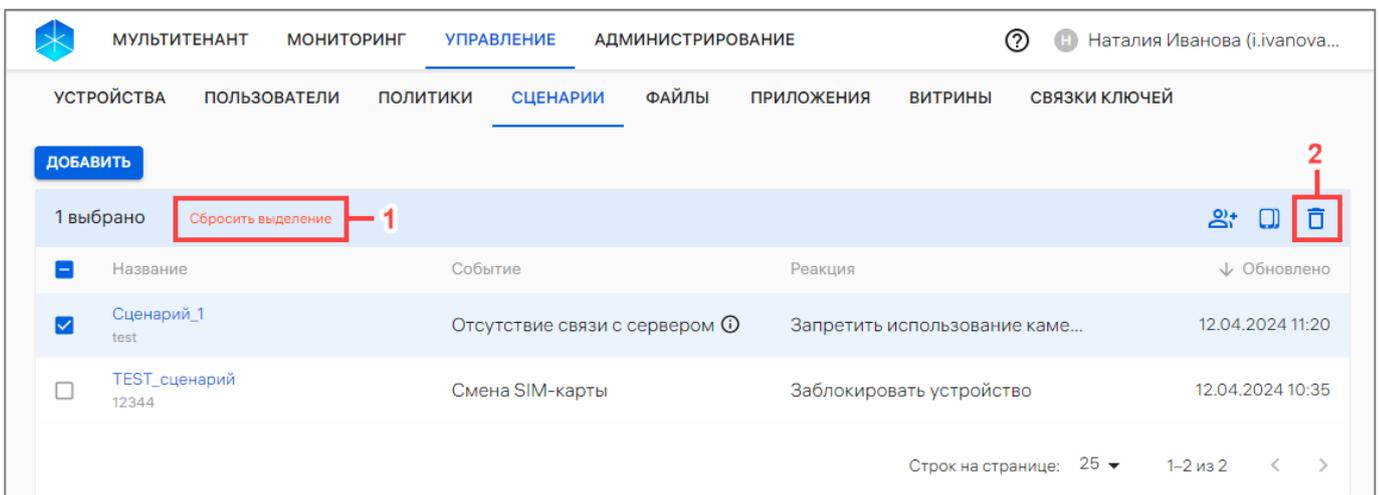


Рисунок 199

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 200);

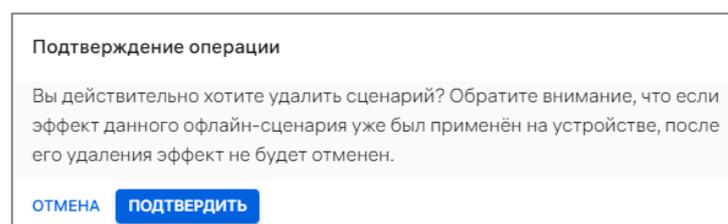


Рисунок 200

- 2) Через карточку офлайн-сценария. Для это необходимо:
- перейти в подраздел «Сценарии» раздела «Управление»;
 - перейти в карточку офлайн-сценария (п. 2.1.6), который необходимо удалить;
 - нажать кнопку «Удалить» (Рисунок 201);

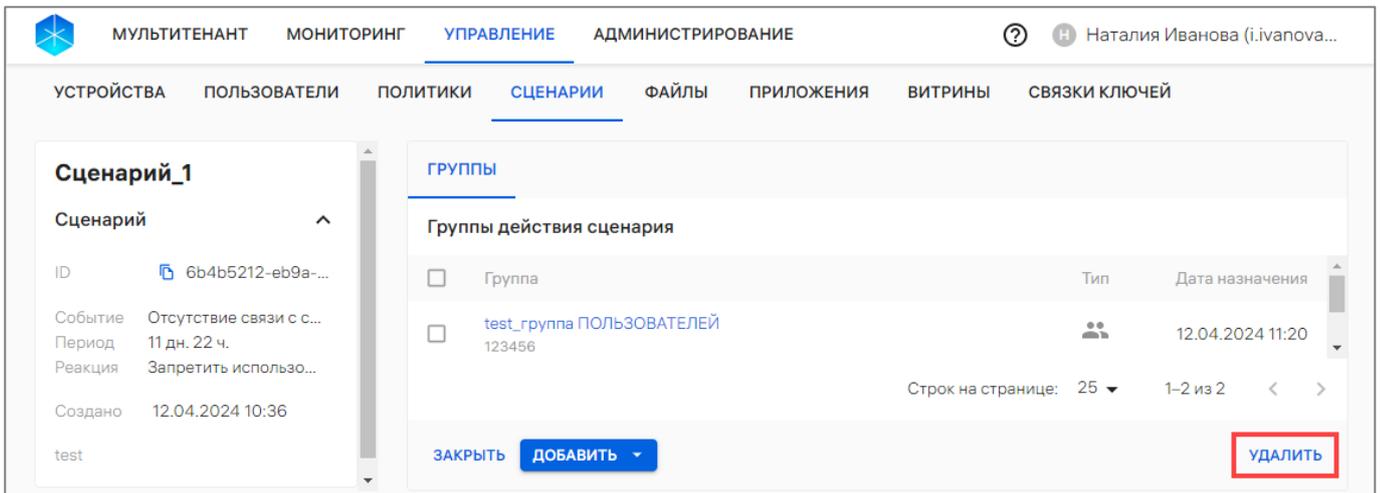


Рисунок 201

– в отобразившемся окне подтвердить либо отменить действия (см. Рисунок 200).

В результате успешного удаления офлайн-сценария из системы отобразится соответствующее сообщение и будут удалены все связи офлайн-сценария с группами, а также он будет удален со всех устройств, на которые был назначен.

ВНИМАНИЕ! Если результат данного офлайн-сценария уже применен на устройствах и при этом на них не назначена политика с противоположным действием, после отвязки офлайн-сценария его результат не будет отменен.

2.6. Подраздел «Файлы»

Подраздел «Файлы» Консоли администратора ПУ предназначен для работы со списком файлов (скриптов), которые возможно добавить на устройства.

Для доставки файла (скрипта) на устройство его необходимо добавить в ПУ.

В Консоли администратора ПУ предусмотрена возможность добавления файлов (скриптов) одним из следующих способов:

- добавление файла с локального компьютера (пп. 2.6.1.1);
- добавление файла из Git-репозитория (пп. 2.6.1.2).

ПРИМЕЧАНИЕ. Возможно загрузить несколько версий одного файла и при необходимости скачать, согласовать и удалить нужную версию (п. 2.6.2), либо удалить все версии файла (п. 2.6.4).

Для перехода в подраздел необходимо выбрать в верхней панели подраздел «Файлы» раздела «Управление». В результате в рабочей области появится список файлов (скриптов) (Рисунок 202 [2]), информация о которых отображается в столбцах,

приведенных в таблице (Таблица 44), а при отсутствии добавленных файлов отображается сообщение «Нет данных».

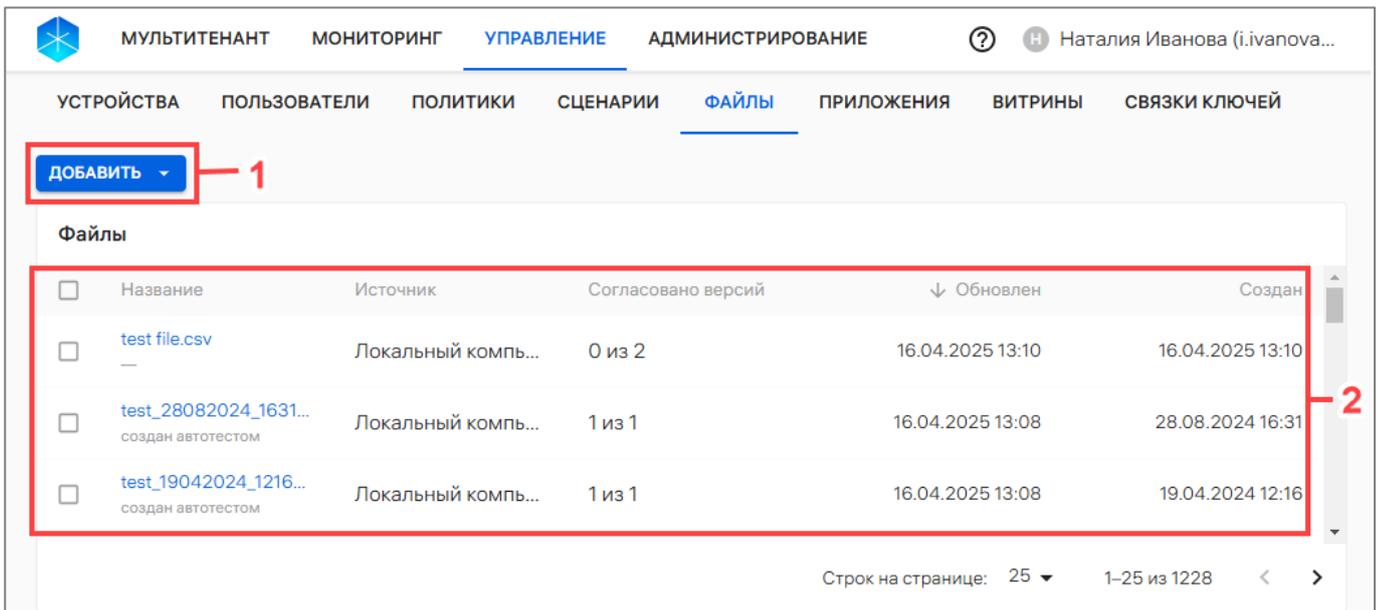


Рисунок 202

Таблица 44

Параметр	Описание
Название	– название файла (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке файла); – комментарий – дополнительная информация (заполняется при необходимости)
Источник	Источник, откуда был загружен рабочий файл
Согласовано версий	Количество согласованных версий файла
Обновлен	Дата обновления рабочего файла
Создан	Дата создания рабочего файла

2.6.1. Добавление файла (скрипта)

2.6.1.1. Добавление файла (скрипта) с компьютера

Для добавления файла (скрипта) с компьютера на устройство необходимо добавить его в ПУ, выполнив следующие действия:

- нажать кнопку «Добавить» (см. Рисунок 202 [1]);
- в раскрывающемся списке выбрать пункт «Добавить файл с компьютера» (Рисунок 203);

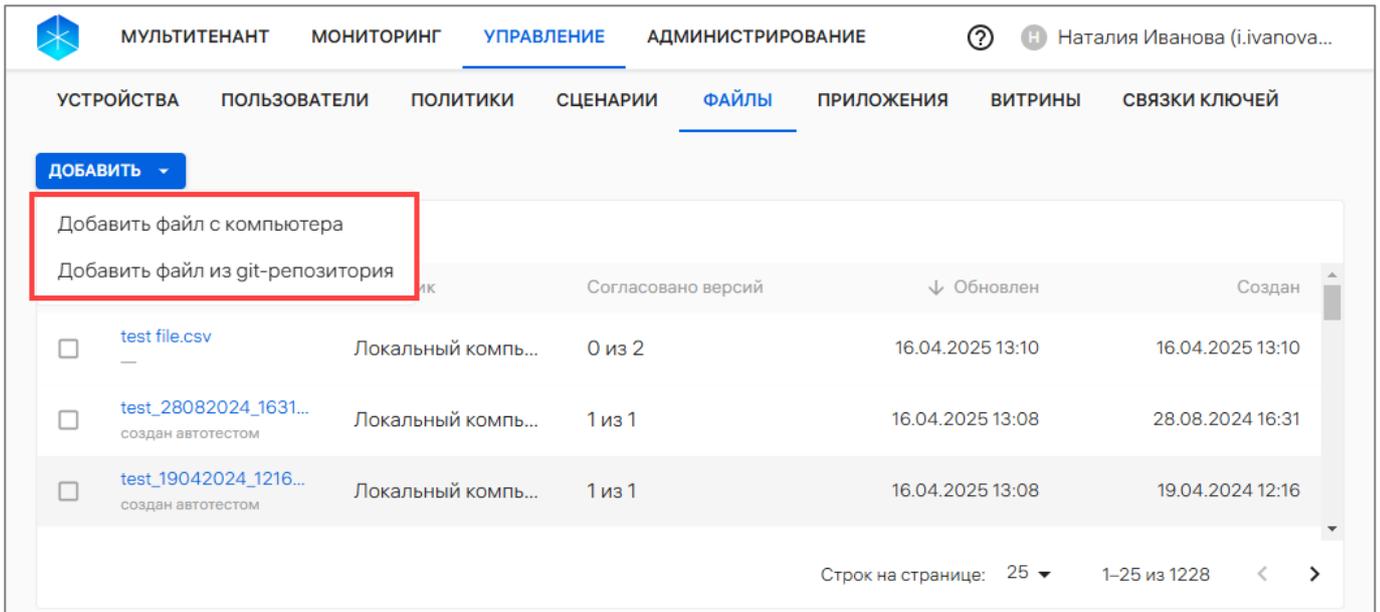


Рисунок 203

– в открывшемся окне (Рисунок 204) добавить комментарий (при необходимости) и загрузить файл одним из способов:

- переместить файл в область загрузки;
- нажать кнопку «Загрузить файл» с последующим выбором файла для загрузки.

ПРИМЕЧАНИЕ. Максимальный размер загружаемого файла – 2048 МБ. Ограничений на формат файла нет;

- подтвердить либо отменить действия.

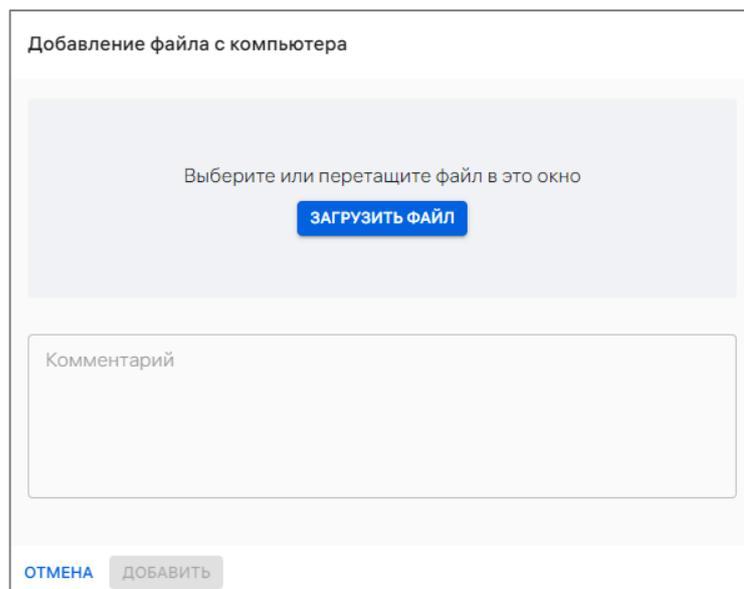


Рисунок 204

При успешном добавлении файл (скрипт) будет добавлен в ПУ и отобразится в списке файлов. Эта версия файла будет считаться первой. При необходимости возможно добавить другие версии файла (п. 2.6.2).

2.6.1.2. Добавление файла (скрипта) из Git-репозитория

Для добавления файла (скрипта) из Git-репозитория на устройство необходимо добавить его в ПУ, выполнив следующие действия:

- нажать кнопку «Добавить» (см. Рисунок 202 [1]);
- в раскрывающемся списке выбрать пункт «Добавить файл из git-репозитория» (см. Рисунок 203);
- в открывшемся окне (Рисунок 205) заполнить поля приведенные в таблице (Таблица 45);

Таблица 45

Поле	Описание
Git-репозиторий	В раскрывающемся списке выбрать необходимый Git-репозиторий. Если нужного Git-репозитория нет в списке, добавить в ПУ интеграцию с ним (пп. 4.1.4.6)
Относительный путь к файлу	Ввести относительный путь к файлу в Git-репозитории
Комментарий	Дополнительная информация (заполняется при необходимости)

Рисунок 205

При успешном добавлении, файл (скрипт) будет добавлен в ПУ и отобразится в списке файлов. Эта версия файла будет считаться первой. При необходимости возможно добавить другие версии файла (п. 2.6.2).

2.6.2. Добавление, скачивание, согласование и удаление версии файла (скрипта)

ПРИМЕЧАНИЕ. Если файл был добавлен из Git-репозитория и в настройках интеграции с Git-репозиторием была задана частота синхронизации, то ППО автоматически загрузит новую версию файла (при ее наличии) при следующей синхронизации. Если частота синхронизации не была задана, то для добавления новой версии файла используйте инструкцию ниже.

АДМГ.20134-01 90 01-3

Для добавления версии файла (скрипта) необходимо:

- перейти в карточку файла (п. 2.1.7);
- нажать кнопку «Добавить версию» (Рисунок 206 [1]);

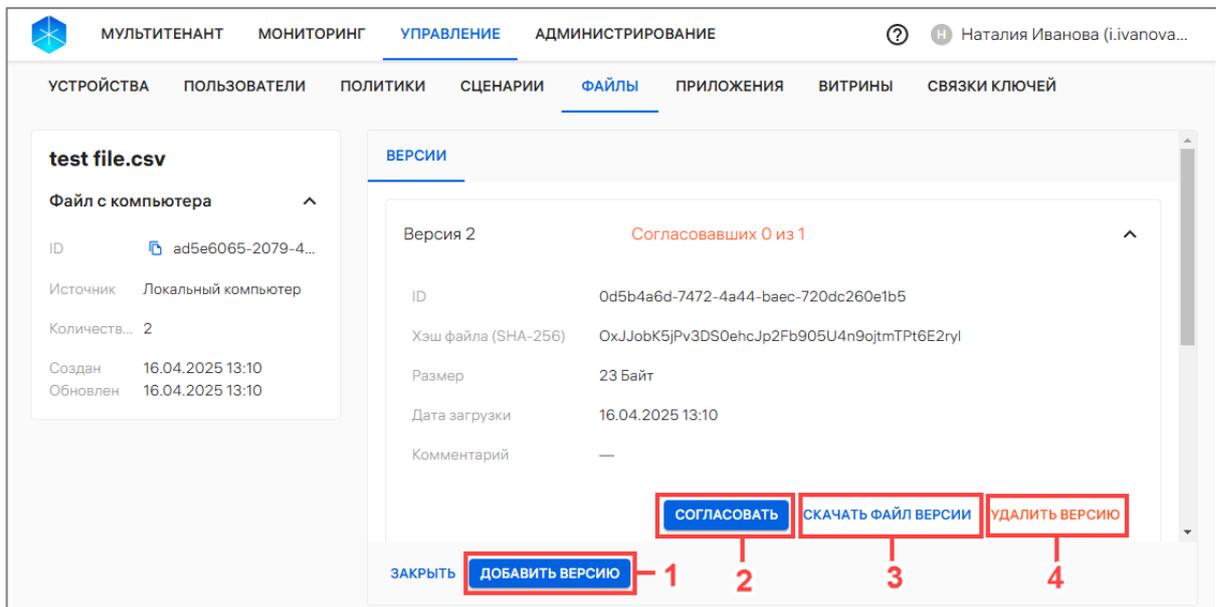


Рисунок 206

– в отобразившемся окне:

- если файл был загружен с локального компьютера, необходимо перетащить файл в область загрузки или нажать «Загрузить файл» и выбрать необходимый файл (Рисунок 207);

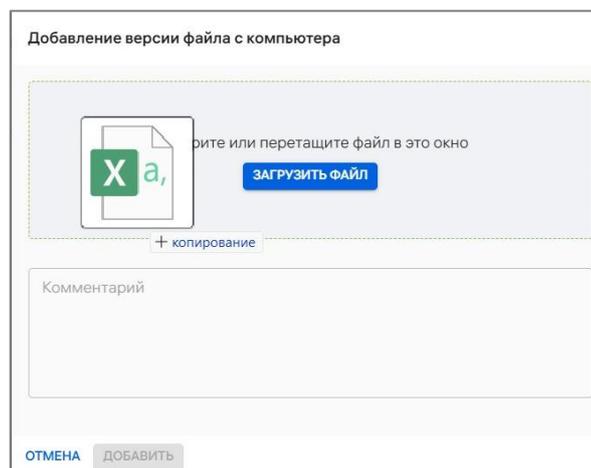


Рисунок 207

- если файл из Git-репозитория, то ПУ автоматически найдет новую версию файла (Рисунок 208);

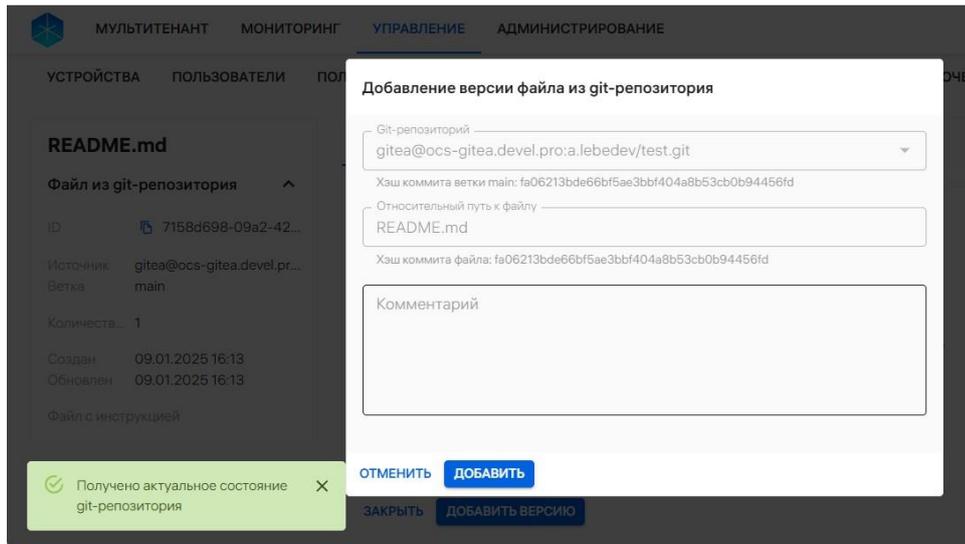


Рисунок 208

- при необходимости в поле «Комментарий» ввести дополнительную информацию к версии файла;

- подтвердить либо отменить действия.

При успешном добавлении файла его версия будет добавлена в ПУ.

Также доступно согласовать необходимую версию файла, загруженного другим администратором, нажав на кнопку «Согласовать» (см. Рисунок 206 [2]).

ПРИМЕЧАНИЕ. Если в настройках администрирования ПУ было задано количество администраторов для согласования файлов (подробнее в пп. 4.1.3.2), то, чтобы версия файла была доступна для распространения через политику, она должна быть согласована заданным количеством администраторов. При этом администратор, который загрузил версию файла в ПУ, не может ее согласовать.

При необходимости версии файлов возможно:

- скачать из ПУ на локальный компьютер, нажав на кнопку «Скачать файл версии» (см. Рисунок 206 [3]);

- удалить, нажав на кнопку «Удалить версию» (см. Рисунок 206 [4]), если файл не добавлен ни в одну политику в ПУ.

2.6.3. Доставка файла и выполнение скрипта на устройстве с помощью ПУ

С помощью ПУ возможно доставлять файлы (в том числе и скрипты) на активированное устройство, функционирующее под управлением ОС Android и ОС семейства Linux, а также выполнять доставленные скрипты.

Для доставки файла и выполнения скрипта необходимо:

- добавить файл (скрипт) в ПУ (п. 2.6.1);
- создать политику «Файлы/Доставка на устройство» (пп. 2.4.1.37) и «Скрипты/Выполнение на устройстве» (пп. 2.4.1.39) или отредактировать существующую политику, добавив в нее новое правило по доставке файлов или выполнению скриптов;
- назначить политику на группу, в которую входит устройство.

В результате:

- файл будет доставлен на устройство и доступен только для чтения;
- скрипт будет доставлен и выполнен на устройстве.

ПРИМЕЧАНИЕ. Для успешного выполнения скрипта необходимо ознакомиться с особенностями выполнения скриптов на устройстве (Приложение 3).

2.6.4. Удаление файла (скрипта) со всеми его версиями

Для удаления файла (скрипта) со всеми его версиями необходимо выполнить следующие действия:

– выбрать файл, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 209 [1]).

ВНИМАНИЕ! Доступно удаление только одного файла за раз;

– в списке быстрых действий выбрать значок  «Удалить файл» (Рисунок 209 [2]);

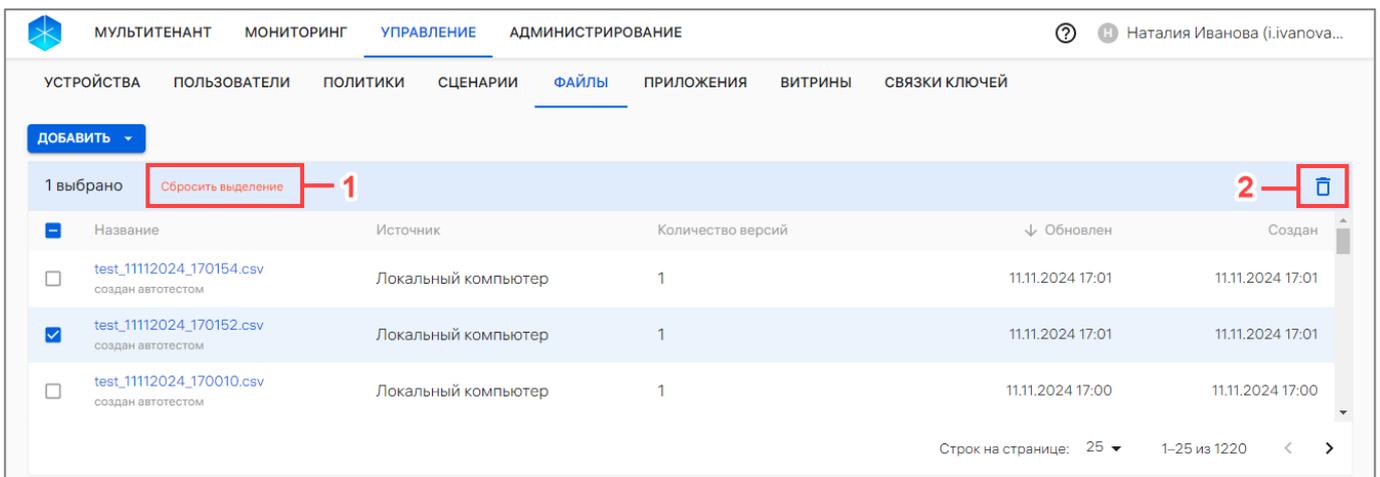


Рисунок 209

– в отобразившемся окне (Рисунок 210) подтвердить либо отменить действия.

ПРИМЕЧАНИЕ. Если файл применен в политике «Файлы/Доставка на устройство», отобразится предупреждающее сообщение о том, что удалить файл невозможно. Для удаления файла необходимо исключить файл из правила политики и выполнить шаги, указанные выше.

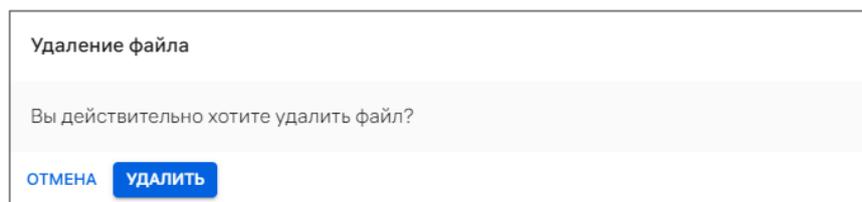


Рисунок 210

В результате файл будет успешно удален.

3. РАБОТА В РАЗДЕЛЕ «МОНИТОРИНГ» КОНСОЛИ АДМИНИСТРАТОРА ПУ В ПОДРАЗДЕЛЕ «ИНДИКАТОРЫ»

Подраздел «Индикаторы» Консоли администратора ПУ предназначен для мониторинга показателей устройств и контроля их отклонений.

Для перехода в подраздел необходимо в верхней панели выбрать подраздел «Индикаторы» раздела «Мониторинг». В результате отобразится информация о устройствах в виде диаграмм и пояснений к ним, а также фоновый процесс импорта устройств, пользователей и их групп в следующих окнах (Рисунок 211):

- «Подключение устройств»;
- «Соответствие политикам»;
- «Активация устройств»;
- «Процессы»;
- «Статус клиента АЦ».

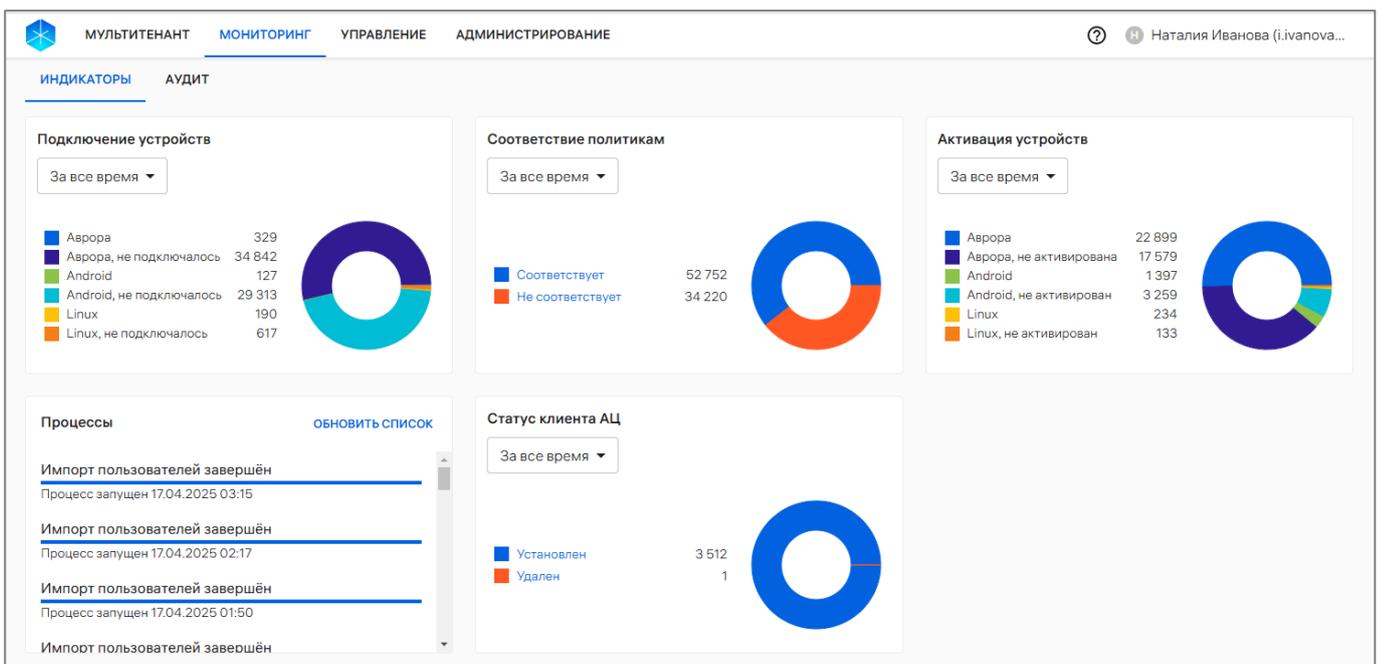


Рисунок 211

Возможно выбрать необходимый период отображения данных по устройствам из раскрывающегося списка (Рисунок 212):

- «За все время»;
- «За сутки»;
- «За неделю»;
- «За месяц».

Статистическая информация будет отображена за выбранный период времени.

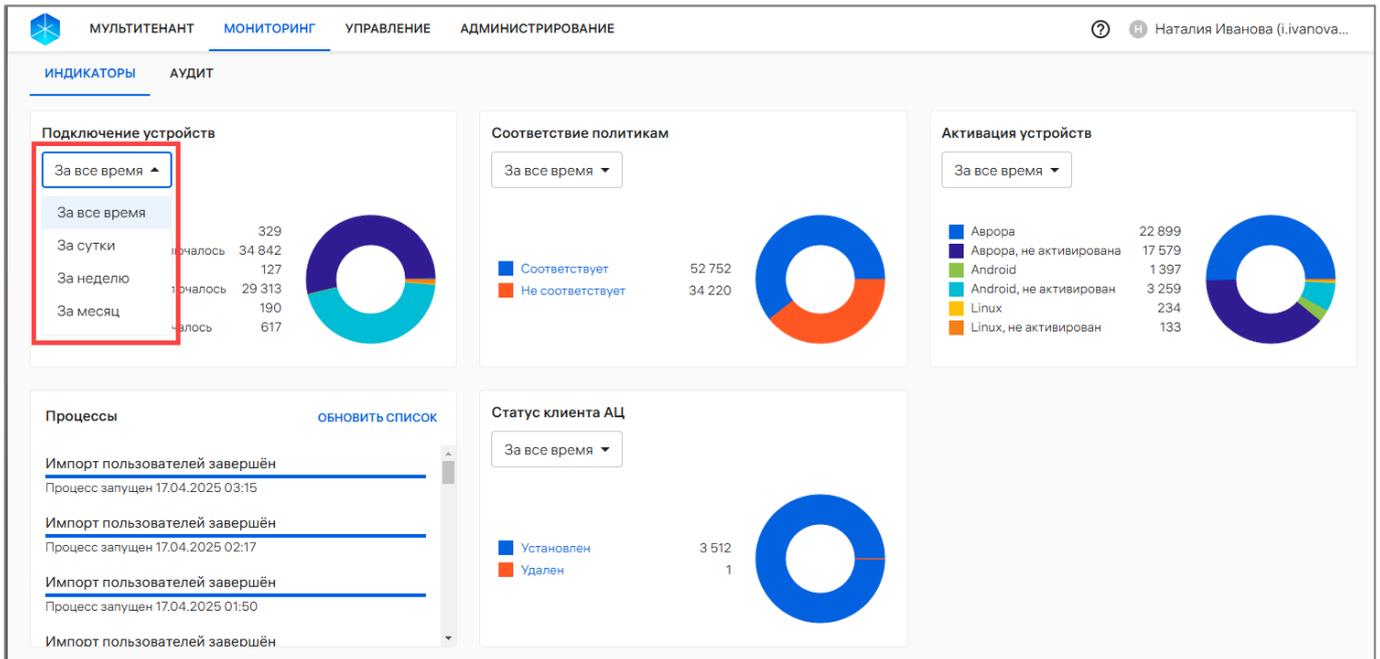


Рисунок 212

В подразделе «Индикаторы» предусмотрена возможность просмотра подключений и активаций устройств для определенной платформы, а также соответствие политикам по следующим показателям:

– «Подключение устройств»:

- «Аврора» - количество подключений устройств с ОС Аврора;
- «Аврора, не подключалось» - количество устройств с ОС Аврора, которые добавлены в ППО, но еще не подключались к нему;
- «Android» - количество подключений устройств с ОС Android;
- «Android, не подключалось» - количество устройств с ОС Android, которые добавлены в ППО, но еще не подключались к нему;
- «Linux» - количество подключений устройств с ОС семейства Linux;
- «Linux, не подключалось» - количество устройств с ОС семейства Linux, которые добавлены в ППО, но еще не подключались к нему;

– «Соответствие политикам»:

- «Соответствует» - количество устройств, соответствующих политикам. Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу политик «Соответствует»;
- «Не соответствует» - количество устройств, не соответствующих политикам. Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу политик «Не соответствует».

ПРИМЕЧАНИЕ. В список устройств попадут не только активированные устройства, у которых целевое значение не совпадает с текущим, но и устройства в статусах «Зарегистрировано» и «В процессе активации», на которые назначена политика;

АДМГ.20134-01 90 01-3

– «Активация устройств»:

- «Аврора» - количество активаций устройств с ОС Аврора;
- «Аврора, не активирована» - количество устройств с ОС Аврора, которые добавлены в ППО, но не активированы;
- «Android» - количество активаций устройств с ОС Android;
- «Android, не активирован» - количество устройств с ОС Android, которые добавлены в ППО, но не активированы;
- «Linux» - количество активаций устройств с ОС семейства Linux;
- «Linux, не активирован» - количество устройств с ОС семейства Linux, которые добавлены в ППО, но не активированы;

– «Статус клиента АЦ»:

- «Установлен» - количество устройств, на которых было установлено приложение «Аврора Центр». Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу приложения «Аврора Центр» «Установлен»;
- «Удален» - количество устройств, на которых было удалено приложение «Аврора Центр» (данная информация доступна только для устройств с ОС семейства Linux). Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу приложения «Аврора Центр» «Удален».

В окне «Процессы» отображаются завершенные и текущие процессы импорта устройств, пользователей и их групп из CSV-файла. Возможны следующие статусы выполнения задач с запущенным импортом:

- завершен (импорт завершен успешно);
- в процессе (импорт/фоновый процесс выполняется);
- прервался (импорт прервался по какой-либо причине, например, если сервис недоступен).

Статус задачи не зависит от результата выполнения импорта, например, статус может быть завершен, но при этом загружен ошибочный файл.

Для просмотра состояния или результата импорта, необходимо нажать на интересующий процесс. В результате отобразится окно с информацией о состоянии импорта, если он еще выполняется, или с результатом импорта, если он завершен (даже с ошибкой) (см. Рисунок 57, Рисунок 58).

4. РАБОТА В РАЗДЕЛЕ «АДМИНИСТРИРОВАНИЕ» КОНСОЛИ АДМИНИСТРАТОРА ПУ

4.1. Подраздел «Настройки»

Подраздел «Настройки» Консоли администратора ПУ предназначен для:

- управления доверенными корневыми сертификатами на устройствах (п. 4.1.1, Рисунок 213 [1]);
- добавления и просмотра категорий пользовательских сертификатов (п. 4.1.2, Рисунок 213 [2]);
- управления отображением архивных устройств, настройки отображения списка устройств (пп. 4.1.3.1, Рисунок 213 [3]), а также согласования файлов (пп. 4.1.3.2, Рисунок 213 [4]);
- просмотра информации о (Рисунок 213 [5]):
 - Сервере приложений (также представлена возможность включения/отключения витрин с приложением) (пп. 4.1.4.1);
 - Обновлении ОС (пп. 4.1.4.2);
 - Сервере LDAP (также представлена возможность добавления интеграции с сервером LDAP и настройки синхронизации данных с ППО) (пп. 4.1.4.3);
 - Сервисе уведомлений Аврора (СУА) (также представлена возможность изменения настроек ПСУ) (пп. 4.1.4.4);
 - Центрах сертификации (пп. 4.1.4.5);
 - Git-репозитории (интеграция с удаленным Git-репозиторием) (п. 4.1.4.6);
- просмотра и добавления территории на карте (п. 4.1.5, Рисунок 213 [6]);
- настройки правил политик (п. 4.1.6, Рисунок 213 [7]);
- добавления и удаления доверенных сетей (п. 4.1.7, Рисунок 213 [8]);
- просмотра и настройки управляемых переменных (п. 4.1.8, Рисунок 213 [9]).

Для перехода в подраздел необходимо в верхней панели перейти в раздел «Администрирование» и выбрать подраздел «Настройки».

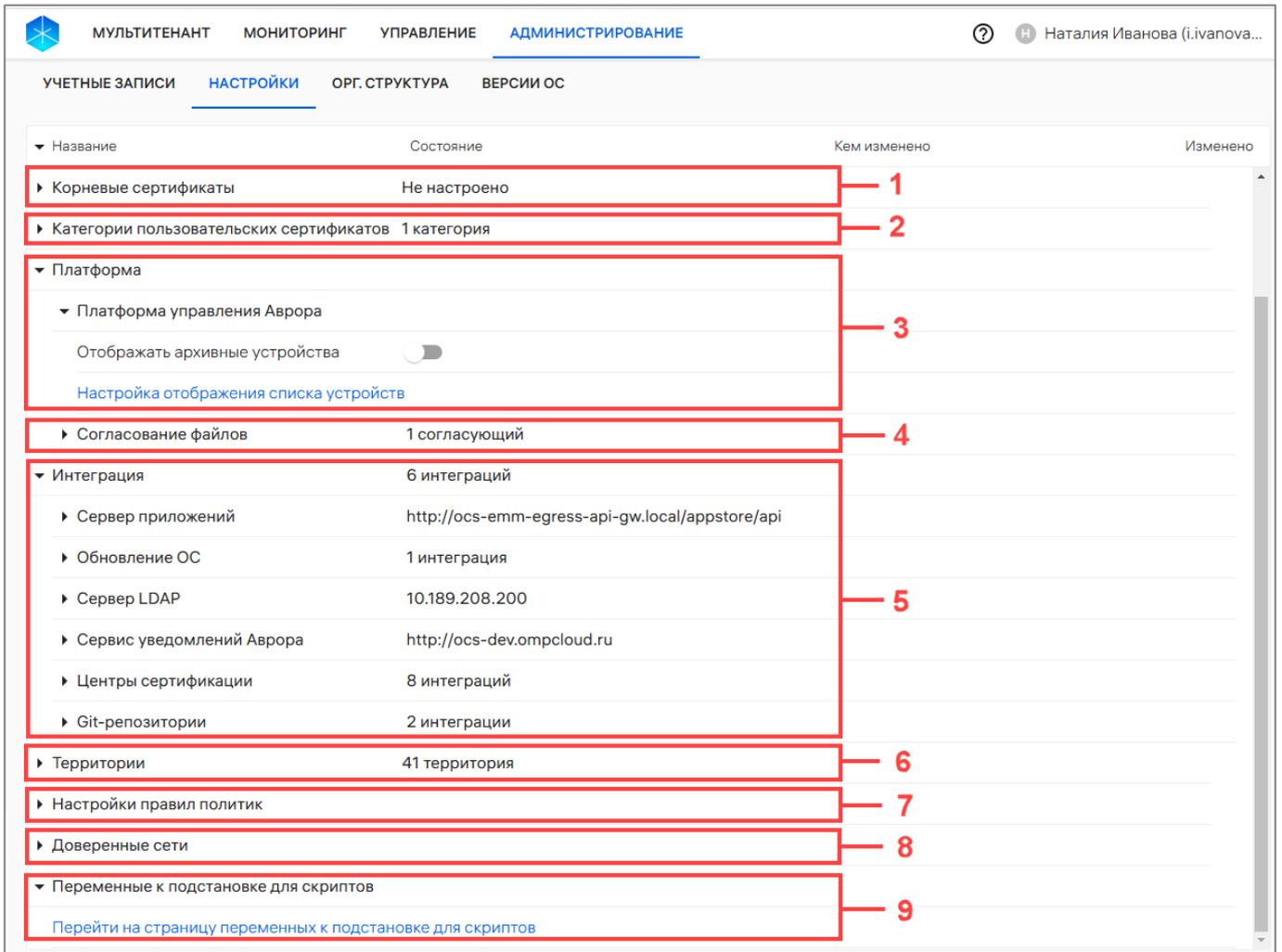


Рисунок 213

4.1.1. Доверенные сертификаты

В раскрывающейся строке «Корневые сертификаты» при нажатии на значок  (см. Рисунок 213 [1]) отображается список доверенных сертификатов, добавленных в ПУ (Рисунок 214 [2]).

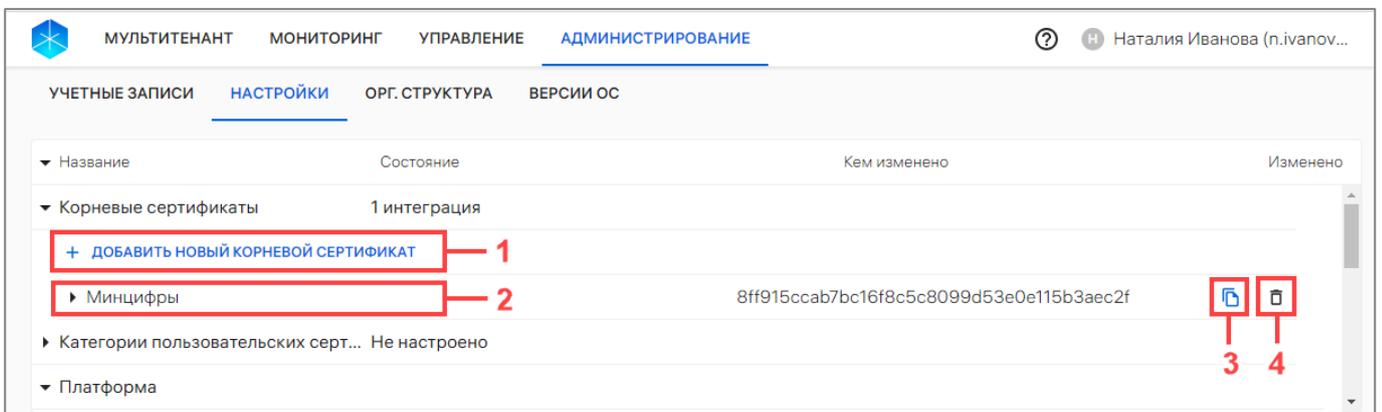


Рисунок 214

АДМГ.20134-01 90 01-3

Для просмотра информации о доверенном сертификате необходимо в раскрывающейся строке названия сертификата нажать значок , в результате чего отобразится следующая информация (Рисунок 215):

- название удостоверяющего центра;
- дата выпуска сертификата;
- срок действия сертификата;
- используется ли сертификат при активации и самостоятельной регистрации устройства.

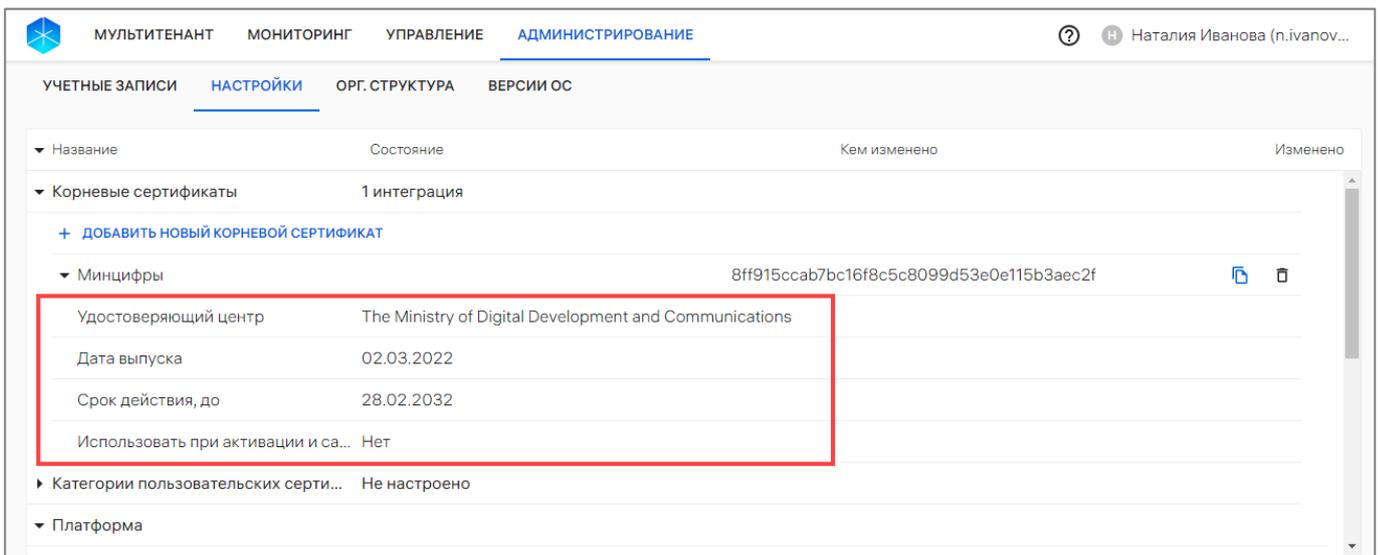


Рисунок 215

Для добавления корневых сертификатов необходимо выполнить следующие действия:

- нажать кнопку «Добавить новый корневой сертификат» (см. Рисунок 214 [1]);
- в открывшемся окне в поле «Имя корневого сертификата» ввести название сертификата (Рисунок 216 [1]). Максимальная длина – 32 символа;
- перевести переключатель «Использовать при активации и саморегистрации» в положение «Включено» (Рисунок 216 [2]), если при помощи данного сертификата требуется пройти процесс активации (например, в закрытом контуре Аврора Центр).

ПРИМЕЧАНИЕ. Возможно добавление не более 3 сертификатов;

- нажать кнопку «Загрузить файл» (Рисунок 216 [3]) для последующего выбора файла для загрузки. Допустимые форматы: .crt, .cer, .pem;
- подтвердить либо отменить действия (Рисунок 216 [4]).

При успешном добавлении сертификат отобразится в списке доверенных сертификатов.

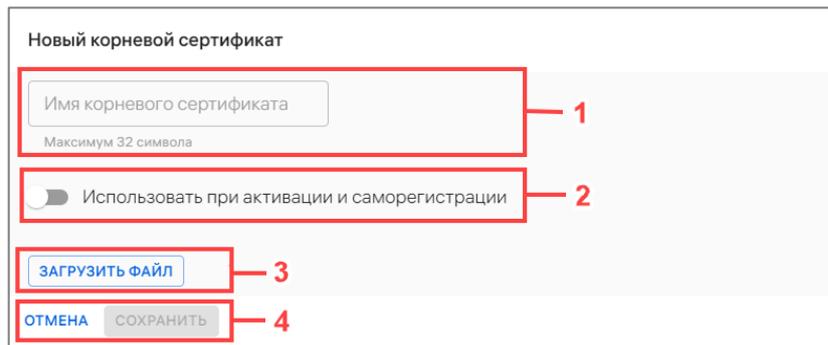


Рисунок 216

При необходимости цифровой отпечаток (Fingerprint) сертификата возможно скопировать в буфер обмена нажатием значка  «Копировать в буфер обмена» (см. Рисунок 214 [3]) в строке с сертификатом.

Для удаления корневых сертификатов необходимо нажать значок  «Удалить сертификат» в строке сертификатов (см. Рисунок 214 [4]) и в открывшемся окне подтвердить либо отменить действие.

ПРИМЕЧАНИЕ. При следующем подключении устройства к Серверу приложений ПУ добавленные сертификаты будут установлены на устройстве, а удаленные сертификаты будут удалены с устройства.

4.1.2. Категории пользовательских сертификатов

Категории пользовательских сертификатов используются для выпуска разных типов сертификатов для разных подключений определенному пользователю.

ПРИМЕЧАНИЕ. Чтобы доставить на устройство сертификат созданной категории, необходимо привязать устройство к пользователю и назначить на группу, в которую входит устройство, политику с одним из правил:

- «Настройки пользователя/Сертификаты пользователя» (пп. 2.4.1.36);
- «Конфигурация WLAN/Подключения к сети WLAN» (пп. 2.4.1.19).

Список созданных категорий возможно посмотреть в раскрывающейся строке «Категории пользовательских сертификатов» при нажатии значка  (см. Рисунок 213 [2]).

Для добавления категории пользовательских сертификатов необходимо выполнить следующие действия:

- нажать кнопку «Добавить категорию» (Рисунок 217);

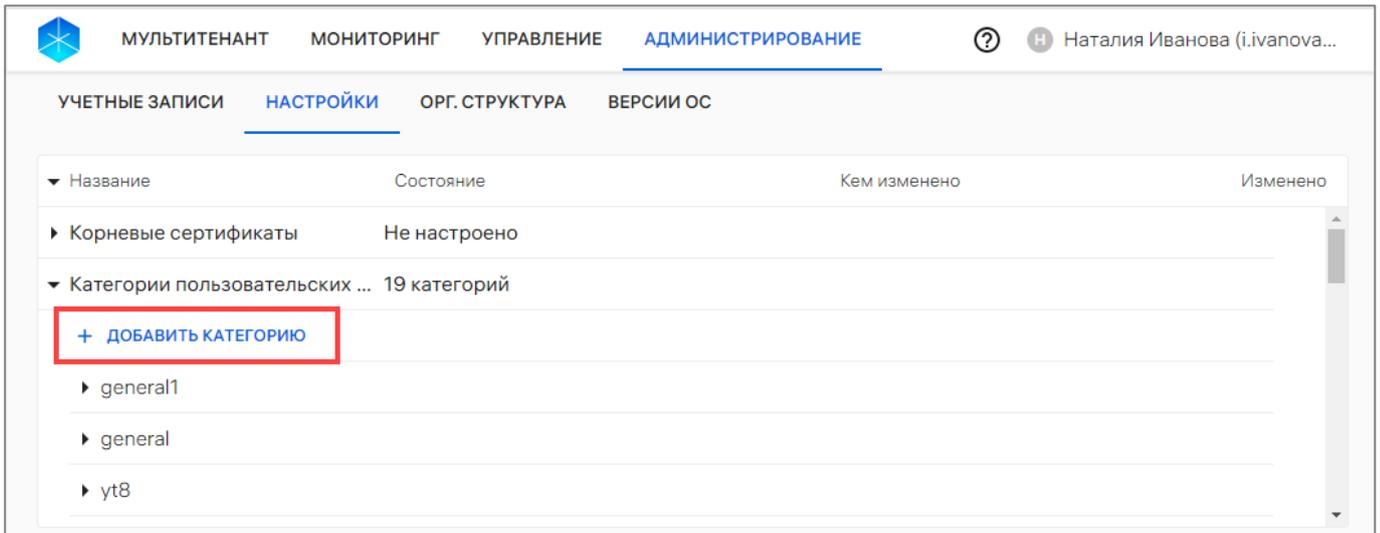


Рисунок 217

– в открывшемся окне (Рисунок 218) заполнить поля, приведенные в таблице (Таблица 46);

– сохранить изменения либо отменить действия.

При успешном сохранении категория пользовательских сертификатов будет добавлена.

ВНИМАНИЕ! Удаление и редактирование категории сертификата недоступно. При необходимости доступно создать новую категорию пользовательских сертификатов.

Категория пользовательских сертификатов

Название категории

Центр сертификации

Название шаблона

Subject

Значение шаблона {{...}} подставится автоматически из атрибутов пользователя устройства.

Key Value

ДОБАВИТЬ

Subject alt name

email:{{UserEmail}},otherName:Microsoft User Principal Name,UTF8:{{UserPrincipalName}}

Тип шифрования и длина ключа Хэш-алгоритм запроса

ОТМЕНА **СОХРАНИТЬ**

Рисунок 218

Таблица 46

Параметр		Описание
Название категории		Ввод значения с клавиатуры. Может содержать только строчные буквы и дефис, максимальное количество символов – 50. Поле обязательно для заполнения
Центр сертификации		Выбор значения из раскрывающегося списка «Центр сертификации». При отсутствии необходимого центра сертификации в списке требуется добавить его (п. 4.1.3.2). Поле обязательно для заполнения
Название шаблона		Ввод значения с клавиатуры. Может содержать 255 символов. Поле обязательно для заполнения
Subject	key	Ввод значения с клавиатуры. Может содержать 255 символов. Поле обязательно для заполнения. ПРИМЕЧАНИЕ. При отсутствии ключа для сертификата необходимо обратиться к администратору службы сертификатов Active Directory. Для добавления дополнительного субъекта для сертификата необходимо нажать кнопку «Добавить»
	value	Доступен ввод значения с клавиатуры (может содержать 255 символов) или выбор из раскрывающегося списка динамических переменных, которые будут автоматически подставлять в сертификат атрибуты пользователя: – {{UserEmail}} – Email из карточки пользователя; – {{UserPrincipalName}} – логин (значение параметра userPrincipalName из LDAP-данных о пользователе); – {{sAMAccountName}} – логин (значение параметра sAMAccountName из LDAP-данных о пользователе); – {{distinguishedName}} – значение параметра distinguishedName из LDAP-данных о пользователе. Если Администратор Платформы управления не знает значение субъекта для сертификата, необходимо обратиться к администратору службы сертификатов Active Directory. Поле обязательно для заполнения. ВНИМАНИЕ! Ввод других динамических переменных недоступен. ПРИМЕЧАНИЕ. Для ключа C (country) значение должно состоять из 2 символов (например, RU). Для добавления дополнительного субъекта для сертификата необходимо нажать кнопку «Добавить»

Параметр	Описание
Subject alt name	<p>При необходимости доступен ввод дополнительных имен субъекта для сертификата. Каждое имя субъекта должно состоять из набора параметров – названия параметра (<i>key</i>) и его значения (<i>value</i>). Может содержать 1000 символов. Доступен ввод динамических переменных, которые будут автоматически подставляться в сертификат атрибуты пользователя:</p> <ul style="list-style-type: none"> – {{UserEmail}} – Email из карточки пользователя; – {{UserPrincipalName}} – логин (значение параметра <i>userPrincipalName</i> из LDAP-данных о пользователе); – {{sAMAccountName}} – логин (значение параметра <i>sAMAccountName</i> из LDAP-данных о пользователе); – {{distinguishedName}} – значение параметра <i>distinguishedName</i> из LDAP-данных о пользователе. <p>ВНИМАНИЕ! Ввод других динамических переменных недоступен.</p> <p>Пример заполнения Subject alt name: email:{{UserEmail}},otherName:Microsoft User Principal Name;UTF8:{{UserPrincipalName}}</p>

4.1.3. Платформа

В раскрывающейся строке «Платформа» доступно:

- управление отображением архивных устройств и настройка отображения списка устройств (пп. 4.1.3.1);
- согласование файлов (пп. 4.1.3.2).

4.1.3.1. Отображение архивных устройств и настройка отображения списка устройств

Для активации отображения архивных устройств (см. Рисунок 213 [3]) необходимо перевести переключатель в положение «Включено» . В результате в подразделе «Устройства» раздела «Управление» в списке устройств будут отображаться архивные устройства (Рисунок 219).

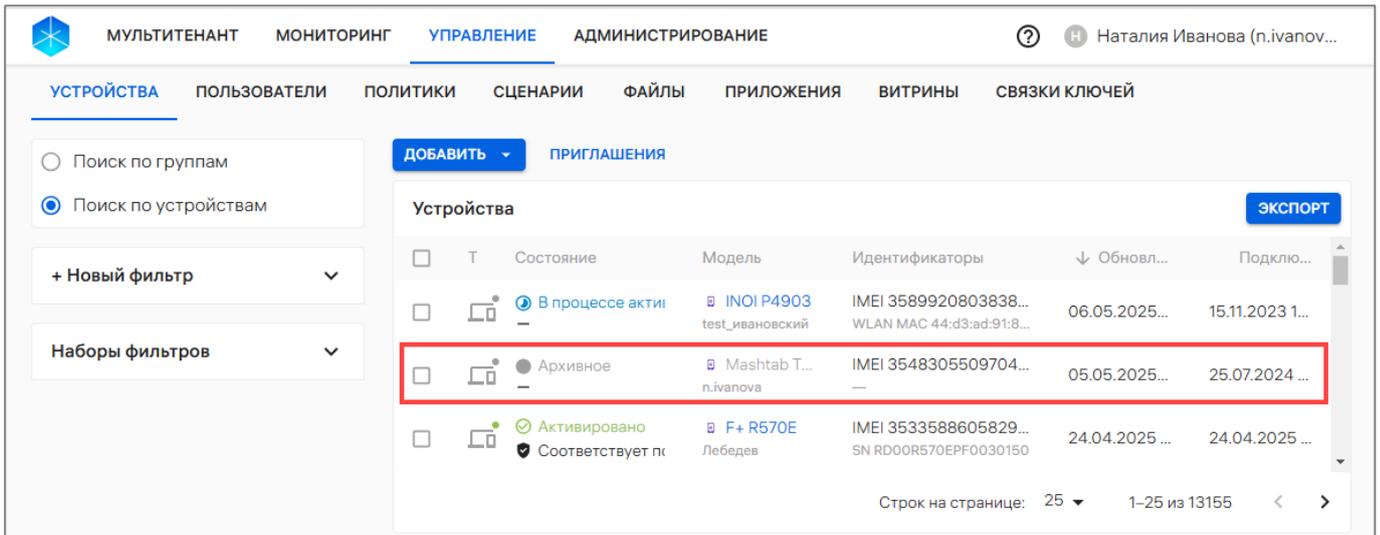


Рисунок 219

Для настройки отображения списка устройств необходимо нажать на одноименную кнопку. В результате откроется окно, где требуется выбрать платформу (ОС Аврора, ОС Android или ОС Linux (Рисунок 220 [2]) и расположить идентификаторы устройства в порядке уменьшения их значимости (Рисунок 220 [1]) и далее нажать кнопку «Сохранить».

В результате порядок отображения идентификаторов устройства в списке устройств будет изменен.

Первый и второй идентификаторы будут отображаться в списке устройств как основной и дополнительный, при их отсутствии будут отображаться менее приоритетные идентификаторы (третий, четвертый и т.д.).

ВНИМАНИЕ! Если очистить localStorage браузера, то настройки отображения идентификаторов примут значения по умолчанию.

МУЛЬТИТЕНАНТ МОНИТОРИНГ УПРАВЛЕНИЕ **АДМИНИСТРИРОВАНИЕ** ? Н Наталия Иванова (i.ivanova)

УЧЕТНЫЕ ЗАПИСИ **НАСТРОЙКИ** ОРГ. СТРУКТУРА ВЕРСИИ ОС

< Настройка отображения списка устройств

Расположите идентификаторы устройства в порядке уменьшения их значимости.
1-ый и 2-ой идентификаторы будут отображаться в списке устройств как основной и дополнительный, при их отсутствии будут отображаться менее приоритетные идентификаторы (3-ий, 4-ый и т.д.)

ОС Аврора ^

1 IMEI

2 Серийный номер

3 WLAN MAC

4 Ethernet MAC — 1

5 Сетевое имя устройства

6 IP адрес устройства

7 Имя устройства

ОС Android v

ОС Linux v

СОХРАНИТЬ

Рисунок 220

По умолчанию идентификаторы устройства в списке устройств отображаются согласно следующим приоритетам:

– ОС Аврора, ОС Android:

- IMEI;
- Серийный номер;
- WLAN MAC;
- Ethernet MAC;
- Сетевое имя;
- IP;
- Имя устройства;

– ОС семейства Linux:

- Сетевое имя;
- Ethernet MAC;
- IP;

- IMEI;
- WLAN MAC;
- Серийный номер;
- Имя устройства.

4.1.3.2. Согласование файла

Для повышения безопасности в ППО реализована возможность согласования файлов, загружаемых в ПУ, администраторами. Если файл не был согласован или согласован меньшим количеством администраторов, чем задано в настройках ППО, то данный файл недоступен для выбора в политике распространения файлов или скриптов.

Чтобы установить количество администраторов для согласования загружаемых файлов, необходимо в раскрывающейся строке «Согласование файлов» в поле «Количество согласующих администраторов» ввести нужное количество администраторов для согласования файлов и нажать на «Подтвердить» (Рисунок 221).

В результате успешного подтверждения количество согласующих администраторов будет установлено.

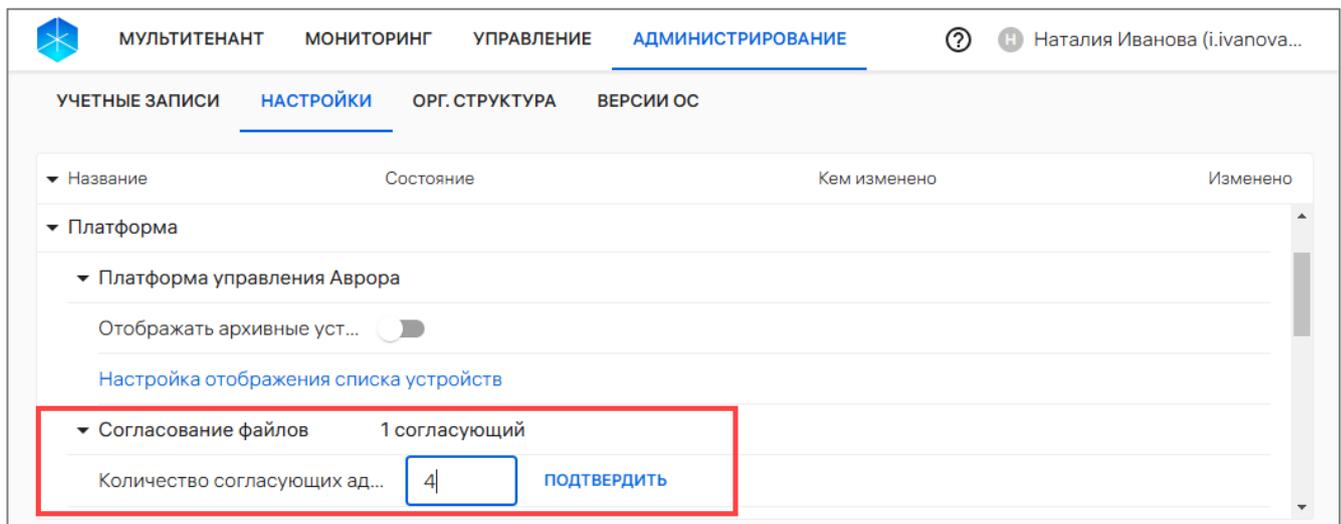


Рисунок 221

4.1.4. Интеграция (информация о серверах)

Для просмотра детальной информации о серверах необходимо в раскрывающейся строке «Интеграция» нажать значок  напротив выбранной вкладки.

4.1.4.1. Сервер приложений

Сервер приложений – адрес Сервера приложений ПМ (Рисунок 222 [1]) и список опубликованных витрин на Сервере приложений ПМ (Рисунок 222 [2]).

Переключатель  позволяет включать или отключать витрину. После отключения витрина становится недоступной в списке выбора витрины при создании правила «Приложения/Установка приложений на устройство» в политике.

ПРИМЕЧАНИЕ. В случае, если приложения на устройствах установлены с помощью политики, они не будут удалены с устройств после отключения витрины.

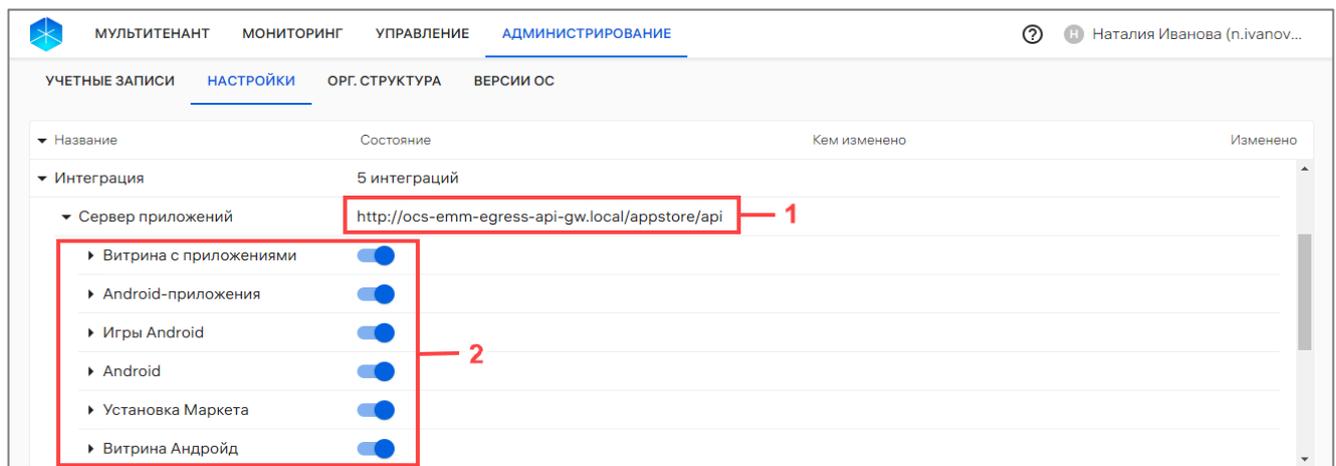


Рисунок 222

Для просмотра детальной информации о витринах во вложенных строках, которые доступны созданному тенанту, следует нажать значок .

Список опубликованных приложений формируется в ПМ. При отсутствии на сервере опубликованных приложений отображается сообщение «Нет приложений, доступных для назначения».

Если необходимой витрины нет в списке, требуется добавить ее и/или выдать доступ к витрине (параметр «Подключаемые Платформы управления» в настройках витрины).

ПРИМЕЧАНИЕ. Процессы добавления и редактирования витрины приведены в документе «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2».

4.1.4.2. Обновление ОС

Обновление ОС – адрес сервера обновления ОС.

Для просмотра версий ОС необходимо нажать значок  в строке «Обновление ОС».

4.1.4.3. Сервер LDAP

Сервер LDAP – адрес сервера LDAP. Во вкладке «Сервер LDAP» предусмотрена возможность посмотреть дату начала и статус синхронизации данных, а также возможность управлять интеграцией с сервером LDAP (добавлять, редактировать и удалять интеграцию).

4.1.4.3.1. Добавление интеграции с LDAP-сервером

Для синхронизации устройств, пользователей и групп с ПУ предусмотрена возможность добавления интеграции ПУ с LDAP-сервером Microsoft Active Directory. Синхронизация является односторонней – данные из ПУ не будут переноситься на LDAP-сервер.

ПРИМЕЧАНИЯ:

- ✓ ПУ протестирован с интеграцией с центрами сертификации, имеющими тип сервера Microsoft Active Directory Certificate Services (AD CS) в Windows Server 2019;
- ✓ Предусматривается возможность добавления интеграции с LDAP-сервером для каждого тенанта;
- ✓ ПУ поддерживает синхронизацию с LDAP-серверами, в которых устройства, пользователи и группы безопасности хранятся в одном или разных организационных юнитах (Organizational Unit);
- ✓ Категории пользовательских сертификатов и Microsoft Active Directory должны использовать один и тот же центр сертификации AD CS.

Для добавления интеграции ПУ с LDAP-сервером необходимо:

- выполнить подключение ПУ к LDAP-серверу (пп. 4.1.4.3.1.1);
- если требуется синхронизировать:
 - пользователей и их группы, настроить интеграцию пользователей (пп. 4.1.4.3.1.2);
 - устройства и их группы, настроить интеграцию устройств (п. 4.1.4.3.1.3).

4.1.4.3.1.1. Подключение ПУ к LDAP-серверу

Для выполнения подключения ПУ к LDAP-серверу необходимо:

- во вложенном списке «Интеграция» нажать «Настроить» (Рисунок 223);

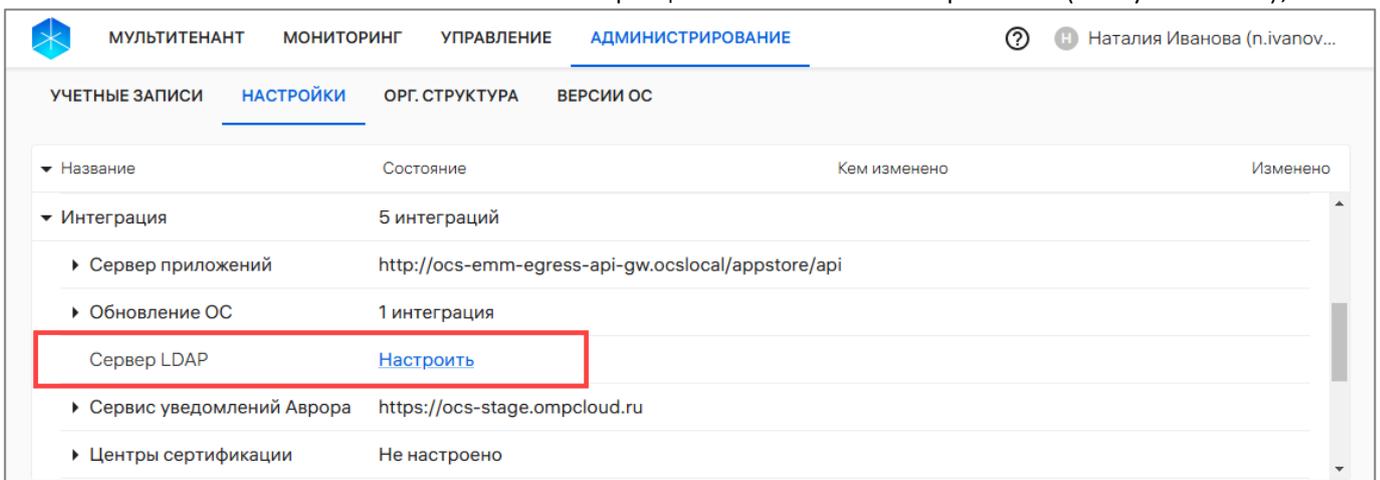


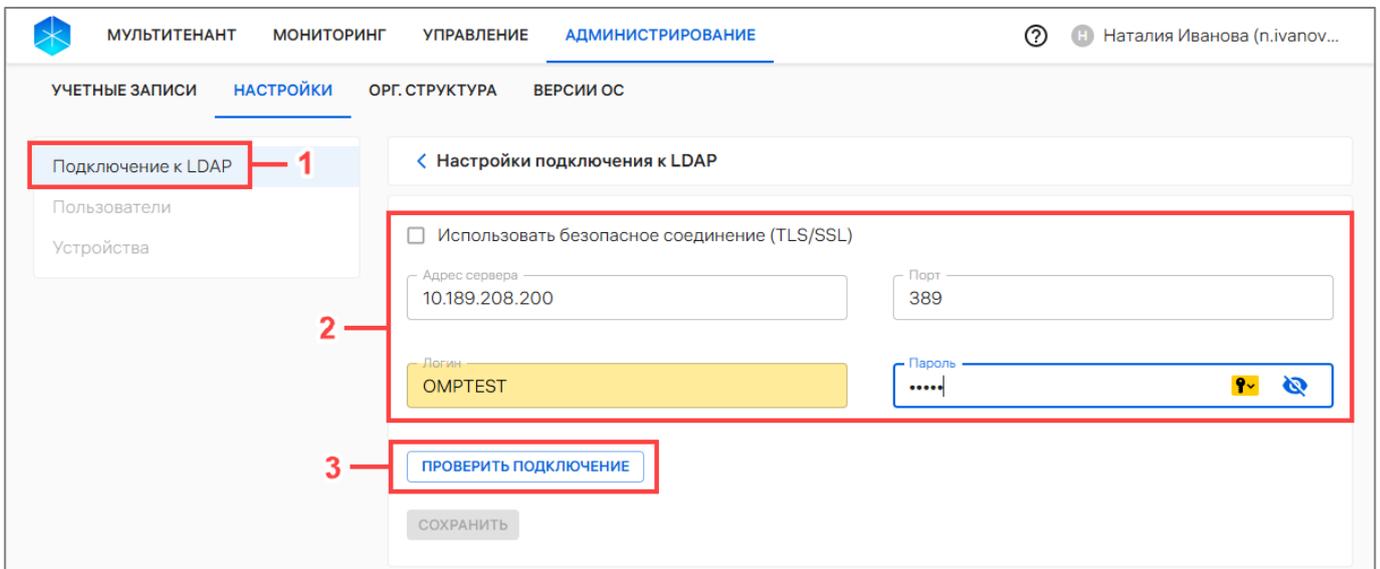
Рисунок 223

- в области фильтров во вкладке «Подключение к LDAP» (Рисунок 224 [1]) задать настройки для подключения к LDAP-серверу (Рисунок 224 [2]) согласно таблице (Таблица 47) и далее для проверки работоспособности подключения к LDAP-серверу с заданными настройками нажать кнопку «Проверить подключение» (Рисунок 224 [3]).

Таблица 47

Поле	Описание
Использовать безопасное	Если необходимо использовать защищенное подключение к LDAP-серверу (с помощью SSL версии протокола LDAP – LDAPS), следует установить галочку в чекбоксе.

Поле	Описание
соединение (TLS/SSL)	По умолчанию галочка в чекбоксе не установлена (используется версия протокола без SSL – LDAP)
Адрес сервера	Ввести адрес LDAP-сервера
Порт	В поле задано значение по умолчанию: – 389 , если в чекбоксе не установлена галочка «Использовать безопасное соединение (TLS/SSL)»; – 636 , если в чекбоксе установлена галочка «Использовать безопасное соединение (TLS/SSL)». ПРИМЕЧАНИЕ. При необходимости можно ввести другой номер порта для подключения к LDAP-серверу
Логин	Ввести логин для подключения к LDAP-серверу в одном из форматов: – логин без домена, например: «Admin»; – логин с доменом, например: «OMP/Admin»; – логин в виде E-mail, например: «Admin@omp.ru»
Пароль	Ввести пароль для подключения к LDAP-серверу. Для просмотра/скрытия пароля необходимо использовать значок  . После сохранения настроек просмотреть пароль будет невозможно



Мультитенант МОНИТОРИНГ УПРАВЛЕНИЕ АДМИНИСТРИРОВАНИЕ ? Наталия Иванова (n.ivanov...)

УЧЕТНЫЕ ЗАПИСИ **НАСТРОЙКИ** ОРГ. СТРУКТУРА ВЕРСИИ ОС

Подключение к LDAP — 1

Пользователи
Устройства

< Настройки подключения к LDAP

Использовать безопасное соединение (TLS/SSL)

Адрес сервера: 10.189.208.200 Порт: 389

Логин: OMPTEST Пароль: 

ПРОВЕРИТЬ ПОДКЛЮЧЕНИЕ СОХРАНИТЬ

Рисунок 224

В случае успешной проверки отобразится сообщение «Подключение доступно» (Рисунок 225).

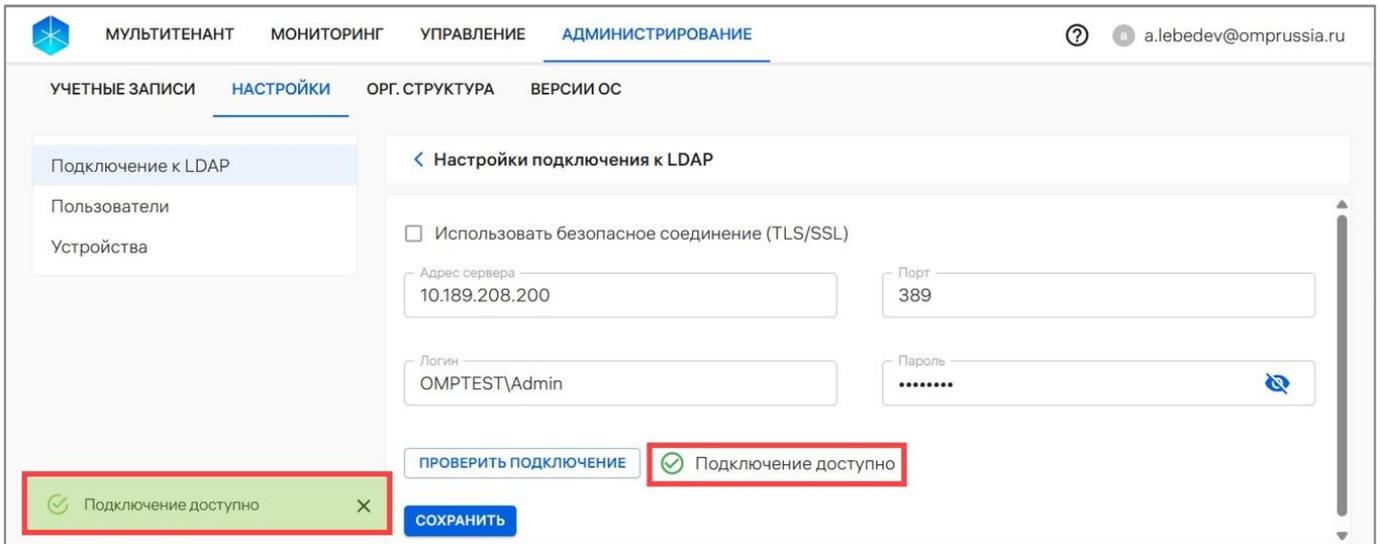


Рисунок 225

В случае неудачного завершения проверки отобразится сообщение об ошибке (Рисунок 226[1]), которую необходимо устранить и повторить проверку или обратиться к системному администратору/администратору LDAP. После успешной проверки подключения нажать «Сохранить».

ПРИМЕЧАНИЕ. Для ознакомления с полным текстом ошибки следует нажать «Подробнее» (Рисунок 226 [2]).

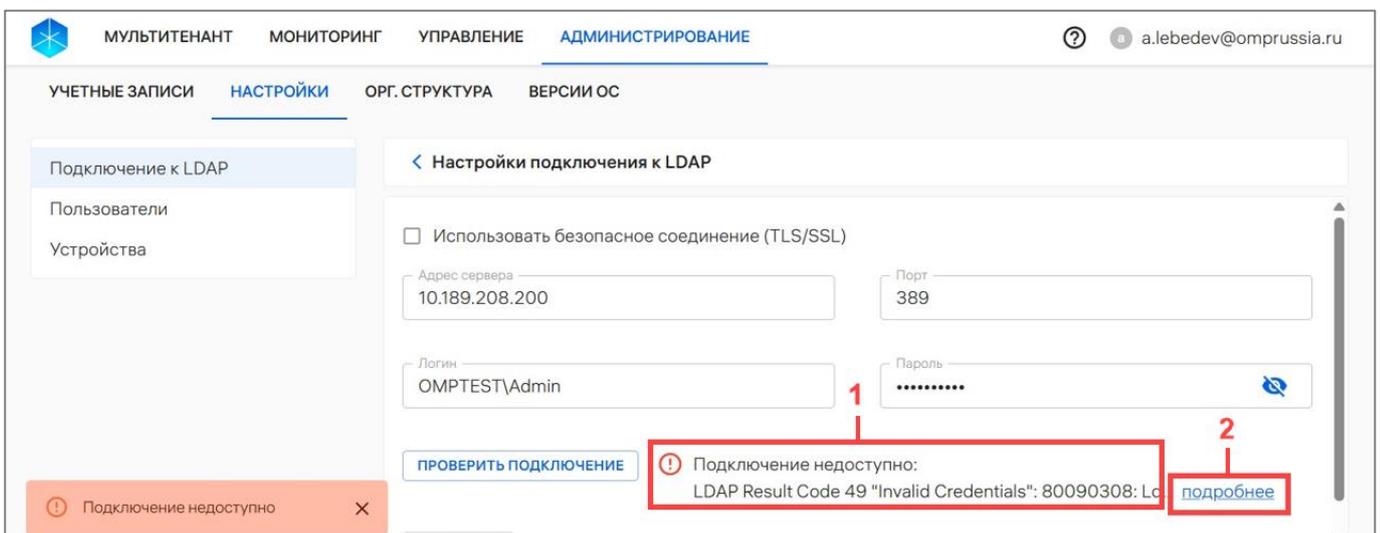


Рисунок 226

4.1.4.3.1.2. Синхронизация пользователей и их групп

Для синхронизации пользователей и их групп необходимо в области фильтров во вкладке «Пользователи» (Рисунок 227 [1]) задать настройки для интеграции пользователей согласно таблице (Таблица 48, Рисунок 227 [2]), данные из которой будут синхронизироваться с ППО.

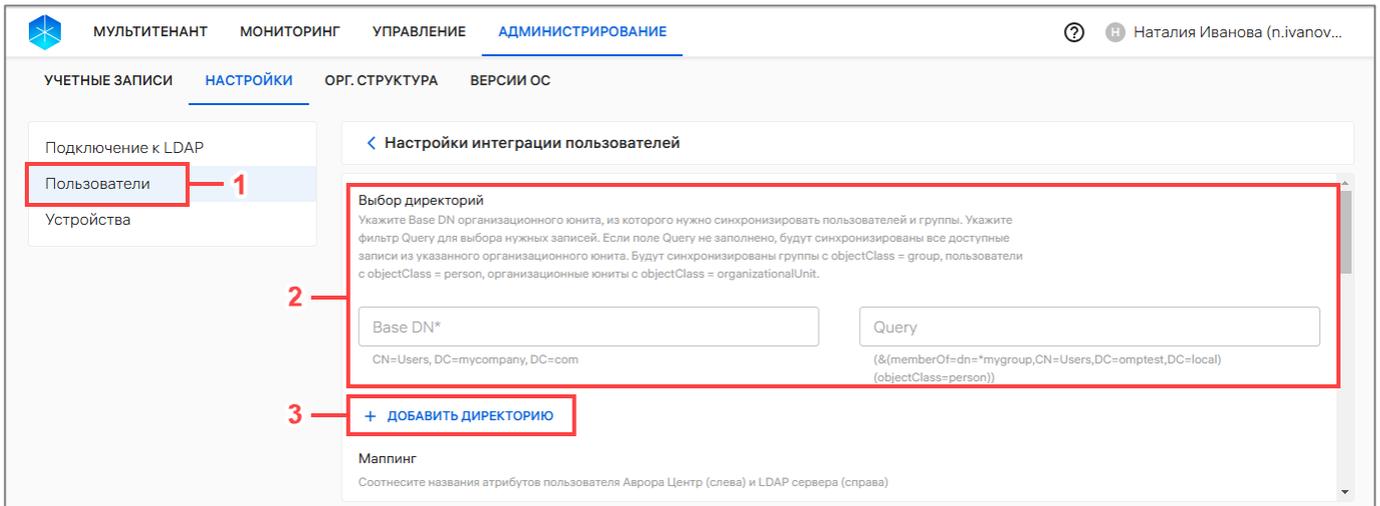


Рисунок 227

Таблица 48

Поле	Описание
Base DN	Поле обязательно для заполнения. Максимально 1000 символов. Если группы безопасности и пользователи хранятся: – в одном организационном юните, то в поле «Base DN» необходимо ввести этот юнит; – в разных организационных юнитах, то в поле «Base DN» ввести все организационные юниты, данные из которых необходимо синхронизировать. Например: CN=Users, DC=mycompany, DC=com.
Query	Поле необязательно для заполнения. При необходимости в поле «Query» ввести фильтр для выбора нужных записей из организационных юнитов. Максимальное количество символов 10000. Фильтр будет применяться ко всем записям внутри организационных юнитов, введенных в поле «Base DN»

ПРИМЕЧАНИЕ. В результате будут синхронизированы все доступные записи из указанных организационных юнитов (группы с `objectClass = group`, пользователи с `objectClass = person`, организационные юниты с `objectClass = organizationalUnit`). Если `objectClass` для пользователей, групп и организационных юнитов на LDAP-сервере отличаются от указанных выше, следует изменить их в конфигурационном файле ППО.

Рекомендации по использованию фильтров:

1) Если для выбора необходимых пользователей и/или групп из юнита требуется задать несколько фильтров, то следует добавить еще одну директорию (как указано ниже), затем в каждой строке ввести одинаковый «Base DN» и задать нужный фильтр;

2) Если требуется синхронизировать в ПУ уволенных сотрудников, следует указать организационный юнит, в котором они хранятся, или задать фильтры для загрузки таких пользователей;

3) Если не требуется синхронизировать в ПУ уволенных сотрудников, следует задать в фильтрах правило, которое исключит таких сотрудников: если сотрудник имеет статус или параметр, определяющий его неактивность, то необходимо указать это в фильтре. Например: `!(employmentType=NEW)`.

При необходимости возможно добавить еще одну директорию для синхронизации. Для этого нажать кнопку «Добавить директорию» (см. Рисунок 227 [3]) и заполнить для нее поля «Base DN» и «Query» согласно таблице (см. Таблица 48).

По умолчанию в блоке «Маппинг» в разделе «Основные атрибуты» заданы параметры маппинга атрибутов пользователя ППО и LDAP-сервера, основанные на часто используемых значениях в Active Directory. При необходимости следует ввести в поля другие атрибуты пользователя из LDAP-сервера, соответствующие названию полей (Рисунок 228), приведенных в таблице (Таблица 49).

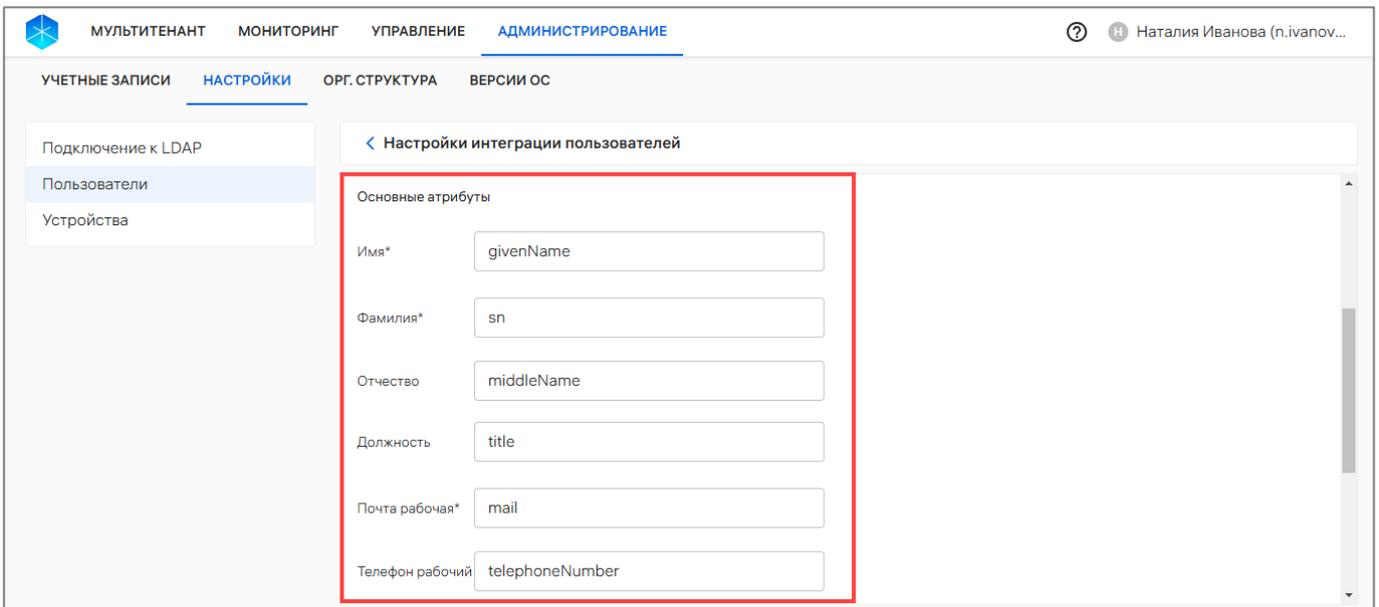


Рисунок 228

Таблица 49

Название поля	Описание
Имя	Поле обязательно для заполнения. Максимально 100 символов
Фамилия	Поле обязательно для заполнения. Максимально 100 символов
Отчество	Поле не обязательно для заполнения. Максимально 100 символов
Должность	Поле не обязательно для заполнения. Максимально 100 символов
Почта рабочая	Поле обязательно для заполнения. Максимально 100 символов
Телефон рабочий	Поле не обязательно для заполнения. Максимально 100 символов

ВНИМАНИЕ! По указанному в маппинге параметру значения должны соответствовать требованиям к данным для пользователей и групп пользователей, содержащимся в Active Directory, которые приведены в таблице (Таблица 50).

Таблица 50

Параметр	Описание	Примечание
Название группы пользователей	Формат: от 2 до 64 символов	Поле обязательно для заполнения
Почта рабочая	Рабочая почта пользователя устройства. Формат: <логин>@<доменное_имя>, от 2 до 256 символов	Поле обязательно для заполнения. Рабочая почта пользователя должна быть уникальной
Имя	Имя пользователя устройства. Формат: от 2 до 64 символов. Символы: а-я; а-z; А-Я; А-Z; -; пробел	Поле обязательно для заполнения
Фамилия	Фамилия пользователя устройства. Формат: от 2 до 64 символов. Символы: а-я; а-z; А-Я; А-Z; -; пробел	Поле обязательно для заполнения
Отчество	Отчество пользователя устройства. Формат: от 2 до 64 символов. Символы: а-я; а-z; А-Я; А-Z; -; пробел	Поле не является обязательным для заполнения
Должность	Должность, занимаемая пользователем устройства. Формат: от 2 до 256 символов. Символы: а-я; а-z; А-Я; А-Z; -; пробел	Поле не является обязательным для заполнения
Телефон рабочий	Номер телефона пользователя устройства. Формат: от 2 до 64 символов. Только цифры	Поле не является обязательным для заполнения

При необходимости в блоке «Маппинг» в разделе «Дополнительные атрибуты» возможно задать до 10 дополнительных атрибутов пользователя для маппинга (Рисунок 229 [1]). Для этого необходимо выбрать нужный атрибут из раскрывающегося списка:

- department – название отдела;
- employeeType – статус работника (работает/уволен);
- Manager – ФИО непосредственного руководителя.

Если необходимого атрибута нет в списке, ввести название атрибута и нажать «Enter» на клавиатуре.

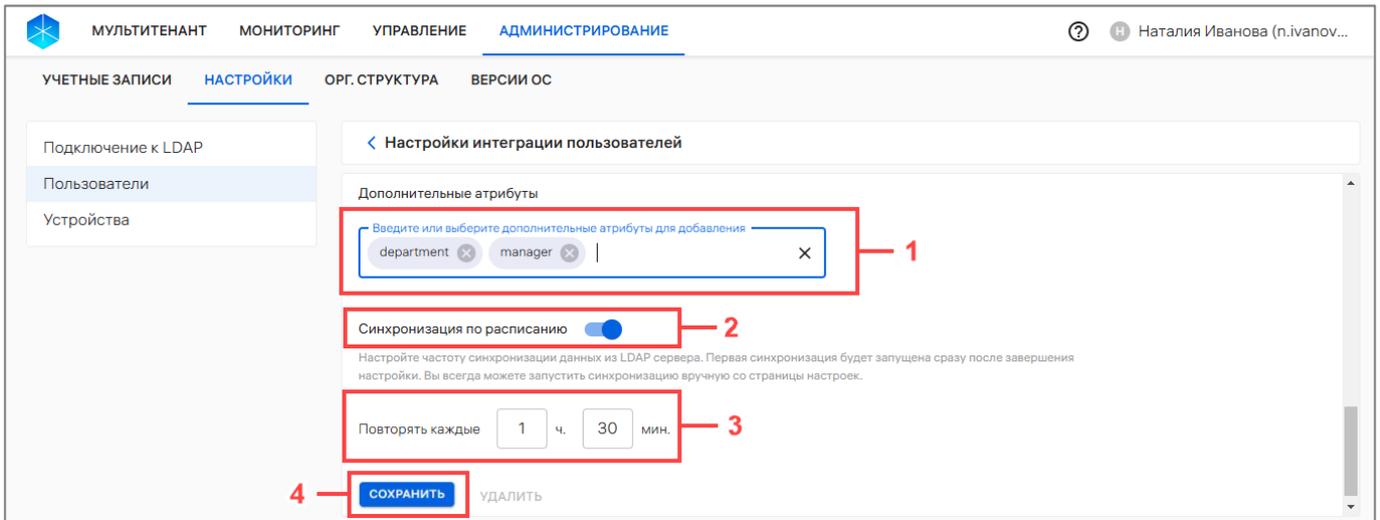


Рисунок 229

ПРИМЕЧАНИЕ. По умолчанию данные из LDAP-сервера будут синхронизироваться каждые 1 час 30 минут.

Если необходимо:

- отключить синхронизацию данных, то следует установить переключатель «Синхронизация по расписанию» в положение «Выключено» (см. Рисунок 229 [2]);
- изменить частоту синхронизации, то следует ввести нужный временной интервал в поле «Повторять каждые» (см. Рисунок 229 [3]).

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных.

Далее нажать «Сохранить» (см. Рисунок 229 [4]).

В результате будет добавлена интеграция пользователей ПУ с LDAP-сервером и запущена первая синхронизация данных.

Для просмотра даты начала синхронизации и ее статуса (Рисунок 230) необходимо нажать значок  в раскрывающейся строке «Сервер LDAP».

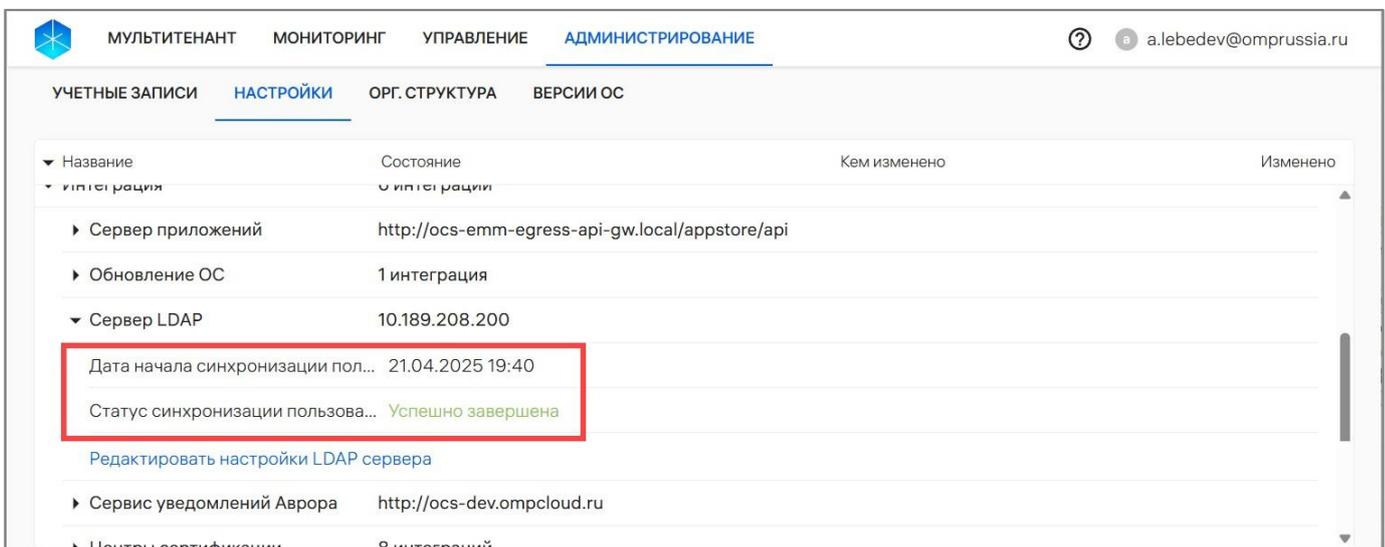


Рисунок 230

В случае ошибки синхронизации данных для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (Рисунок 231).

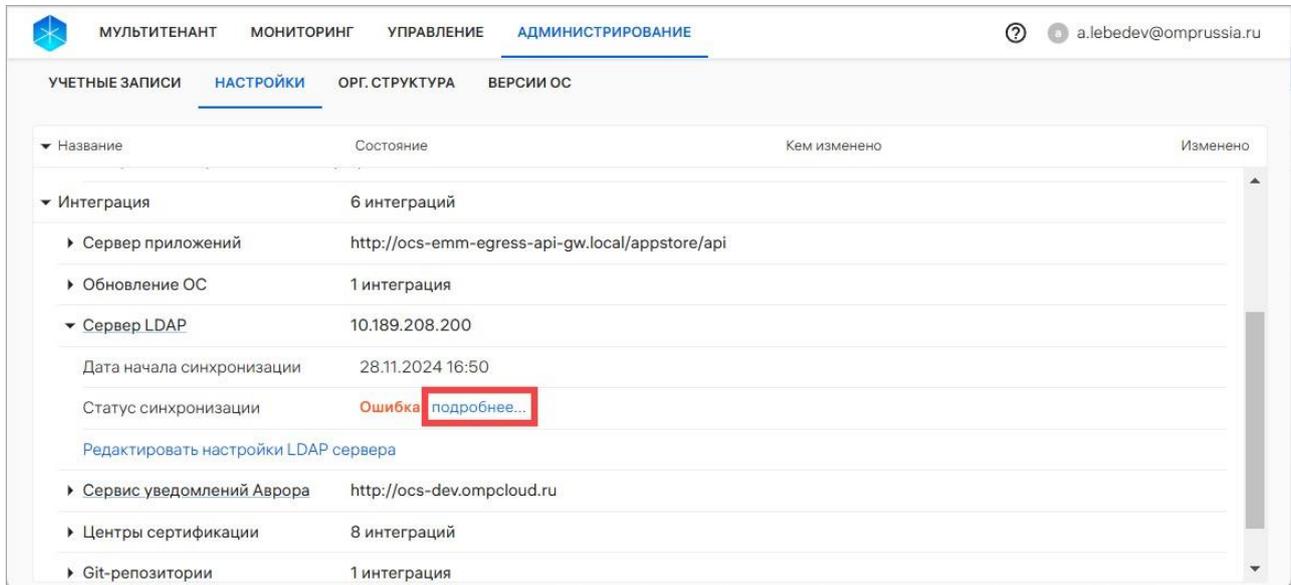


Рисунок 231

4.1.4.3.1.3. Синхронизация устройств и их групп

Для синхронизации устройств и их групп необходимо:

1) В области фильтров во вкладке «Устройства» (Рисунок 232 [1]) задать настройки для интеграции устройств согласно таблице (Таблица 51, Рисунок 232 [2]), данные из которой будут синхронизироваться с ППО;

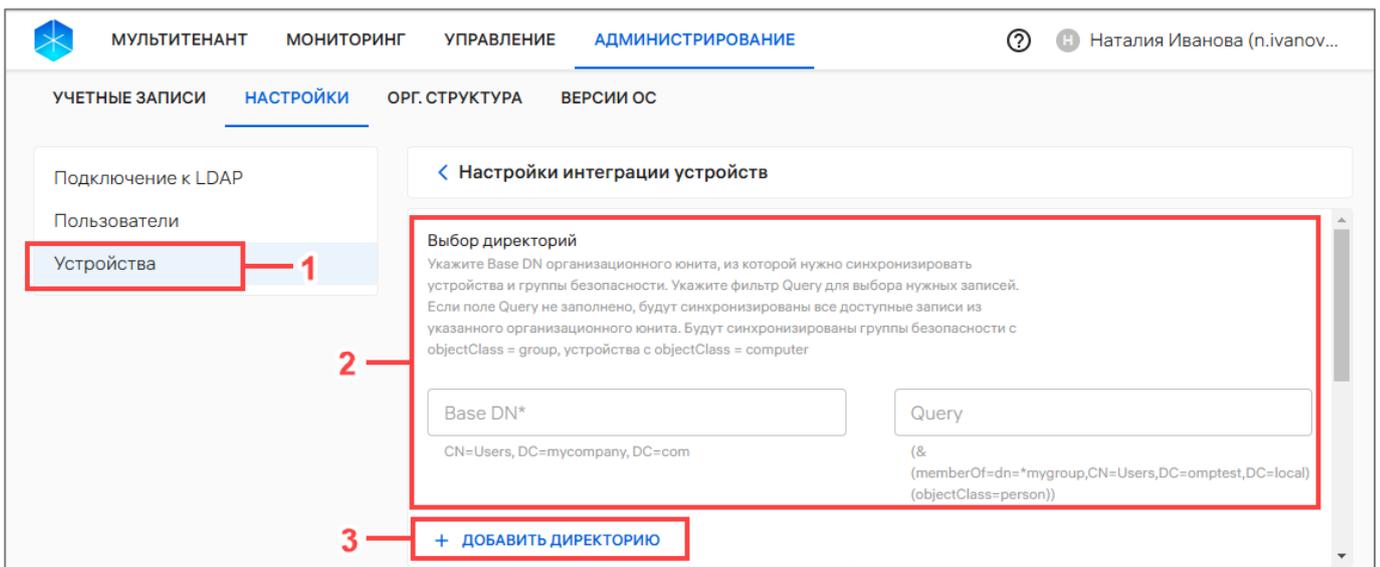


Рисунок 232

Таблица 51

Поле	Описание
Base DN	Поле обязательно для заполнения. Максимально 1000 символов. Если группы безопасности и устройства хранятся: – в одном организационном юните, то в поле «Base DN» необходимо ввести этот юнит; – в разных организационных юнитах, то в поле «Base DN» ввести все организационные юниты, данные из которых необходимо синхронизировать. Например: CN=Users, DC=mycompany, DC=com.
Query	Поле необязательно для заполнения. При необходимости в поле «Query» ввести фильтр для выбора нужных записей из организационных юнитов. Максимальное количество символов 10000. Фильтр будет применяться ко всем записям внутри организационных юнитов, введенных в поле «Base DN»

ПРИМЕЧАНИЕ. В результате будут синхронизированы группы безопасности с `objectClass = group`, устройства с `objectClass = computer`. Если `objectClass` для устройств и групп на LDAP-сервере отличаются от указанных выше, следует изменить их в конфигурационном файле ППО.

Рекомендации по использованию фильтров:

– если для выбора необходимых устройств и/или групп из юнита требуется задать несколько фильтров, то следует добавить еще одну директорию (как указано ниже), затем в каждой строке ввести одинаковый «Base DN» и задать нужный фильтр;
– если требуется синхронизировать в ПУ удаленные устройства, следует указать организационный юнит, в котором они хранятся, или задать фильтры для загрузки таких устройств;

– если не требуется синхронизировать в ПУ удаленные устройства, следует задать в фильтрах правило, которое исключит такие устройства: если устройство имеет статус или параметр, определяющий его неактивность, то необходимо указать это в фильтре. Например: `!(deviceType=NEW)`;

2) Нажать кнопку «Добавить директорию» (см. Рисунок 232 [3]) и заполнить поля «Base DN» и «Query» согласно таблице (см. Таблица 51), если необходимо добавить еще одну директорию для синхронизации;

3) Переключатель «Сохранять десинхронизированные устройства» (Рисунок 233 [1]) оставить в положении «Включен», если требуется, чтобы устройства, которые должны будут заархивироваться в ПУ при синхронизации (удаленные на LDAP-сервере), перемещались в группу `desynced_devices`. Если перевести переключатель в положение «Выключен», то удаленные на LDAP-сервере устройства при синхронизации перейдут в статус «Архивное»;

4) По умолчанию данные по устройствам из LDAP-сервера будут синхронизироваться каждый 1 час. Если необходимо:

– отключить синхронизацию данных, установить переключатель «Синхронизация по расписанию» в положение «Выключено» (Рисунок 233 [2]).

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных;

– изменить частоту синхронизации, ввести нужный временной интервал в поле «Повторять каждые» (Рисунок 233 [3]);

5) Нажать кнопку «Сохранить» (Рисунок 233 [4]).

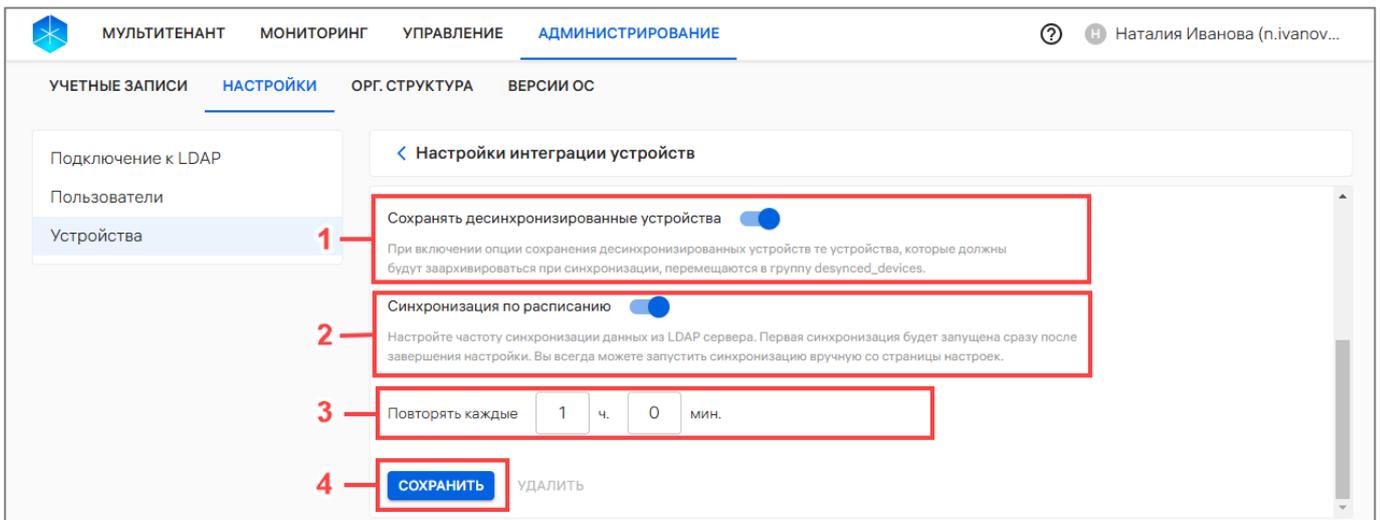


Рисунок 233

В результате будет добавлена интеграция устройств ПУ с LDAP-сервером и запущена первая синхронизация данных.

Для просмотра даты начала и статус синхронизации (Рисунок 234) необходимо нажать значок  в раскрывающейся строке «Сервер LDAP».

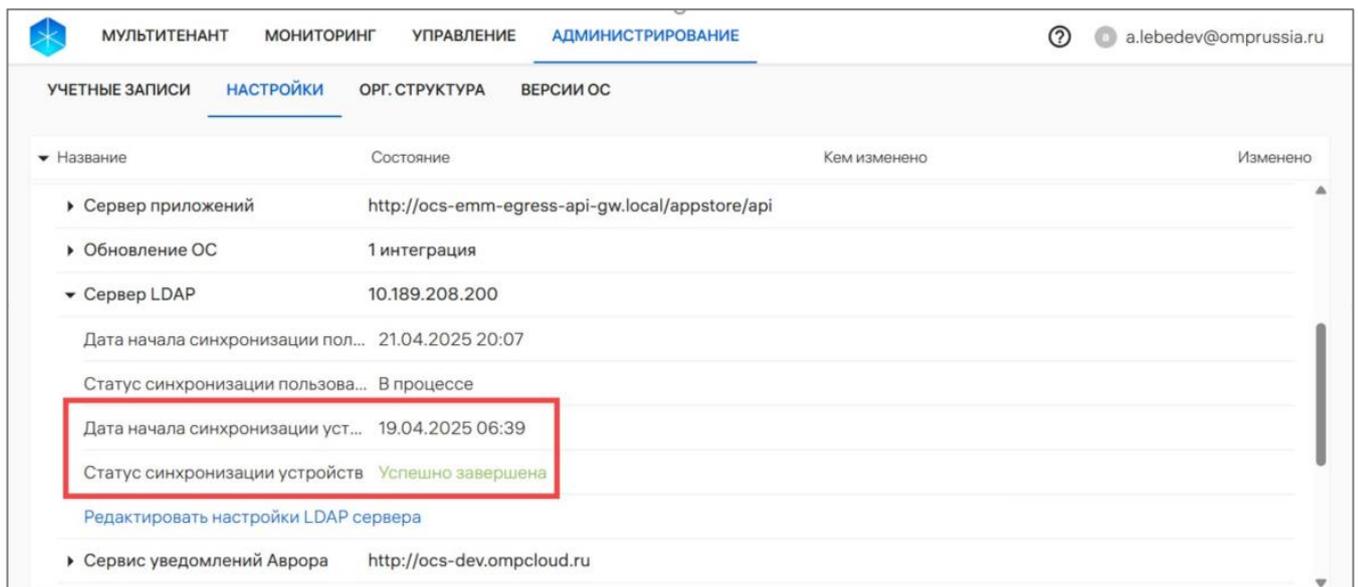


Рисунок 234

В случае ошибки синхронизации данных для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (пример: см. Рисунок 231).

Доступно активировать устройства, синхронизированные из LDAP-сервера, с помощью сгенерированного QR-кода или приглашения на самостоятельную регистрацию. В качестве идентификатора устройства будет использовано сетевое имя (hostname) устройства.

ВНИМАНИЕ!

✓ При активации устройств, импортированных по LDAP, необходимо учитывать, что их сетевые имена будут содержать не более 15 символов в службе каталогов. Таким образом, устройства, у которых различаются только 16-й и далее символы, считаются как одно и то же устройство. Не рекомендуется использовать длинные сетевые имена, так как при передаче в ПУ они будут обрезаться (не более 15 символов);

✓ Сетевое имя устройства присылается приложением «Аврора Центр» с добавленным к нему названием домена. Например: для устройства «рс1» в домене «omr.ru» параметр будет содержать «рс1.omr.ru». Из этих же соображений не рекомендуется использовать точку «.» в названии устройства.

4.1.4.3.2. Редактирование настроек интеграции с LDAP-сервером

При необходимости возможно изменить настройки интеграции ПУ с LDAP-сервером Microsoft Active Directory, после чего синхронизация также будет односторонняя – данные из ПУ не будут переноситься на LDAP-сервер.

Для редактирования настройки интеграции с LDAP-сервером необходимо выполнить следующие действия:

– в раскрывающейся строке «Интеграция» развернуть строку «Сервер LDAP» (Рисунок 235 [1]) и нажать «Редактировать настройки LDAP-сервера» (Рисунок 235 [2]);

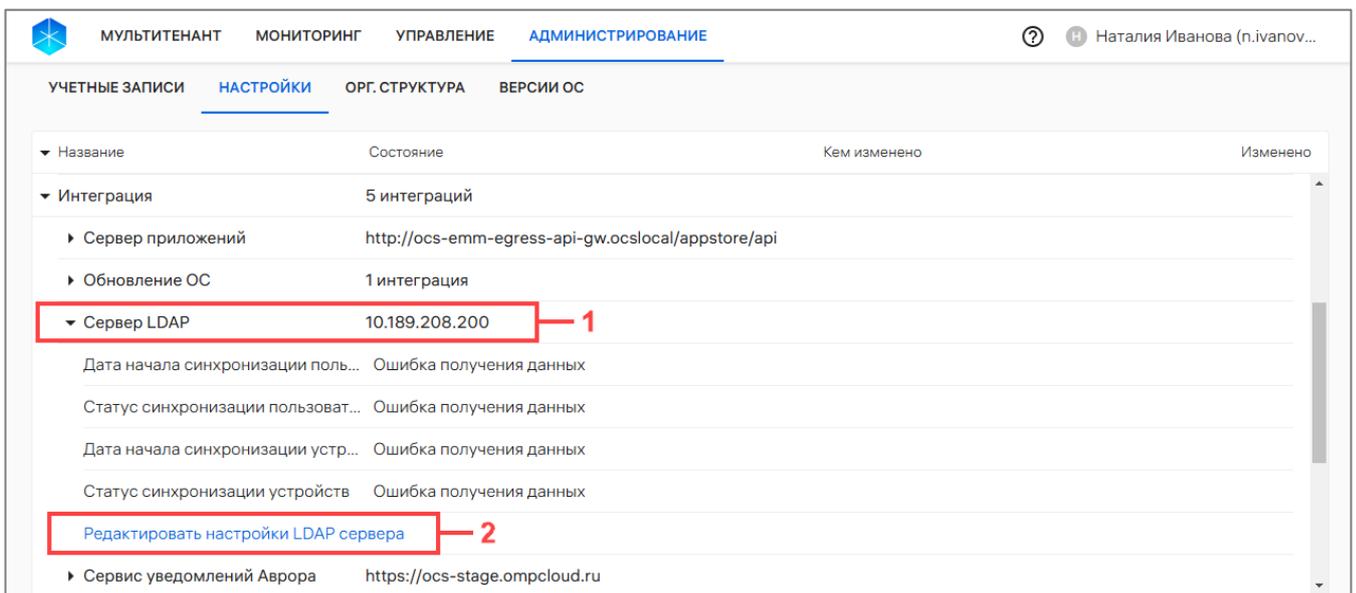


Рисунок 235

– при необходимости изменить:

- настройки для подключения к LDAP-серверу в соответствии с описанием, приведенным в пп. 4.1.4.3.1.1. В результате успешного редактирования настройки подключения ПУ к LDAP-серверу будут изменены. Если была настроена интеграция пользователей и/или устройств, то начнется новая синхронизация данных;
- настройки интеграции пользователей в соответствии с описанием, приведенным в пп. 4.1.4.3.1.2. В результате успешного редактирования настройки интеграции пользователей будут изменены. Начнется новая синхронизация данных;
- настройки интеграции устройств в соответствии с описанием, приведенным в пп. 4.1.4.3.1.3. В результате успешного редактирования настройки интеграции устройств будут изменены. Начнется новая синхронизация данных.

4.1.4.3.3. Удаление интеграции с LDAP-сервером

При необходимости возможно удалить интеграцию пользователей и/или устройств ПУ с LDAP-сервером. В этом случае синхронизировать данные с ППО будет возможно, пока не будет добавлена новая интеграции с LDAP-сервером.

Для удаления интеграции с LDAP-сервером необходимо выполнить следующие действия:

- в раскрывающейся строке «Интеграция» развернуть строку «Сервер LDAP» (см. Рисунок 235 [1]) и нажать «Редактировать настройки LDAP-сервера» (см. Рисунок 235 [2]);
- в области фильтров перейти во вкладку:
 - «Пользователи» (Рисунок 236 [1]) и нажать кнопку «Удалить» (Рисунок 236 [2]) для удаления интеграции пользователей;

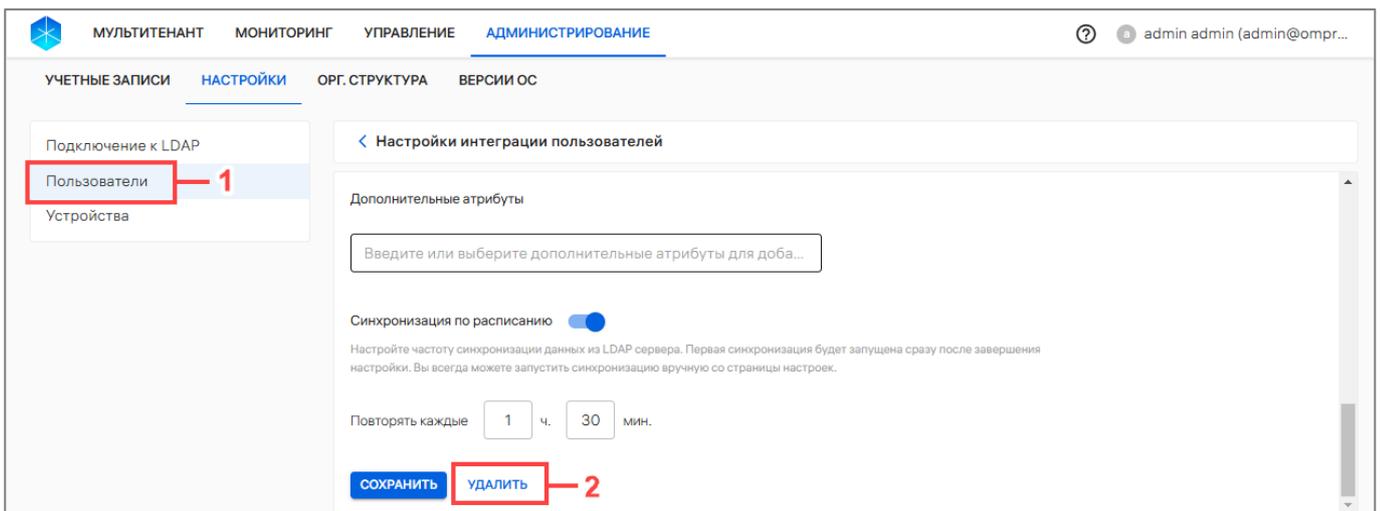


Рисунок 236

- «Устройства» (Рисунок 237 [1]) и нажать кнопку «Удалить» (Рисунок 237 [2]) для удаления интеграции устройств;

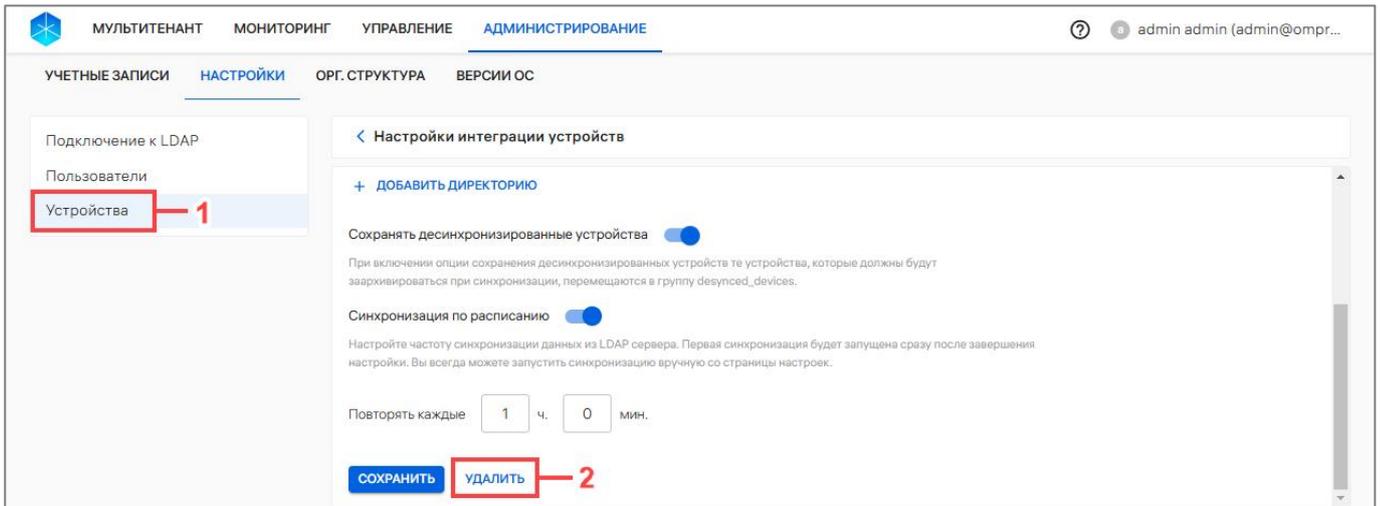


Рисунок 237

– в отобразившемся окне:

- при удалении интеграции пользователей подтвердить либо отменить действия (Рисунок 238);

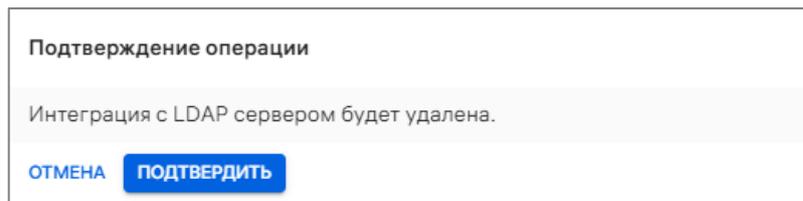


Рисунок 238

- при удалении интеграции устройств, если требуется чтобы:
 - ◆ синхронизированные ранее устройства были перенесены в группу `desynced_devices`, нажать кнопку «Сохранить устройства» (Рисунок 239);
 - ◆ устройства были заархивированы, нажать кнопку «Удалить устройства» (Рисунок 239).

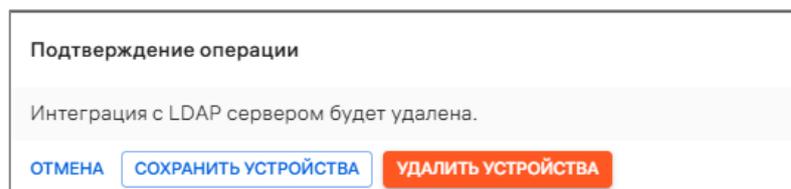


Рисунок 239

В результате успешного удаления:

- интеграция пользователей будет удалена. Синхронизированные ранее пользователи будут заархивированы;
- интеграция устройств будет удалена. Синхронизированные ранее устройства будут заархивированы или перемещены в папку `desynced_devices` (в зависимости от того, что было выбрано в окне подтверждения (см. Рисунок 239)).

Для синхронизации пользователей и/или устройств и групп с ПУ потребуется добавить новую интеграцию с LDAP-сервером (пп. 4.1.4.3.1).

4.1.4.4. Сервис уведомлений Аврора

Сервис уведомлений Аврора – настройка ПСУ.

С помощью ПСУ на устройства осуществляется оперативная доставка информации (текстовые сообщения и команды) в виде текстовых push-уведомлений.

Описание работы ПСУ приведено в документе «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений» АДМГ.20134-01 90 01-5.

Описание доставки push-уведомлений на устройства приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора» АДМГ.20134-01 90 01-7.

Для просмотра настроек ПСУ необходимо нажать значок , в результате чего отобразятся параметры, приведенные в таблице (Таблица 52).

Таблица 52

Настройки	Описание
Интеграция с СУА	Определяет включение отправки настроек ПСУ для приложения «Аврора Центр»
Настройки устройства	
Адрес для мобильного клиента	Адрес ПСУ для приложения «Аврора Центр»
Порт для мобильного клиента	Порт уведомлений для приложения «Аврора Центр»
ID приложения	Идентификатор приложения «Аврора Центр», с которым оно регистрируется в ПСУ
Дополнительные параметры (отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они не учитываются на устройствах на базе ОС Android)	
CRL: Проверка отзыва сертификатов	Определяет, включена ли проверка наличия сертификата ПСУ среди списка отозванных сертификатов
CRL: Интервал обновления в секундах	Временной интервал обновления списка отозванных сертификатов
SSL: Валидация сертификата	Определяет, включена ли валидация сертификата ПСУ
SSL: Уровень валидации сертификата	Уровень валидации имени хоста, указанного в сертификате ПСУ. Возможные значения: – «Не проверяется»; – «Поддержка поддоменов»; – «Точное совпадение»

Настройки	Описание
Настройки сервера	
Адрес API	Адрес API ПСУ для приложения «Аврора Центр»
ID проекта для отправки уведомлений	Идентификатор проекта в ПСУ для отправки уведомлений

Для изменения настроек ПСУ необходимо выполнить одно из следующих действий:

- нажать на название поля «Сервис уведомления Аврора» (Рисунок 240 [1]);
- нажать «Редактировать настройки Сервиса уведомлений Аврора» (Рисунок 240 [2]).

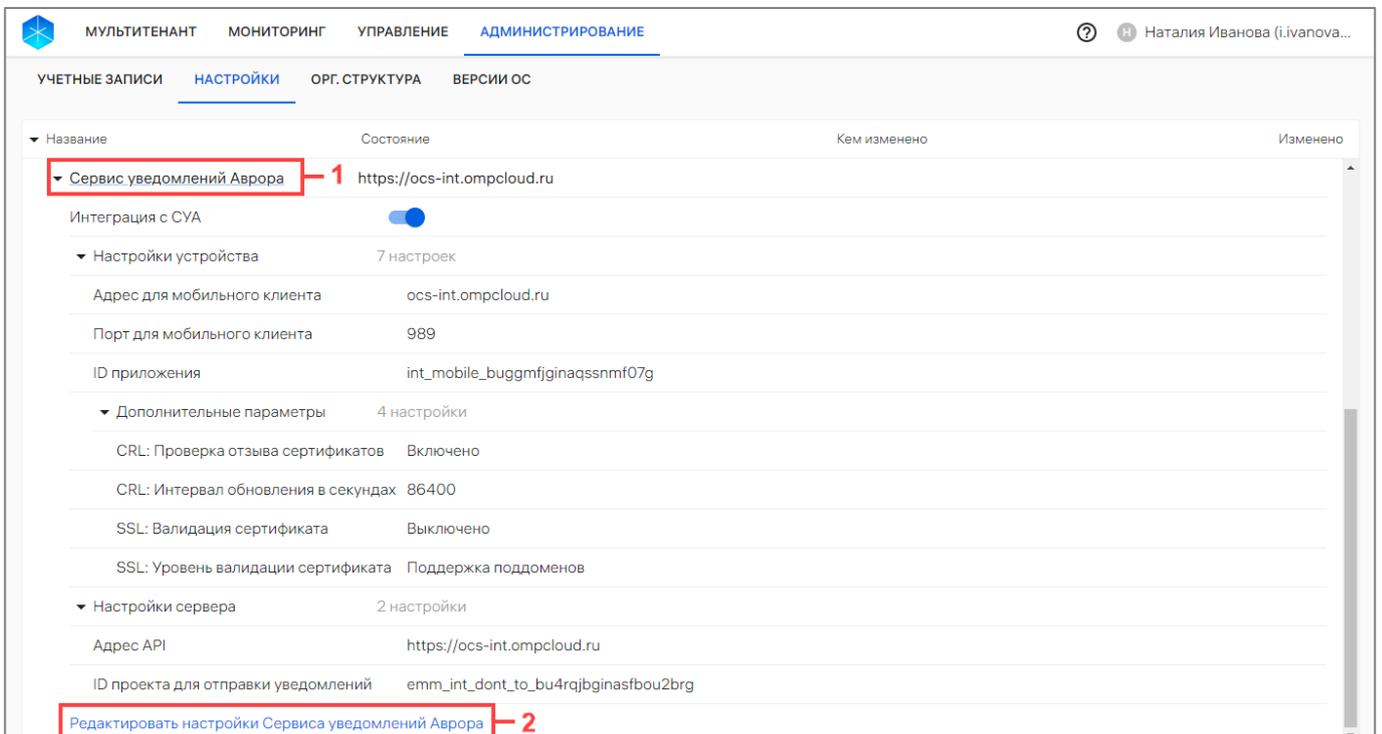


Рисунок 240

В результате выполнения одного из указанных действий будут доступны поля для редактирования настройки ПСУ одним из следующих способов (Рисунок 241):

- загрузка JSON-файлов с настройками нажатием кнопки «Загрузить файлы настроек»;

МУЛЬТИТЕНАНТ
МОНИТОРИНГ
УПРАВЛЕНИЕ
АДМИНИСТРИРОВАНИЕ

?
Наталья Иванова (n.ivanov...)

УЧЕТНЫЕ ЗАПИСИ
НАСТРОЙКИ
ОРГ. СТРУКТУРА
ВЕРСИИ ОС

[← Настройки Сервиса уведомлений Аврора](#)

ЗАГРУЗИТЬ ФАЙЛЫ НАСТРОЕК

Загрузка настроек проекта в json-формате, файл можно запросить у функционального администратора СУА

Мобильные устройства

Имя хоста для мобильного клиента

IP-адрес или имя хоста сервиса уведомлений Аврора для мобильного приложения Аврора Центр

ID приложения мобильного клиента

Идентификатор приложения, с которым регистрируется мобильное приложение Аврора Центр в сервисе уведомлений Аврора

SSL

Валидация соединения с сервером

Включено

Валидация сертификата сервиса уведомлений Аврора

Уровень валидации имени хоста

Не выбрано

Уровень валидации имени хоста, указанного в сертификате

CRL

Проверка отозванности сертификата

Включено

Определяет, включена ли проверка наличия сертификата среди списка отозванных сертификатов

Период обновления

Указывается в секундах

Параметры сервера

Адрес API

IP-адрес или имя хоста API сервиса уведомлений Аврора для мобильного приложения Аврора Центр

ID проекта для отправки уведомлений

Идентификатор проекта из системы уведомлений Аврора

Параметры для авторизации

Token URL

Ссылка для получения токена авторизации

Client ID

Идентификатор клиента технической учетной записи

Key ID

Идентификатор ключа технической учетной записи, который используется на сервисе авторизации

Приватный ключ установлен ОБНОВИТЬ КЛЮЧ

Приватный ключ технической учетной записи

Audience

✎

Аудитории токена доступа

Scopes

✎

Области (скоупы) для OIDC-клиента, которые используются для аутентификации в СУА

Интеграция

НАСТРОИТЬ ИНТЕГРАЦИЮ С ВНЕШНИМ СЕРВИСОМ УВЕДОМЛЕНИЙ

Выгрузка файла с настройками Аврора Центр для подключения к отдельно развернутому Сервису уведомлений

СОХРАНИТЬ

Интеграция с СУА

Рисунок 241

– внесение изменений вручную в соответствии с таблицей (Таблица 53).

После внесения уточнения в соответствии с таблицей (Таблица 53) необходимо подтвердить либо отменить действия.

Таблица 53

Поле	Описание
Интеграция с СУА	Данное поле предназначено для включения или выключения отправки настроек ПСУ для приложения «Аврора Центр» при помощи переключателя 
Мобильные устройства	
Имя хоста для мобильного клиента	IP-адрес или имя хоста ПСУ для приложения «Аврора Центр»
Порт для мобильного клиента	Номер порта уведомлений для приложения «Аврора Центр»
ID приложения мобильного клиента	Идентификатор приложения, с которым приложение «Аврора Центр» регистрируется в ПСУ
SSL (параметры SSL отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они учитываются на устройствах на базе ОС Android)	
Валидация соединения с сервером	Выбор из раскрывающегося списка значения, которое определяет, включена ли валидация сертификата ПСУ: <ul style="list-style-type: none"> – Выключено; – Включено
Уровень валидации имени хоста	Выбор из раскрывающегося списка уровня валидации имени хоста, указанного в ПСУ: <ul style="list-style-type: none"> – Не выбрано; – Не проверяется; – Поддержка поддоменов; – Точное совпадение
CRL (параметры CRL отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они не учитываются на устройствах с ОС Android)	
Проверка отозванности сертификата	Выбор из раскрывающегося списка значения, определяющего, включена ли проверка наличия сертификата ПСУ среди списка отозванных сертификатов: <ul style="list-style-type: none"> – Выключено; – Включено
Период обновления	Ввод значения с клавиатуры временного интервала обновления списка отозванных сертификатов (в секундах)

Поле	Описание
Параметры сервера	
Адрес API	Адрес API ПСУ для приложения «Аврора Центр» (в виде proto://host:port). Параметр должен быть задан администратором в конфигурационном файле ППО. При изменении параметра вручную настройки ПСУ не меняются
ID проекта для отправки уведомлений	Ввод значения с клавиатуры: идентификатор проекта в ПСУ для отправки уведомлений
Параметры для авторизации	
Token URL	Ввод значения с клавиатуры: URL для получения токена авторизации
ClientID	Ввод значения с клавиатуры: идентификатор клиента технической учетной записи
KeyID	Ввод значения с клавиатуры: приватный ключ технической учетной записи. Параметр указывает, какой ключ используется на сервисе авторизации
Приватный ключ	Необходимо нажать «Обновить ключ» и ввести приватный ключ технической учетной записи
Audience	Ввод значения с клавиатуры: аудитория токена доступа после нажатия значка  . Для удаления аудитории необходимо нажать значок  справа от его названия
Scopes	Ввод значения с клавиатуры: область (скоуп) для OIDC-клиента, используемая для аутентификации в ПСУ. Для ввода значения необходимо нажать значок  . Для удаления области необходимо нажать значок  справа от ее названия
Интеграция	
Настроить интеграцию с внешним сервисом уведомлений	При нажатии «Настроить интеграцию с внешним сервисом уведомлений» произойдет выгрузка JSON-файла с настройками Аврора Центр для подключения к отдельно развернутому Сервису уведомлений. ПРИМЕЧАНИЕ. Процесс подключения к отдельно развернутому Сервису уведомлений приведен в документе «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений» АДМГ.20134-01 90 01-5

4.1.4.5. Центры сертификации

В ППО доступна возможность добавить интеграцию с центром сертификации, который выпускает пользовательские сертификаты для подключения к беспроводным сетям.

ВНИМАНИЕ! ППО протестировано с интеграцией с центрами сертификации, имеющими тип сервера Microsoft Active Directory Certificate Services (AD CS) в Windows Server 2019.

Для просмотра списка интеграций с центрами сертификации необходимо нажать значок . Для добавления центра сертификации необходимо выполнить следующие действия:

- нажать «Добавить центр сертификации» (Рисунок 242);
- заполнить поля ввода, приведенные в таблице (Таблица 54);
- нажать кнопку «Создать».

В результате интеграция с центром сертификации будет добавлена в ППО.

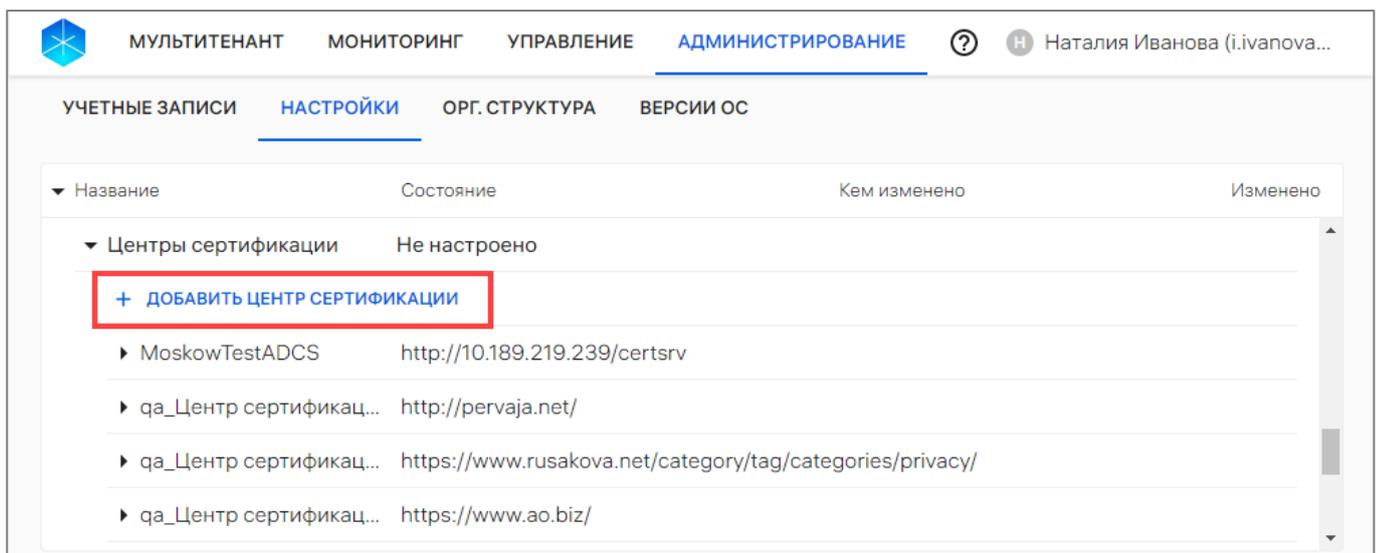


Рисунок 242

Таблица 54

Поле	Описание
Название	Название центра сертификации. Ввод значения с клавиатуры. Может содержать от 1 до 256 символов
URL до сервера	URL-адрес сервера для подключения к центру сертификации. Может содержать от 1 до 256 символов
Тип сервера	По умолчанию установлено значение Microsoft AD CS. Поле недоступно для редактирования
Логин	Логин для подключения к центру сертификации. Может содержать от 1 до 256 символов
Пароль	Пароль для подключения к центру сертификации. Может содержать от 1 до 256 символов

4.1.4.6. Git-репозитории

Для добавления в ПУ различных файлов скриптов/конфигураций для распространения на устройства доступно подключение удаленных репозиториях GIT. Для этого необходимо добавить интеграцию с Git- репозиторием.

Для просмотра списка подключенных Git-репозиториях, даты начала и статуса его синхронизации с ППО (Рисунок 243 [2]) необходимо нажать значок  в строке «Git-репозитории».

Для подключения необходимо выполнить следующие действия:

- нажать на кнопку «Подключить Git-репозиторий» (Рисунок 243 [1]);

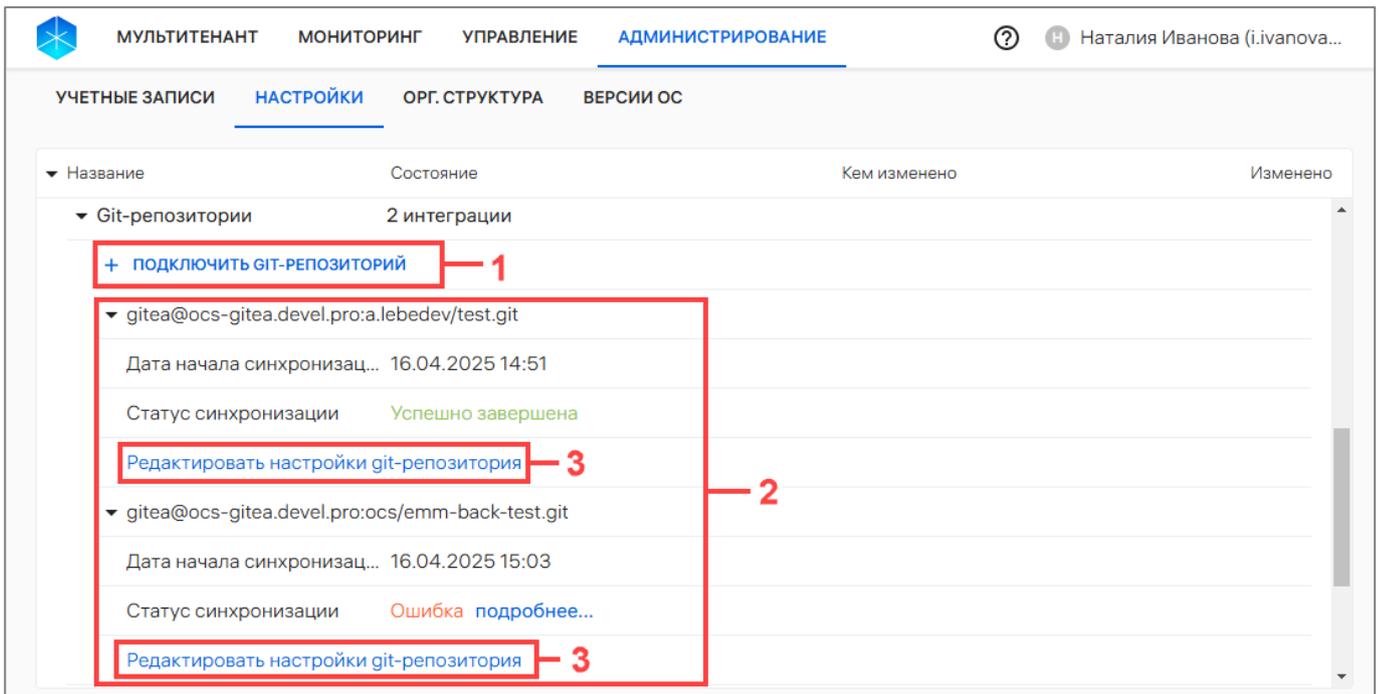


Рисунок 243

– в отобразившемся окне в поле «Публичный SSH-ключ» будет сгенерирован SSH-ключ, который необходимо скопировать с помощью кнопки  (Рисунок 244 [2]) и добавить в Git-репозиторий, который необходимо подключить;

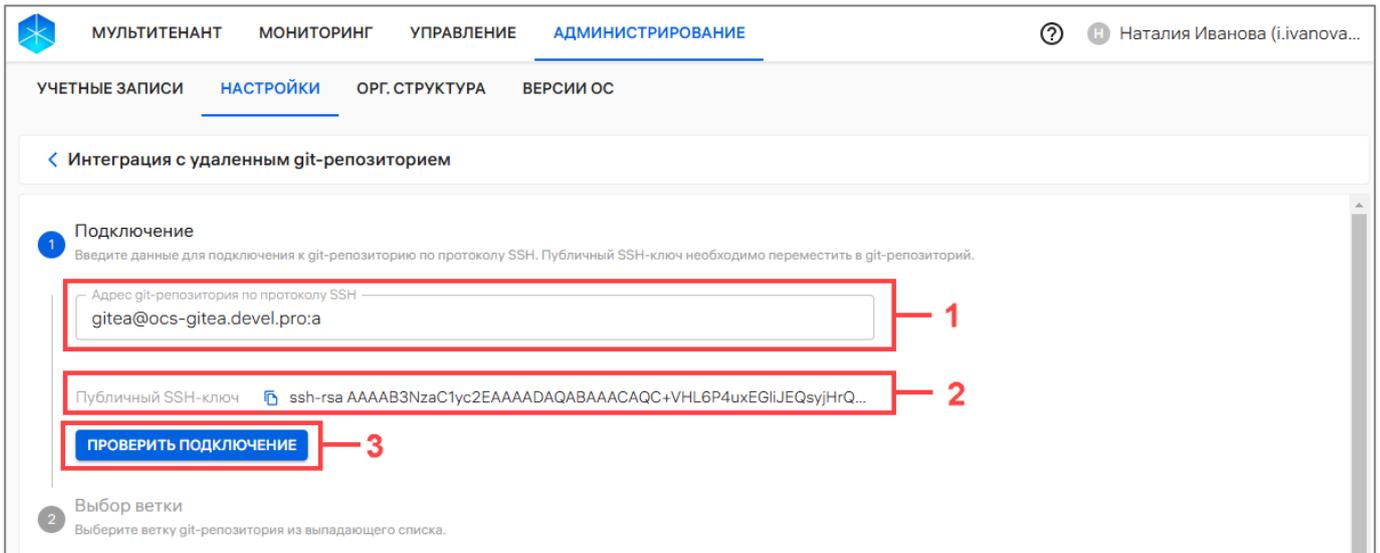


Рисунок 244

– в поле «Адрес Git-репозитория по протоколу SSH» (см. Рисунок 244 [1]) ввести адрес и нажать на кнопку «Проверить подключение» (см. Рисунок 244 [3]);

ВНИМАНИЕ! Если сервис для хостинга Git-репозитория использует нестандартный SSH-порт, то данный порт должен быть задан при создании интеграции с Git. Для этого необходимо в строке подключения использовать следующую scp-style нотацию: `<user>@<host>:<port>:<path>`.

Например: `git@example.com:22222:path/to_repository.git`;

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 245). При успешном подключении к Git-репозиторию отобразится соответствующее сообщение;

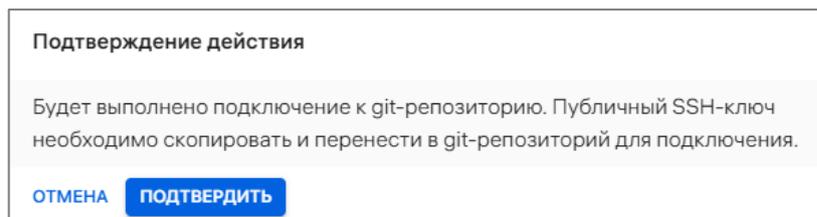


Рисунок 245

– в раскрывающемся списке «Ветка» (Рисунок 246 [1]) выбрать ветку репозитория, файлы из которой требуется добавить в ПУ;

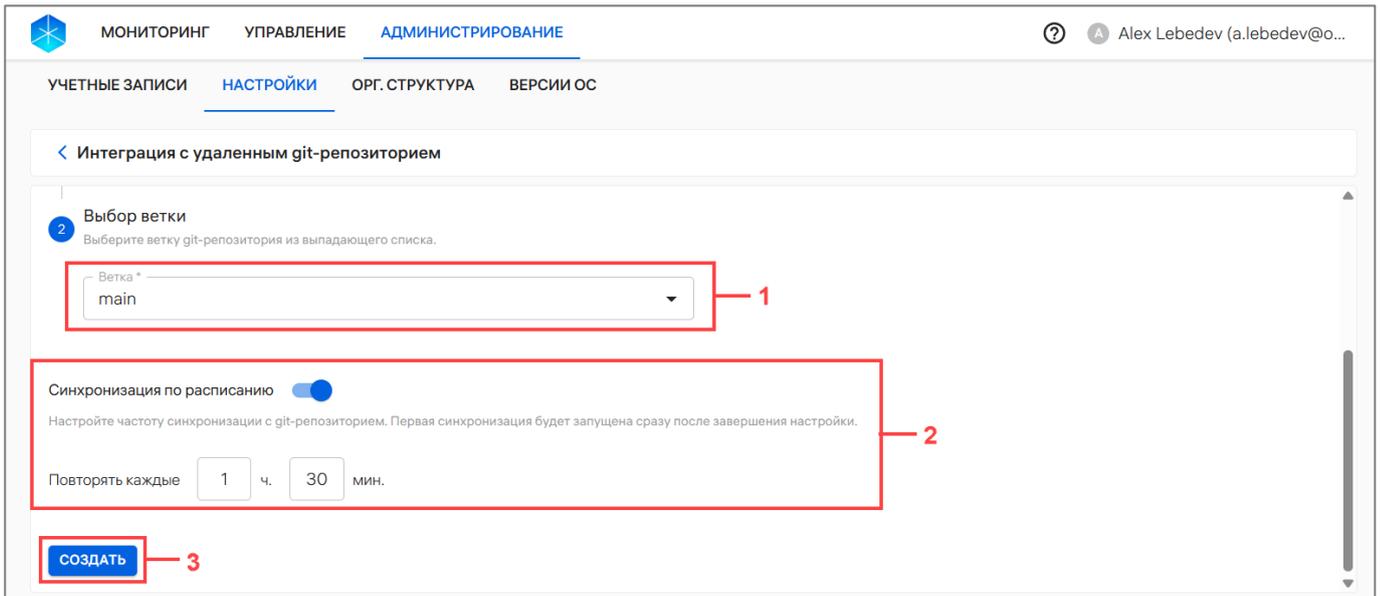


Рисунок 246

– перевести переключатель «Синхронизация по расписанию» (Рисунок 246 [2]) в положение «Включено», если требуется задать частоту синхронизации с Git-репозиторием, а в поле «Повторять каждые» ввести частоту синхронизации. По умолчанию задана частота 5 минут.

ПРИМЕЧАНИЕ. При каждой синхронизации ППО будет проверять наличие новых версий загруженных файлов в Git-репозитории, и, в случае их наличия, автоматически загрузит новые версии в ППО;

– нажать на кнопку «Создать» (см. Рисунок 246 [3]).

В результате Git-репозиторий будет подключен к ППО и произойдет первая синхронизация.

Также для интеграции с Git-репозиторием доступно редактирование (включение, отключение синхронизации, а также изменение ее частоты). Для этого в списке подключенных Git-репозиториев необходимо нажать на «Редактировать настройки git-репозитория» (см. Рисунок 243 [3]).

В открывшемся окне редактирования:

– включить/выключить синхронизацию, для этого перевести переключатель «Синхронизация по расписанию» в нужное положение;

– изменить частоту синхронизации, для этого задать нужную частоту в поле «Повторять каждые»;

– нажать кнопку «Сохранить».

В результате настройки синхронизации с Git-репозиторием будут изменены.

4.1.5. Территории

Территории используются для офлайн-сценариев с событиями «Нахождение на территориях, определяемых координатами»/«Нахождение вне территории, определяемой координатами». Территория может содержать один или несколько четырехугольных полигонов, нанесенных на карту.

В раскрывающейся строке «Территории» при нажатии на значок  (см. Рисунок 213 [6]) отображается список территорий (Рисунок 247 [2]).

Если потребуется просмотреть территорию на карте, необходимо нажать на ее название.

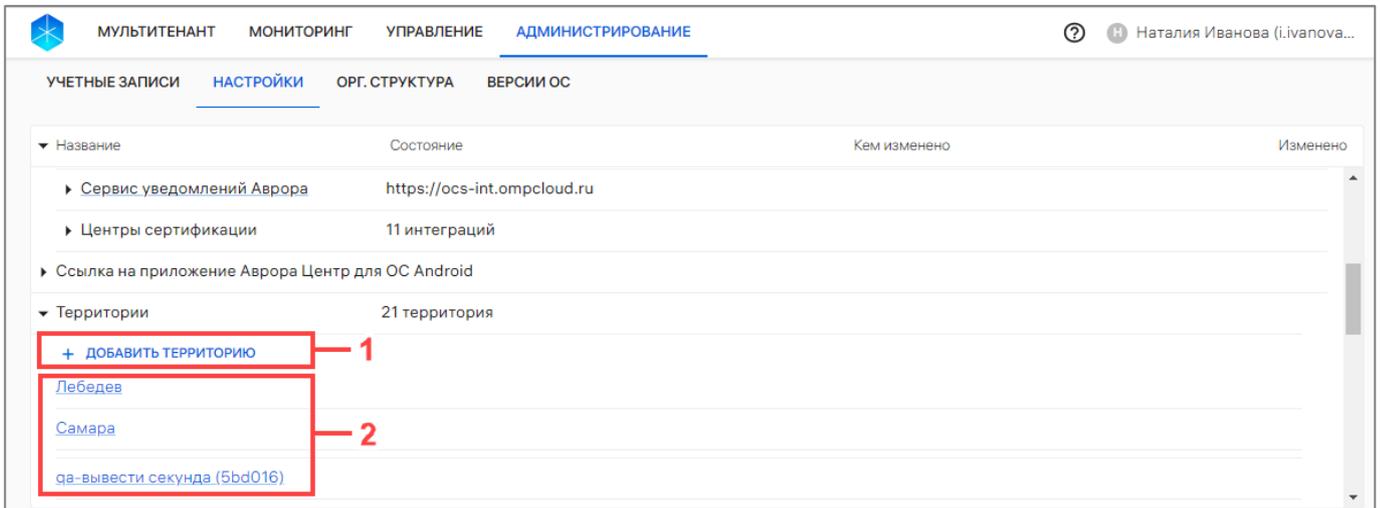


Рисунок 247

Для добавления территории необходимо выполнить следующие действия:

- нажать кнопку «Добавить территорию» (см. Рисунок 247 [1]);
- в отобразившемся окне необходимо ввести название территории в поле «Название» (Рисунок 248 [1]). Поле обязательно для заполнения и может содержать от 1 до 256 символов;

- добавить 1 или несколько полигонов на территории, выполнив следующие действия:

- выбрать объект на карте;
- нажать кнопку  «Добавить полигон» (Рисунок 248 [3]);
- указать на карте 4 вершины полигона (Рисунок 248 [2]). С помощью перемещения вершин полигона возможно менять его форму. У полигона не может быть нулевой площади. Ребра одного полигона не должны пересекать друг друга. Территория должна содержать хотя бы один полигон.

ПРИМЕЧАНИЕ. Возможно добавление до 50 полигонов на территории;

- при необходимости доступно удаление полигонов, выделенных на карте. Для этого необходимо нажать на значок  «Удалить полигон» и выбрать необходимый полигон (Рисунок 248 [4]);

- после ввода данных необходимо подтвердить либо отменить действие (Рисунок 248 [5]).

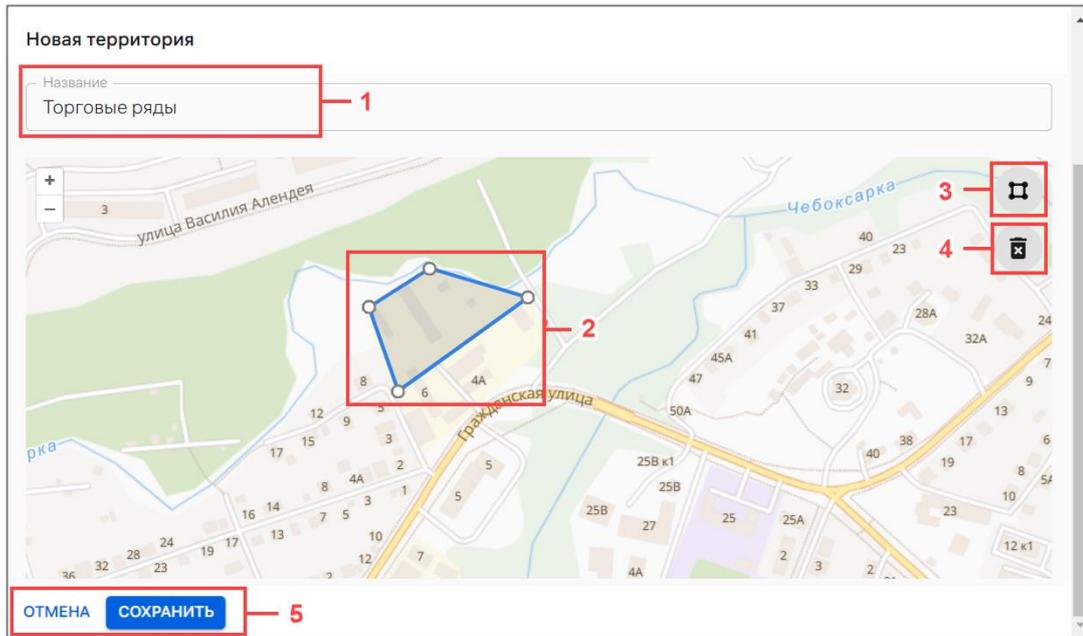


Рисунок 248

В результате успешного сохранения данных, территория будет добавлена в ППО и будет доступна при создании офлайн-сценариев с событиями «Нахождение на территориях, определяемых координатами»/«Нахождение вне территории, определяемой координатами».

4.1.6. Настройки правил политик

При настройке правил политики доступен:

– запрет удаления приложений с устройств при переключении переключателя в положение «Включено»  (Рисунок 249 [1]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 249 [4]). При включенном запрете на удаление приложений с устройств после снятия политики с группы устройств и переходе между другими группами устройств устанавливаемые и установленные ранее приложения:

- будут сохраняться на устройствах;
- не будут влиять на соответствие политике, которая больше не содержит правила по установке приложений.

ВНИМАНИЕ! Если на устройство была назначена политика с правилом по установке приложений с каким-либо интервалом установки, а затем из политики удалили правило по установке приложения и переназначили на устройство до момента наступления интервала установки, то устройство не установит это приложение даже при включенной настройке по запрету удаления приложений с устройств;

– запрет удаления файлов с устройств при переключении переключателя в положение «Включено»  (Рисунок 249 [2]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 249 [4]). При включенном запрете на удаление файлов с устройств после снятия политики с группы устройств и переходе между другими группами устройств доставляемые и доставленные ранее файлы:

- будут сохраняться на устройствах;
- не будут влиять на соответствие политике, которая больше не содержит правила по доставке файлов;

– запрет удаления скриптов с устройств при переведении переключателя в положение «Включено»  (Рисунок 249 [3]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 249 [4]). При включенном запрете на удаление скриптов с устройств после снятия политики с группы устройств и переходе между другими группами устройств выполняемые и выполненные ранее скрипты:

- будут сохраняться на устройствах;
- не будут влиять на соответствие политике, которая больше не содержит правила по выполнению скрипта.

ВНИМАНИЕ! При включении запрета на удаление скриптов с устройств автоматически включается запрет на удаление файлов с устройств.

ПРИМЕЧАНИЕ. После сохранения настройка запрета с соответствующим значением отправится на устройство при следующей синхронизации с сервером Аврора Центр.

Описанный выше результат будет действовать до тех пор, пока в настройках Аврора Центр самостоятельно не будет выключен запрет.

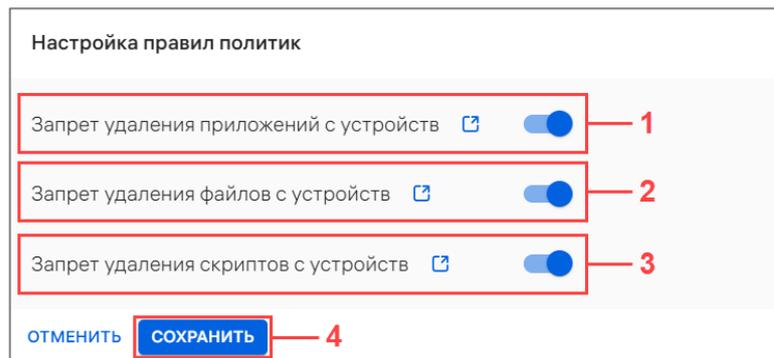


Рисунок 249

4.1.7. Доверенные сети

Доверенные сети используются для проверки IP-адреса устройств, которые используют для самостоятельной регистрации в ПУ приглашение (если такая настройка была включена в приглашении), подробнее п. 2.2.4.

В раскрывающейся строке «Доверенные сети» при нажатии на значок  (см. Рисунок 213 [8]) отображается список доверенных сетей, добавленных в ПУ (Рисунок 250 [2]) с отображением следующей информации:

- «Имя» – название доверенной сети;
- «Адрес сети» – адрес доверенной сети;
- «Комментарий» – комментарий к доверенной сети.

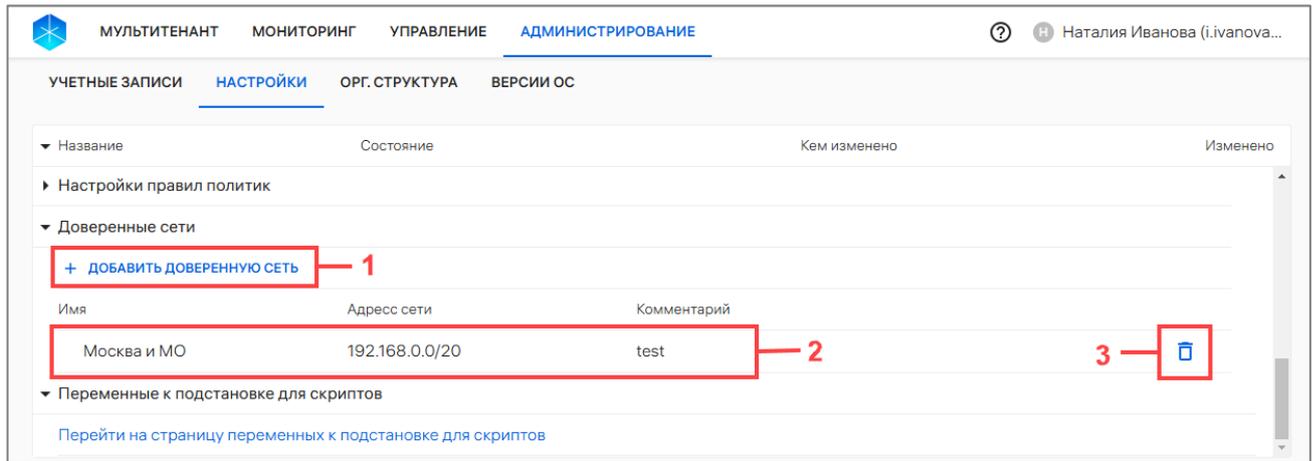


Рисунок 250

Для добавления доверенной сети, необходимо выполнить следующие действия:

- нажать кнопку «Добавить доверенную сеть» (см. Рисунок 250 [1]);
- в отобразившемся окне (Рисунок 251) заполнить поля, приведенные в таблице (Таблица 55);
- после ввода значений необходимо подтвердить либо отменить действия.

Доверенная сеть

Название

Сеть и маска

Комментарий

[ОТМЕНА](#) [СОХРАНИТЬ](#)

Рисунок 251

Таблица 55

Параметр	Описание
Название	Название доверенной сети. Может содержать от 1 до 100 символов. Поле обязательно для заполнения
Сеть и маска	Адрес доверенной сети в формате IPv4/маска. Поле обязательно для заполнения
Комментарий	Дополнительная информация к доверенной сети. Может содержать до 1000 символов. Поле не обязательно для заполнения

Для удаления доверенной сети необходимо нажать на значок  «Удалить доверенную сеть» (см. Рисунок 250 [3]) и в открывшемся окне (Рисунок 252) подтвердить либо отменить действие.

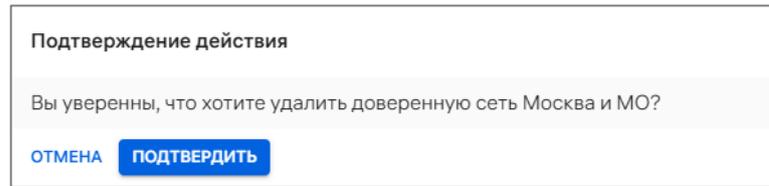


Рисунок 252

4.1.8. Переменные к подстановке для скриптов

В Консоли администратора ПУ доступен просмотр списка всех управляемых переменных, которые существуют в ППО, а при отсутствии добавленных данных отображается сообщение «Нет данных».

Для просмотра данных необходимо:

- в разделе «Переменные к подстановке для скриптов» нажать на «Перейти на страницу переменных к подстановке для скриптов» (см. Рисунок 213 [9]);
- отобразится список управляемых переменных (Рисунок 253 [2]), информация о которых отображается в столбцах, приведенных в таблице (Таблица 56).

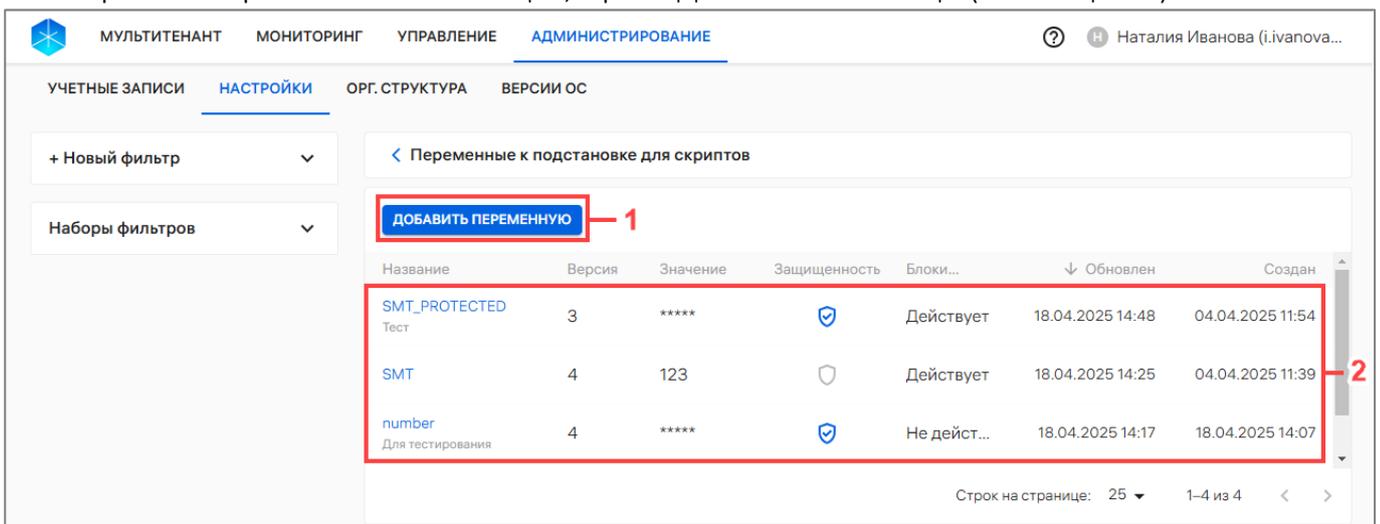


Рисунок 253

Таблица 56

Название столбца	Описание
Название	– название управляемой переменной, заданное при добавлении; – комментарий (при наличии), заданный при добавлении/редактировании
Версия	Номер версии управляемой переменной
Значение	Возможные значения: – открытое исходное значение переменной, если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Выключен»; – 5 звезд, если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Включен»

Название столбца	Описание
Защищенность	Возможные значения: – <input type="radio"/> «Незащищенная переменная» - если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Выключен»; – <input checked="" type="radio"/> «Защищенная переменная» - если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Включен»
Блокировка	Возможные значения: – значение «Не действует», если управляемая переменная была добавлена впервые или в процессе редактирования переключатель «Блокировка» был переведен в положение «Выключен»; – значение «Действует», если при редактировании управляемой переменной переключатель «Блокировка» был переведен в положение «Включен»
Обновлен	Дата и время обновления управляемой переменной в ПУ
Создан	Дата и время добавления управляемой переменной в ПУ

Для добавления новой управляемой переменной в ППО для дальнейшего использования в правиле политики «Скрипты/Выполнение на устройстве» (пп. 2.4.1.39) необходимо нажать на кнопку «Добавить переменную» (см. Рисунок 253 [1]), заполнить параметры, приведенные в таблице (Таблица 57) и нажать на кнопку «Сохранить».

Таблица 57

Параметр	Описание
Название	Ввести название управляемой переменной с выполнением следующих условий: – допустимые символы: - a-z, A-Z, 0-9 и _; – первый символ в названии не должен содержать цифру; – название не должно быть меньше 1-ого и больше 255-ти символов. Поле обязательно для заполнения, не подлежит редактированию
Значение	Ввести значение управляемой переменной. Значение не должно быть меньше 1-ого и больше 4096-ти символов. Поле обязательно для заполнения. ПРИМЕЧАНИЕ! Поле не доступно для редактирования, если переменная заблокирована
Защищенность	Если требуется сделать управляемую переменную защищенной, перевести переключатель «Защищенность» в положение «Включен». По умолчанию он выключен.

Параметр	Описание
	<p>ПРИМЕЧАНИЕ. Если переменная защищена, то она будет храниться в специальном защищенном хранилище ППО. И ее значение нельзя будет увидеть в списке управляемых переменных. Защищенные переменные используются в случаях, когда важно, чтобы устройство получало «чувствительную» информацию для скриптов из защищенного хранилища.</p> <p>ВНИМАНИЕ! Если редактируемая управляемая переменная является уже защищенной, то сделать из нее незащищенную невозможно. Переключатель «Защищенность» при редактировании будет не активен</p>
Блокировка	<p>ВНИМАНИЕ! Переключатель «Блокировка» доступен только при редактировании управляемой переменной.</p> <p>Необходимо перевести переключатель «Блокировка» в положение:</p> <ul style="list-style-type: none"> – «Включено», если требуется сделать переменную заблокированной; – «Выключено», если требуется разблокировать переменную. <p>ПРИМЕЧАНИЯ:</p> <ul style="list-style-type: none"> ✓ Включение блокировки для управляемой переменной позволяет прекратить выполнение скриптов с этой управляемой переменной на устройствах; ✓ Заблокированную переменную возможно выбрать при создании/редактировании правила политики «Скрипты/Выполнение на устройстве» и назначать политику с правилом, содержащим заблокированную управляемую переменную, на группу устройств; ✓ Если редактируемая управляемая переменная является заблокированной, а при редактировании разблокировали ее и были внесены какие-либо изменения в другие поля, а затем заблокировали, то такую управляемую переменную не получится обновить
Комментарий	<p>При необходимости ввести дополнительную информацию к управляемой переменной. Может содержать до 512 символов. Поле не обязательно для заполнения, подлежит редактированию</p>

Также доступно редактирование параметров управляемой переменной. Для этого необходимо:

- в списке управляемых переменных выбрать требуемую переменную (при необходимости воспользоваться фильтром);
- нажать на название нужной переменной;

– в отобразившемся окне внести изменения в полях, приведенных в таблице (см. Таблица 57);

– подтвердить либо отменить действия.

После успешного редактирования переменной ее версия будет увеличена (плюс 1 к предыдущей).

ПРИМЕЧАНИЯ:

✓ Если на устройство назначено 2 политики с одним и тем же выполняемым скриптом, но с разными управляемыми переменными, то при редактировании одной из этих управляемых переменных произойдет перекомбинирование политик, и на устройстве будет действовать более поздняя назначенная политика;

✓ Если при включенной настройке по запрету удаления файлов и скриптов удалить правило по выполнению скрипта с управляемой переменной, то устройство не будет получать обновленные управляемые переменные, несмотря на включенную настройку по запрету удаления скрипта с устройства.

4.2. Подраздел «Орг.структура»

Подраздел «Орг.структура» Консоли администратора ПУ предназначен для просмотра организационной структуры компании, а также получения данных с сервера LDAP, с которым установлено соединение (пп. 4.1.4.3), а при отсутствии добавленных данных отображается сообщение «Нет данных». Заполнение подраздела данными производится с помощью импорта из Active Directory (LDAP) напрямую, если ПУ интегрирована с AD организации (пп. 4.1.4.3).

Для перехода в подраздел необходимо в верхней панели выбрать подраздел «Орг.структура» раздела «Администрирование». В результате отобразится основная информация о пользователях (сотрудниках) и о подразделениях пользователей в следующих столбцах:

– «Подразделение/Пользователь» – название группы или ФИО (при наличии) пользователя, представляющее собой активную ссылку, при нажатии на которую откроется карточка группы или пользователя;

– «Тип» – значок типа группы пользователей или пользователя. При наведении курсора появляется всплывающая подсказка с названием типа;

– «Email» – рабочая электронная почта пользователя. Для групп пользователей в этом столбце информация отсутствует;

– «Телефон» – рабочий телефон пользователя. Для групп пользователей в этом столбце информация отсутствует.

Для просмотра организационной структуры компании необходимо нажать значок  в строке с подразделением. В результате раскроется вложенный список (Рисунок 254) либо при его отсутствии отобразится «Нет дочерних элементов».

МУЛЬТИТЕНАНТ МОНИТОРИНГ УПРАВЛЕНИЕ АДМИНИСТРИРОВАНИЕ ? Н Наталия Иванова (i.ivanova...)

УЧЕТНЫЕ ЗАПИСИ НАСТРОЙКИ ОРГ. СТРУКТУРА ВЕРСИИ ОС

↳ Подразделение / Пользователь	Тип	Email	Телефон
▼ TestStaticUser	☰	—	—
▶ Test Name	☰	—	—
VPN NGate Test	👤	VPN_NGate@omp.ru	—
LName FName	👤	test.test@omptest.local	—

Рисунок 254

5. СООБЩЕНИЯ ОБ ОШИБКАХ И ОГРАНИЧЕНИЯ

5.1. Сообщения об ошибках

В ходе работы с компонентами ПУ пользователям могут выдаваться сообщения об ошибках, приведенные в таблице (Таблица 58).

Таблица 58

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
1	Произошла ошибка. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору
2	Нет связи с сервером. Попробуйте повторить попытку позже	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позже
3	В QR-коде может быть максимум 3 корневых сертификата	Необходимо удалить один из ранее загруженных корневых сертификатов, либо поменять у него свойство «Использовать в QR-коде при активации»
4	Не найдено	Попытка обращения к несуществующему элементу управления. Необходимо обновить страницу
5	Доступ запрещен	Необходимо обратиться к Администратору учетных записей для назначения прав. У учетной записи пользователя нет необходимых прав доступа для просмотра выбранной страницы
6	Истекло время действия активной сессии. Обновите страницу	Авторизованная сессия завершена. Необходимо обновить страницу браузера

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
7	Истек срок действия загруженного Вами QR-кода. Загрузите другой или сгенерируйте новый	Загружен JSON-файл с истекшем сроком действия (<i>expiredAt</i>). Необходимо загрузить JSON-файл с актуальным сроком действия
8	Произошла ошибка на стороне сервера. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору
9	Не удалось считать данные из JSON. Попробуйте другой JSON-файл или исправьте этот	Загрузка некорректного JSON-файла. Необходимо проверить корректность загружаемого файла
10	Не выбрано ни одного устройства для активации	При генерации QR-кода для группы устройств выбрана пустая группа. Необходимо выбрать группу, содержащую хотя бы 1 устройство
11	Загружен JSON-файл с параметрами активации, отличными от параметров текущей конфигурации	Необходимо сверить параметры JSON-файла с конфигурацией. Данная ошибка возникает при несоответствии конфигурации системы одному из значений: – <i>accountDomain</i> ; – <i>gatewayURI</i> ; – <i>clientID</i>
12	Динамическая группа с такими условиями уже существует в системе	Необходимо заменить условия добавления в динамическую группу устройств
13	Устройство с таким MAC WLAN уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле
14	Устройство с таким IMEI уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле
15	Устройство с таким Серийным номером уже есть в системе	Необходимо использовать существующее устройство

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
16	Устройство с таким Ethernet MAC уже есть в системе	Необходимо использовать существующее устройство
17	Данное устройство было удалено из системы	Необходимо обратиться к администратору
18	Нельзя удалить группу, созданную в Active Directory	Невозможно удалить группу, созданную в Active Directory
19	Нельзя удалить непустую группу	Попытка удалить группу с назначенными устройствами или пользователями. Необходимо исключить все дочерние элементы из группы, затем произвести удаление
20	В JSON-файле не указан ID активации (enrollmentID)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным enrollmentID
21	В JSON-файле не указан пароль (password)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным паролем
22	В JSON-файле не указан адрес активации (gatewayURI)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным адресом сервера активации
23	В JSON-файле не указан срок истечения (expiredAt)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с актуальным сроком действия
24	Импорт уже запущен. Дождитесь окончания процесса	Повторная попытка запуска импорта из LDAP при ранее запущенном импорте. Необходимо дождаться завершения выполнения импорта
25	Не удалось создать офлайн-сценарий. Вызов по этому событию уже существует	Попытка создания сценария с существующим событием. Необходимо использовать имеющийся сценарий либо выбрать другое событие
26	Не удалось создать офлайн-сценарий. Сообщите об этой ошибке администратору	Попытка создания сценария с невалидными параметрами. Необходимо обратиться к администратору
27	Корпоративный шаблон уже создан	Предусмотрена возможность создания только 1 корпоративного шаблона. Необходимо использовать шаблон, имеющийся в системе

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
28	Пользователь с указанным Email уже существует	Попытка создать пользователя с существующим Email. Необходимо проверить корректность заполнения поля «Почта рабочая»
29	Группа с таким именем уже существует в системе	Попытка создать группу устройств с существующим наименованием. Необходимо изменить значение в поле «Наименование»
30	Не удалось создать офлайн-сценарий. Пара событие/реакция уже существует	Офлайн-сценарий с заданными событием и реакцией существуют в системе. Необходимо удалить существующий сценарий перед созданием нового либо использовать существующий
31	Редактирование динамических групп не допускается	Динамическая группа не подлежит редактированию
32	Проверьте корректность заполнения правил	Необходимо проверить корректность заполнения правил
33	Политика с таким именем уже существует в системе	Попытка создать политику с существующим наименованием. Необходимо изменить значение в поле «Наименование»
34	Проверьте корректность заполнения названия политики	Попытка создать политику с пустым наименованием. Необходимо заполнить поле «Наименование»
35	Ошибка при разборе файла. Убедитесь, что выбран нужный файл	Необходимо проверить корректность заполненных данных в CSV-файле
36	Некорректная структура файла. Проверьте файл на соответствие шаблону	Необходимо сверить заполненный CSV-файл с установленным шаблоном
37	Файл не содержит данных. Убедитесь, что выбран нужный файл	Необходимо загрузить файл с заполненными данными
38	Некорректная модель устройства	Необходимо проверить корректность заполненных данных в CSV-файле
39	Некорректный статус устройства в системе	Необходимо обратиться к администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
40	Не удалось создать QR-коды	Необходимо повторить попытку позже или обратиться к системному администратору
41	Удаленные устройства привязать к группе не удалось	Дополнительно не предусмотрено выполнение каких-либо действий. Все устройства кроме архивных успешно привязались к группе
42	HTTP ERROR 400	Необходимо очистить кэш и cookies веб-браузера и повторить запрос. В случае повторения ошибки следует обратиться к администратору
43	Интеграция с центром сертификации уже существует	Необходимо использовать существующую интеграцию с центром сертификации или добавить новую с другим центром сертификации
44	Название пусто или больше 256 символов	Необходимо ввести название, содержащее от 1 до 256 символов
45	Проверка формата URL не пройдена	Необходимо ввести электронный адрес в формате URL. Например: https://www.omp.ru/
46	Неподдерживаемый тип сервера	Необходимо указать тип сервера Microsoft Active Directory Certificate Services (AD CS), т.к. Аврора Центр поддерживает интеграцию с центрами сертификации, имеющим данный тип сервера
47	Логин пуст или больше 256 символов	Необходимо ввести логин, содержащий от 1 до 256 символов
48	Пароль пусто или больше 256 символов	Необходимо ввести пароль, содержащий от 1 до 256 символов
49	Ошибка при обработке полученных данных	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее
50	Не удалось удалить настройки интеграции	Необходимо обновить страницу и повторить попытку или обратиться к системному администратору
51	Ошибка сохранения настроек интеграции	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
52	Подключение недоступно	Необходимо нажать «Подробнее», чтобы посмотреть полный текст ошибки (пп. 4.1.4.3.1.1). Обратиться к системному администратору, администратору LDAP или повторить попытку позднее
53	Неверное название территории при создании	Ввести название, содержащее от 1 до 256 символов
54	Неверное количество полигонов при создании территории	Ввести хотя бы один полигон для территории. Количество полигонов не должно превышать 50
55	Неверный идентификатор территории	Обратиться к системному администратору
56	Неверные параметры запроса тайла карты	Обратиться к системному администратору
57	Неверный масштаб запроса тайла карты	Обратиться к системному администратору
58	Ошибка получения тайла карты из источника	Обратиться к системному администратору
59	Тайл карты не найден	Обратиться к системному администратору
60	Название файла не должно быть пустым	Добавить файл с названием не больше 255 символов
61	В названии файла должно быть не больше 255 символов	Добавьте файл с названием не больше 255 символов
62	В названии файла должны быть только буквы, цифры и спецсимволы "-", ".", "_", а также пробелы	Добавить файл, в названии которого только буквы, цифры и спецсимволы "-", ".", "_", а также пробелы
63	Файл с таким именем уже существует в системе	Добавить файл с другим именем
64	Файл не должен быть пустым	Добавить файл с содержанием
65	GIT-репозиторий с таким параметром remote не найден	Проверить правильность введенного адреса до удаленного git-репозитория по протоколу ssh
66	GIT-репозиторий недоступен для аутентификации	Обратиться к системному администратору, администратору GIT-репозитория или повторить попытку позднее
67	Ошибка при валидации длины параметра remote	Обратиться к системному администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
68	Ошибка при валидации допустимых символов параметра remote	Обратиться к системному администратору
69	Ошибка при валидации допустимых значений параметра branch	Обратиться к системному администратору
70	Ошибка при валидации допустимых значений параметра sshKeyID	Обратиться к системному администратору
71	Пара SSH-ключей с таким ID не найдена. Генерация пары SSH-ключей не завершена до конца. Указанный файл не найден	Обратиться к системному администратору и повторить попытку позднее
72	Пара SSH-ключей с таким ID уже используется	Перегенерировать пару SSH-ключей, обновив страницу
73	GIT-репозиторий с таким параметром remote уже существует	Удалить интеграцию с существующим git-репозиторием или создать интеграцию с другим git-репозиторием
74	Ошибка валидации заголовка. Указаны некорректные названия колонок. Правильные названия колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
75	Ошибка валидации заголовка. Указаны не все колонки. Количество колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
76	Ошибка валидации заголовка. Неправильный порядок колонок. Правильный порядок колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта

5.2. Ошибки импорта

5.2.1. Ошибки импорта устройств

Импорт устройств из CSV-файла может проходить с ошибками, описание которых приведено в таблице (Таблица 59).

Таблица 59

№ п/п	Текст ошибки	Действие для устранения ошибки
1	Модель устройства (MODEL_CODE). Ошибка валидации значения. Указанное значение не соответствует названию модели устройства в системе. Ознакомиться с корректными названиями моделей устройств можно в справке об импорте или в справочнике моделей при создании устройства	Указать корректное значение
2	Платформа (PLATFORM). Ошибка валидации значения. Указанное значение не соответствует названию платформы в системе. Ознакомиться с корректными названиями платформ можно в справке об импорте или в предложенном списке платформ при создании устройства	Указать корректное значение
3	Ошибка привязки устройства к группе. Указанная в файле группа является динамической группой в системе. К динамической группе нельзя привязывать устройства. Укажите другое название группы в файле	Указать другое название группы в файле
4	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
5	Ошибка импорта группы. Группа с таким названием была помещена в архив. Восстановить ее невозможно, поэтому необходимо использовать другое название группы	Указать другое название группы в файле
6	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
7	SN. Ошибка валидации значения. SN необходимо переписать из параметров устройства	Указать корректное значение
8	Ethernet MAC. Ошибка валидации значения. Ethernet необходимо переписать из параметров устройства	Указать корректное значение
9	WLAN MAC. Ошибка валидации значения. WLAN MAC необходимо переписать из параметров устройства	Указать корректное значение
10	Ошибка импорта устройства. Устройство с таким идентификатором было помещено в архив. Необходимо найти его в архиве и восстановить	Найти устройство в архиве и восстановить
11	Ошибка импорта устройства. В системе найдено устройство по одному из идентификаторов, но другие идентификаторы не совпадают. Найдите устройство в системе и проверьте указанные в файле данные на соответствие	Найти устройство в системе и проверить на соответствие указанных в файле данных
12	Ошибка валидации строки. Система не смогла распознать содержимое строки. Проверьте корректность заполнения данных, воспользовавшись рекомендациями в справке об импорте	Проверить корректность заполнения данных (пп. 2.2.3.1, пп. 2.3.3.1)
13	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Заполнить файл данными
14	Ошибка импорта устройства. Количество значений в строке не равно количеству колонок в заголовке. Разделители должны соответствовать разделителям первой строки	Необходимо проверить корректность заполненных данных в CSV-файле. Разделители должны соответствовать разделителям первой строки
15	Комментарий (COMMENT). Ошибка валидации значения. Длина должна быть до 512 символов	Длина должна быть до 512 символов

№ п/п	Текст ошибки	Действие для устранения ошибки
16	Ошибка привязки устройства к группе. Указанная в стратегии импорта группа удалена из системы. Устройство было добавлено в группу, указанную в файле. Если в файле отсутствовала группа, тогда устройство находится в системе без группы	Указать корректную группу
17	Ошибка импорта устройства. Указано слишком много идентификаторов одного типа. Идентификаторов одного типа должно быть не более 10	Указать не более 10 идентификаторов в файле
18	Ошибка импорта устройства. Указано слишком много идентификаторов одного типа для существующего устройства. Идентификаторов одного типа должно быть не более 10	Указать не более 10 идентификаторов в файле
19	Ошибка импорта устройства. Указаны дублирующиеся идентификаторы	Исключить дублирующие идентификаторы из файла
20	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Указать корректное значение

5.2.2. Ошибки импорта пользователей

Импорт пользователей из CSV-файла может проходить с ошибками, описание которых приведено в таблице (Таблица 60).

Таблица 60

№ п/п	Текст ошибки	Действие для устранения ошибки
1	Ошибка поиска устройства. Указанные данные идентификаторов некорректны, либо по ним не удалось найти устройство	Указать корректное значение или добавить устройство в систему, в случае его отсутствия
2	Имя (FIRST_NAME). Ошибка валидации значения. Имя может содержать: а-я ё а-z А-Я Ё А-Z - ' пробел	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
3	Фамилия (LAST_NAME). Ошибка валидации значения. Фамилия может содержать: а-я ё а-z А-Я Ё А-Z - ' пробел	Указать корректное значение
4	Отчество (PATRONYMIC). Ошибка валидации значения. Отчество может содержать: а-я ё а-z А-Я Ё А-Z - ' пробел	Указать корректное значение
5	Электронная почта (EMAIL). Ошибка валидации значения. Электронная почта состоит из двух частей (логина пользователя и доменного имени сервера), разделённых символом «@». Пример: example@example.ru	Указать корректное значение
6	Должность (JOB_TITLE). Ошибка валидации значения. Должность может содержать: а-я ё а-z А-Я Ё А-Z - пробел	Указать корректное значение
7	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Номер телефона должен состоять из цифр	Указать корректное значение
8	Имя (FIRST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
9	Фамилия (LAST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
10	Отчество (PATRONYMIC). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
11	Электронная почта (EMAIL). Ошибка валидации значения. Длина должна быть от 1 до 256 символов	Длина должна быть от 1 до 256 символов
12	Должность (JOB_TITLE). Ошибка валидации значения. Длина должна быть от 2 до 256 символов	Длина должна быть от 2 до 256 символов
13	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов

№ п/п	Текст ошибки	Действие для устранения ошибки
14	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
15	WLAN MAC. Ошибка валидации значения. WLAN MAC необходимо переписать из параметров устройства	Указать корректное значение
16	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Указать корректное значение
17	Ethernet MAC. Ошибка валидации значения. Ethernet необходимо переписать из параметров устройства	Указать корректное значение
18	SN. Ошибка валидации значения. SN необходимо переписать из параметров устройства	Указать корректное значение
19	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Заполнить файл данными
20	Ошибка импорта. Файл содержит только заголовок. Файл должен быть заполнен данными	Заполнить файл данными
21	Ошибка импорта пользователя. Количество значений в строке не равно количеству колонок в заголовке. Разделители должны соответствовать разделителям первой строки	Разделители должны соответствовать разделителям первой строки
22	Ошибка импорта пользователя. Пользователь получен из LDAP, изменение его данных недоступно. Для продолжения импорта удалите данную строку из файла	Для продолжения импорта необходимо удалить данную строку из файла
23	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Указать корректное значение

5.3. Ограничения

В ходе работы с ПУ могут быть выделены различные ограничения в работе системы, информация о которых приводится в документе «Release Notes», расположенном на веб-сайте: <https://auroraos.ru/documentation/>.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 61).

Таблица 61

Термин/ Сокращение	Расшифровка
ОС	Операционная система
Офлайн-сценарий	Правило, которое отправляется с указанием события срабатывания на устройства и должно «мгновенно» примениться по этому событию (в том числе, если в этот момент нет связи с сервером)
ПБ	Подсистема безопасности
ПМ	Подсистема «Маркет»
ПО	Программное обеспечение
ПООС	Подсистема обновления ОС
ППО	Прикладное программное обеспечение «Аврора Центр»
Приложение	Приложением является: <ul style="list-style-type: none"> – мобильное приложение, функционирующее под управлением ОС Аврора/ОС Android; – приложение для ЭВМ, функционирующей под управлением ОС семейства Linux
ПУ	Подсистема Платформа управления
СУА	Сервис уведомлений Аврора
Устройство	Под устройством подразумевается мобильное устройство и/или ЭВМ, на которой функционируют соответствующие компоненты ППО
Чекбокс	Элемент управления, предоставляющий возможность осуществить выбор, а также вызвать список быстрых действий
ЭВМ	Электронно-вычислительная машина
Bluetooth®	Стандарт беспроводной связи, обеспечивающий обмен данными между устройствами на основе ультракоротких радиоволн
BSSID	Basic Service Set Id – 48-битный идентификационный номер в беспроводных сетях стандарта IEEE 802.11
CSV	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
Fingerprint	Цифровой отпечаток (информация, собранная об удаленном устройстве для дальнейшей идентификации)

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), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом
IMEI	Уникальный номер устройства, состоящий из 15 цифр
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
MTP	Media Transfer Protocol – основанный на PTP аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к ЭВМ
Push-уведомления	Текстовые сообщения, предназначенные для оперативной (мгновенной) доставки на устройство пользователей
QR-код	Quick response code – код быстрого реагирования, матричный код (двумерный штрихкод)
SSID	Service Set Identifier – символьное название беспроводной точки доступа Wi-Fi, служащее для идентификации ее среди других точек пользователями или устройствами, подключающимися к сети
WLAN	Wireless Local Area Network – локальная сеть, построенная на основе беспроводных технологий

Описание используемых значков

Значок	Описание
Модель устройства	
	– смартфон Аврора; – защищенный смартфон Аврора
	– планшет Аврора; – защищенный планшет Аврора
	– смартфон Android; – защищенный смартфон Android
	– планшет Android; – защищенный планшет Android
	Неизвестная модель устройства Android
	КПК Аврора
	КПК Android
	ПК Linux
	Неизвестная модель устройства Аврора
	Неизвестная модель устройства Android
	Неизвестная модель устройства Linux
Тип устройства	
	Устройство, клиент АЦ установлен
	Устройство, нет данных о Клиенте
	Устройство, клиент АЦ удален
Тип группы устройств	
	Динамическая группа. ПРИМЕЧАНИЕ. Группа, в которую устройства добавляются автоматически согласно выбранному алгоритму добавления
	Статическая группа
Тип пользователя	
	Пользователь. ПРИМЕЧАНИЕ. Добавляется в ПУ вручную или с помощью импорта CSV-файла
	Пользователь из орг.подразделения. ПРИМЕЧАНИЕ. Пользователь, полученный из LDAP

Значок	Описание
Тип группы пользователей	
	Группа пользователей. ПРИМЕЧАНИЕ. Создается вручную или с помощью импорта CSV-файла
	Организационное подразделение. ПРИМЕЧАНИЕ. Группа пользователей, полученная из LDAP
	Динамическая группа. ПРИМЕЧАНИЕ. Группа пользователей, полученная по дополнительным атрибутам из LDAP
Статус жизненного цикла	
	Зарегистрировано. ПРИМЕЧАНИЕ. Устройство, добавленное в ПУ
	В процессе активации. ПРИМЕЧАНИЕ. Сгенерирован QR-код для устройств
	Активировано. ПРИМЕЧАНИЕ. Устройство активировано
	Очищено. ПРИМЕЧАНИЕ. Устройство очищено (сброшено к заводским настройкам)
	Архивное. ПРИМЕЧАНИЕ. Устройство архивировано (удалено)
Соответствие назначенной политике	
	Соответствует политике. ПРИМЕЧАНИЕ. Устройство активировано и соответствует назначенным политикам
	Не соответствует политике. ПРИМЕЧАНИЕ. Устройство активировано и не соответствует хотя бы 1 назначенной политике
	Не управляется. ПРИМЕЧАНИЕ. Устройство не управляется ПУ
	Управление политиками доступно только для активированных устройств
Тип сообщения о событии	
	Информационное
	Предупреждение
	Критическое
	Отладочное

Рекомендации по конвертации CSV-файла в книгу Excel

Для успешной конвертации экспортированного CSV-файла (п. 2.2.5) в книгу Excel необходимо выполнить следующие действия:

- открыть CSV-файл с помощью MS Excel;
- перейти во вкладку «Данные» (Рисунок 2.1);
- на панели инструментов выбрать «Получить данные»;
- в раскрывающемся списке выбрать «Из файла», далее «Из текстового/CSV-файла»;

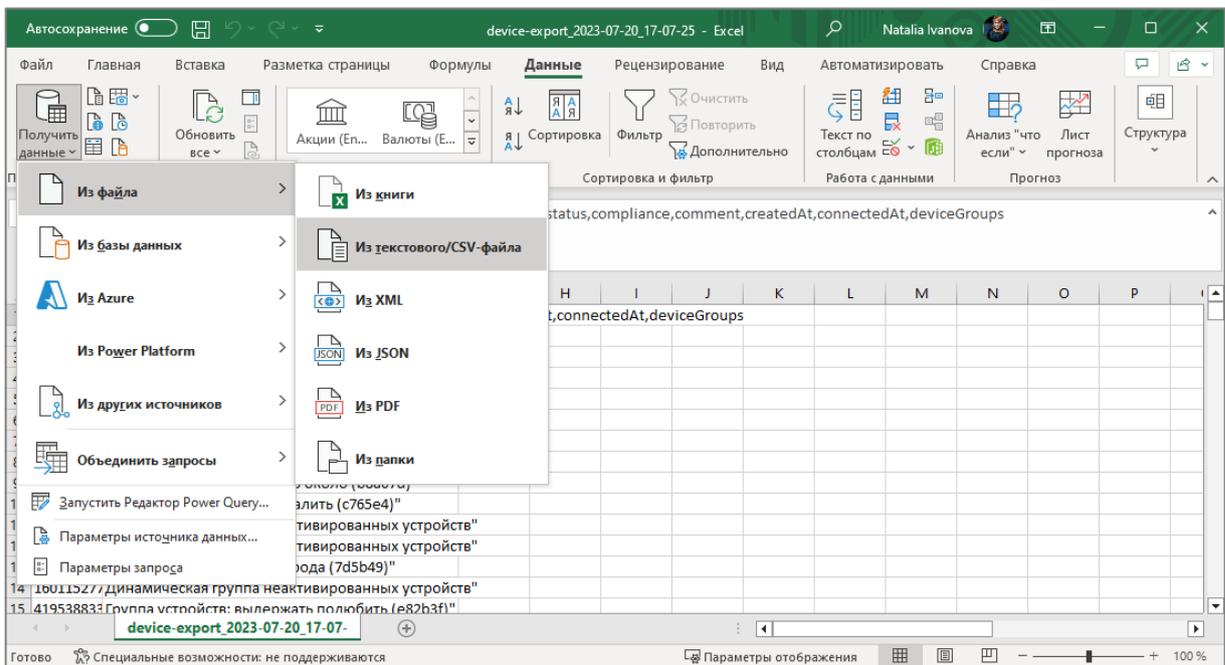


Рисунок 2.1

- выбрать файл экспорта и нажать кнопку «Импорт» (Рисунок 2.2);

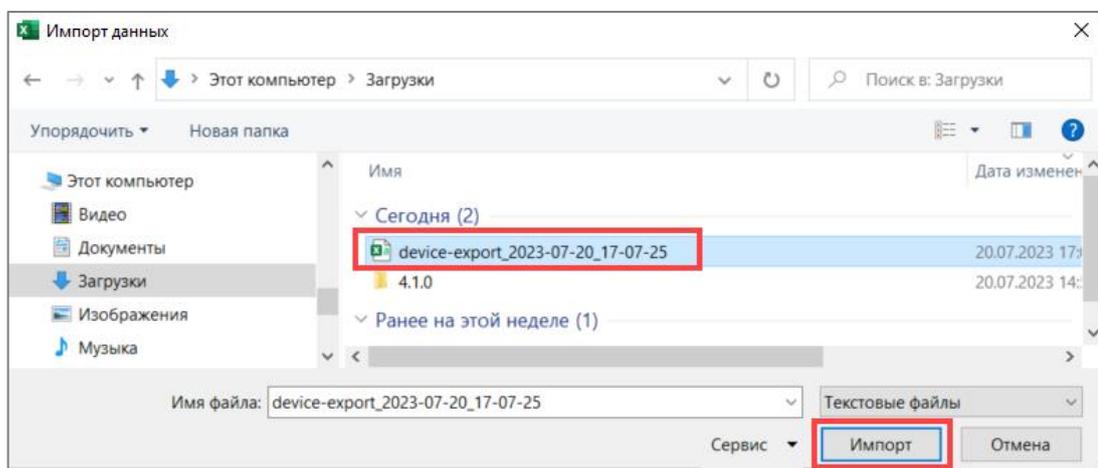


Рисунок 2.2

– убедиться, что в поле «Разделитель» выбрано значение «Запятая», и нажать на кнопку «Преобразовать данные» (Рисунок 2.3);

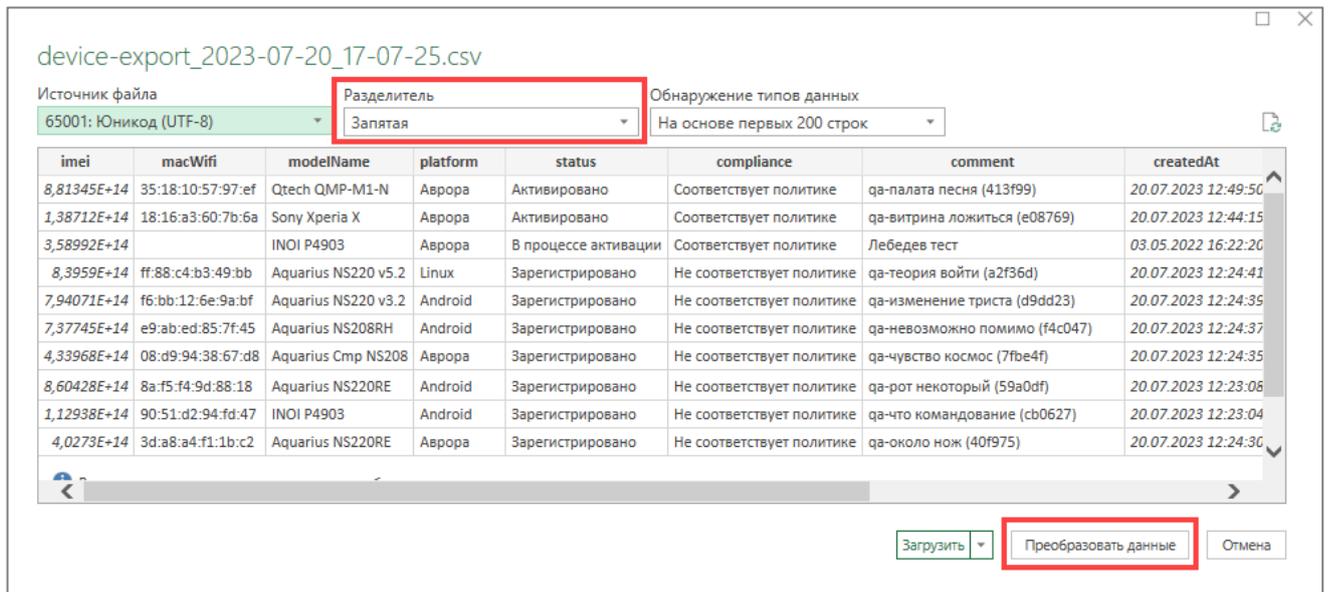


Рисунок 2.3

– убедиться, что в столбце «deviceGroups» отображаются связки групп (группы, перечисленные через точку с запятой) (Рисунок 2.4);

– нажать «Закреть и загрузить».

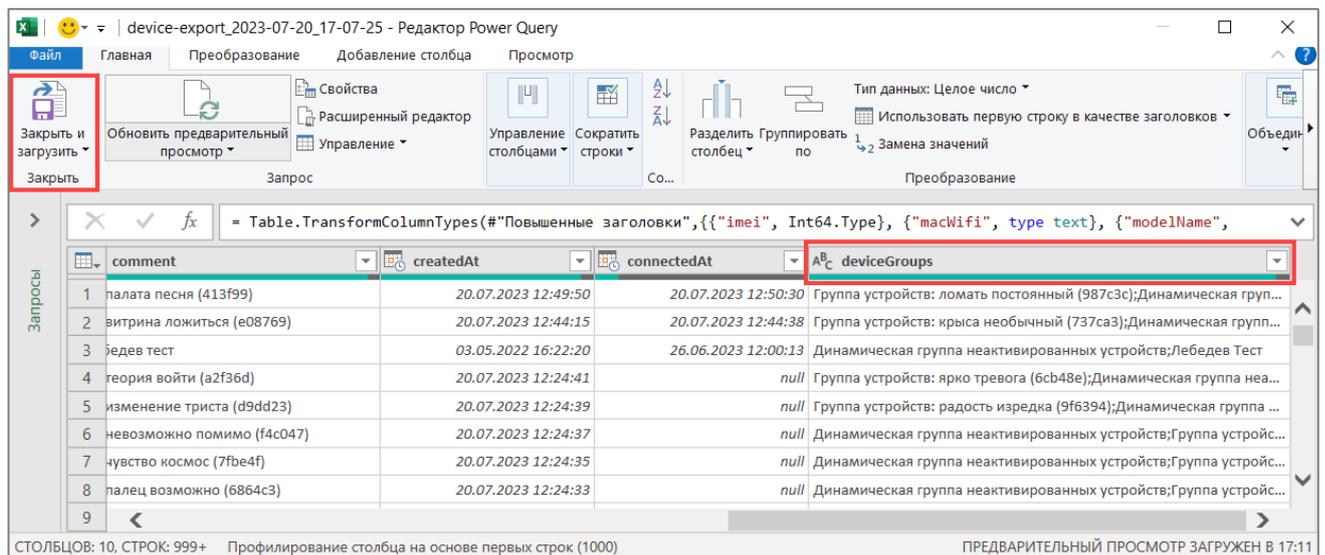


Рисунок 2.4

В результате отобразится книга Excel, сконvertированная из CSV-файла экспорта.

Если необходимо отфильтровать устройства по группе, то необходимо:

- нажать на значок фильтра справа от названия столбца (Рисунок 2.5 [1]);
- ввести название группы;
- выбрать все результаты, содержащие название группы (Рисунок 2.5 [2]);
- нажать кнопку «ОК» (Рисунок 2.5 [3]).

The screenshot shows the Microsoft Excel interface with a table containing data from a device export. The table has columns for 'comment', 'createdAt', 'connectedAt', and 'deviceGroups'. A search filter is applied to the 'deviceGroups' column, and a search results dialog is open, showing a list of filtered items. Red boxes and numbers 1, 2, and 3 highlight the search input, the list of results, and the 'OK' button respectively.

	F	G	H	I	J	K
	comment	createdAt	connectedAt	deviceGroups		
2	qa-палата песня (413f99)	20.07.2023 12:49	20.07.2023 12:50	Группа устройств: ломать постоянный (987c3c);Динамическая группа неактивированных устройств		
3	qa-витрина ложиться (e08769)	20.07.2023 12:44	20.07.2023 12:44	Группа устройств: крыса необычный (737ca3);Динамическая группа неактивированных устройств		
4	qa-Лебедев тест	03.05.2022 16:22	26.06.2023 12:00	Динамическая группа неактивированных устройств		
5	qa-теория войти (a2f36d)	20.07.2023 12:24		Группа устройств: ярко тревога (6cb48e);Динамическая группа неактивированных устройств		
6	qa-изменение триста (d9dd23)	20.07.2023 12:24		Группа устройств: радость изредка (9f6394);Динамическая группа неактивированных устройств		
7	qa-невозможно помимо (f4cd47)	20.07.2023 12:24		Динамическая группа неактивированных устройств		
8	qa-чувство космос (7fbc4f)	20.07.2023 12:24		Динамическая группа неактивированных устройств		
9	qa-палец возможно (6864c3)	20.07.2023 12:24		Динамическая группа неактивированных устройств		
10	qa-полностью прежний (9d634a)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
11	qa-естественный пересечь (86214c)	20.07.2023 12:23		Группа устройств: стель беспомощный (937d62);Динамическая группа неактивированных устройств		
12	qa-хозяйка грустный (152d6b)	20.07.2023 12:23		Группа устройств: актриса пламя (87e307);Динамическая группа неактивированных устройств		
13	qa-целочка палка (50cf20)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
14	qa-плод число (13eddc)	20.07.2023 12:24		Группа устройств: инфекция торговля (877c8b);Динамическая группа неактивированных устройств		
15	qa-сверхающий зато (3fb233)	20.07.2023 12:24		Динамическая группа неактивированных устройств		
16	qa-правление граница (ee2714)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
17	qa-преьера равнодушный (d74710)	20.07.2023 12:23		Группа устройств: сынок трубка (d34ea0);Динамическая группа неактивированных устройств		
18	qa-один штаб (882237)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
19	qa-рот некоторый (59a0df)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
20	qa-что командование (cb0627)	20.07.2023 12:23		Группа устройств: зима заработать (cc550d);Динамическая группа неактивированных устройств		
21	qa-около нож (40f975)	20.07.2023 12:24		Динамическая группа неактивированных устройств		
22	qa-запретить освобождение (e808ce)	20.07.2023 12:23		Группа устройств: горький интеллектуальн (265d);Динамическая группа неактивированных устройств		
23	qa-полоска горький (309317)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
24	qa-приходить дорогой (a9d2de)	20.07.2023 12:24		Группа устройств: спась деловой (d49763);Динамическая группа неактивированных устройств		
25	qa-низкий оставить (ed8ac7)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
26	qa-идея полоска (4445ae)	20.07.2023 12:23		Динамическая группа неактивированных устройств		
27	qa-выкинуть медицина (a11a3f)	20.07.2023 12:23		Группа устройств: порядок инии (02d0bc);Динамическая группа неактивированных устройств		
28	qa-остановить поколение (9603d6)	20.07.2023 12:24		Динамическая группа неактивированных устройств;Группа устройств: художественный выкинут (930a);Динамическая группа неактивированных устройств		
29	qa-исключительный этап (0a79a1)	20.07.2023 12:23		Группа устройств: умирать способ (106817);Динамическая группа неактивированных устройств;Группа устройств: cnopt cnaлит (c765a4)		

Рисунок 2.5

Особенности выполнения скриптов на устройстве

Чтобы скрипт запустился, он должен обязательно иметь shebang.

Для ОС семейства Linux скрипт запускается как исполняемый файл (равносильно вызову `./script.sh`).

Для ОС Android скрипт запускается через интерпретатор. Например, если в shebang указана строка `#!/usr/bin/env sh`, то полная команда запуска будет выглядеть:

```
/usr/bin/env sh script.sh
```

Для ОС семейства Linux скрипты запускаются с правами суперпользователя (root).

Для ОС Android скрипты запускаются с правами текущего (непривилегированного) пользователя.

Скрипты позволяют вернуть произвольный результат выполнения в виде строки, которая отобразится в состоянии карточки устройства. Этот результат можно использовать для формирования динамических групп.

Чтобы вернуть результат из скрипта, необходимо записать строку в файл, путь до которого передается в переменной окружения:

```
__OMP_SCRIPT_RESULT_FILE__.
```

ПРИМЕЧАНИЕ. Из файла считывается не более 64 ASCII-символов.

Пример скрипта на Bash для ОС семейства Linux:

```
#!/usr/bin/env sh
echo -n "Hello world!" > "${__OMP_SCRIPT_RESULT_FILE__}"
```

где:

- `-n` убирает `\n` в конце строки;
- кавычки и фигурные скобки вокруг имени переменной предотвращают ошибку `ambiguous redirect`.

Пример скрипта на Python:

```
#!/usr/bin/env python3 import os
resultFile = open(os.environ["__OMP_SCRIPT_RESULT_FILE__"], "w")
resultFile.write("Hello world!")
resultFile.close()
```

Пример скрипта на Bash для ОС Android:

```
#!/system/bin/env sh
echo -n "Hello world!" > "${__OMP_SCRIPT_RESULT_FILE__}"
```

где: `"sh"` или `"bash"` в конце строки по наличию в ОС Android.

Также допустимо использовать в shebang: `#!/usr/bin/env` вместо `#!/system/bin/env` (произойдет автоматическая замена).

Подготовка устройства на базе ОС Android к удаленному подключению

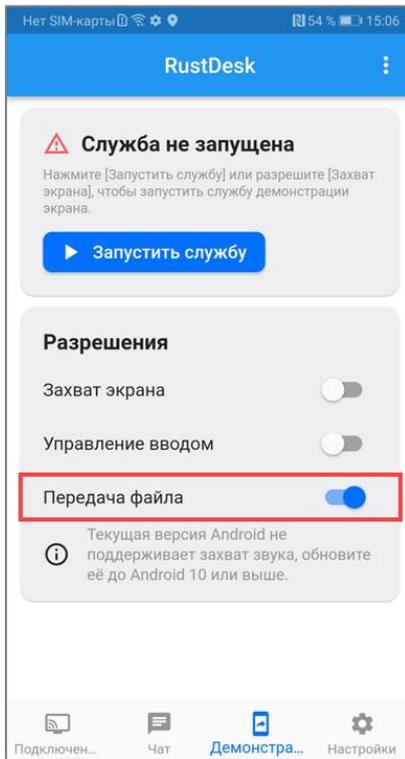


Рисунок 4.1

Для удаленного подключения к рабочему столу устройства необходимо вручную выдать требуемые разрешения приложению RustDesk на устройстве.

Для этого пользователю на устройстве необходимо выполнить следующие действия:

- 1) Открыть приложение RustDesk;
- 2) Убедиться, что разрешение на передачу файлов выдано (Рисунок 4.1). Это разрешение выдается автоматически при запуске удаленного подключения из ПУ.

ПРИМЕЧАНИЕ. Если по какой-либо причине (например, из-за особенности некоторых версий ОС Android) это разрешение не выдано, то необходимо:

- перевести переключатель «Передача файла» в положение «Включено»;
- коснуться кнопки «Разрешить», если ОС Android запросит подтверждение;
- 3) Выдать разрешение на управление вводом. Для этого необходимо:
 - перевести переключатель «Управление вводом» в положение «Включено» (Рисунок 4.2);
 - перейти в системные настройки (Рисунок 4.3);

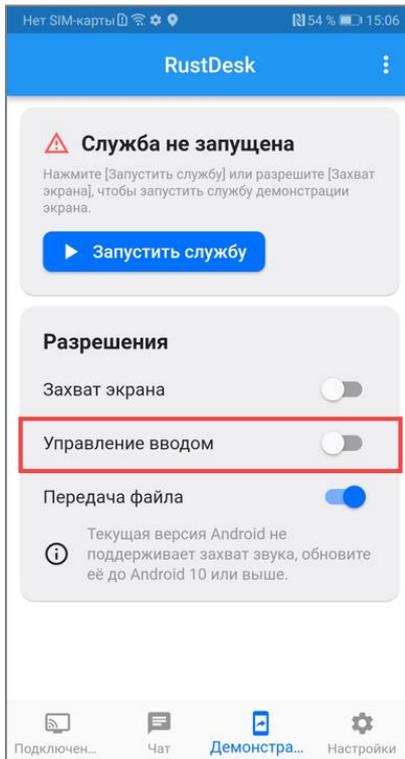


Рисунок 4.2

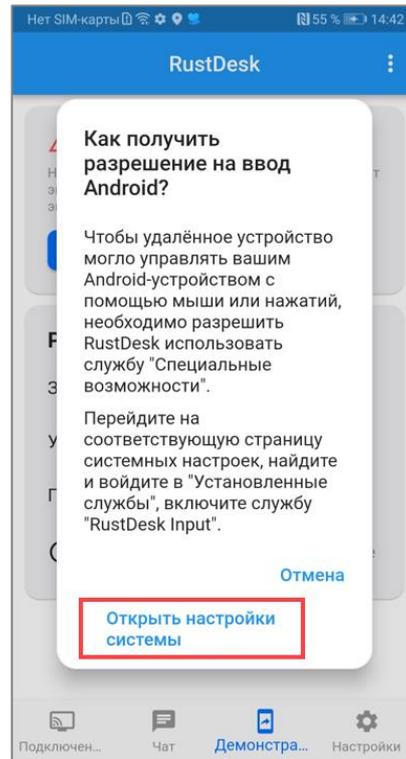


Рисунок 4.3

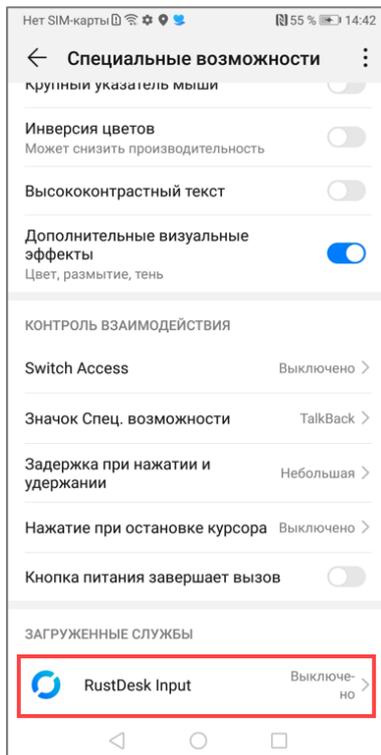


Рисунок 4.4

– коснуться RustDesk Input (Рисунок 4.4), перевести переключатель RustDesk Input в положение «Включено» (Рисунок 4.5) и подтвердить включение (Рисунок 4.6).

ПРИМЕЧАНИЕ. Разрешение на управление вводом выдается единожды, положение переключателя будет сохранено для последующих запусков приложения RustDesk;

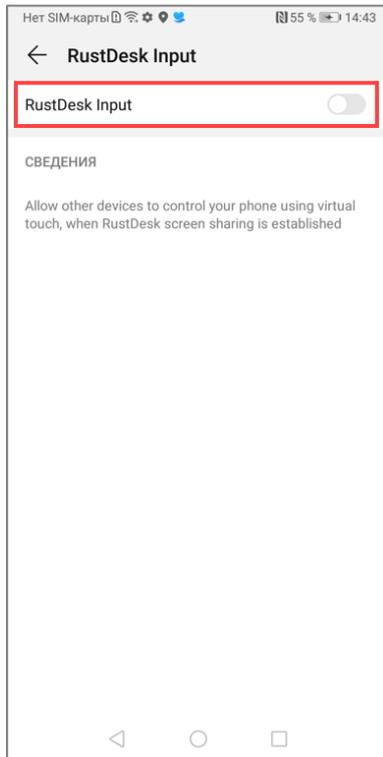


Рисунок 4.5

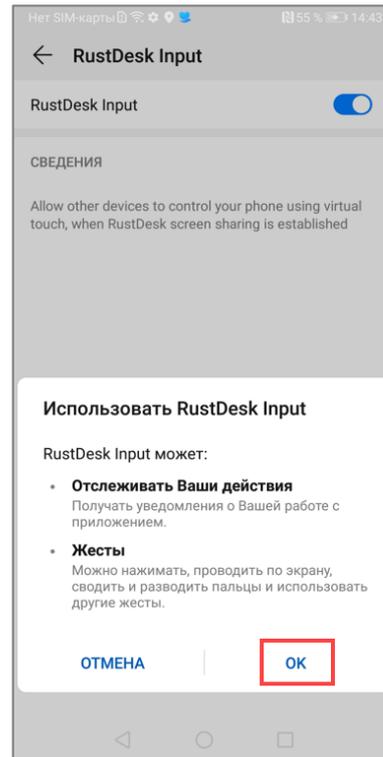


Рисунок 4.6

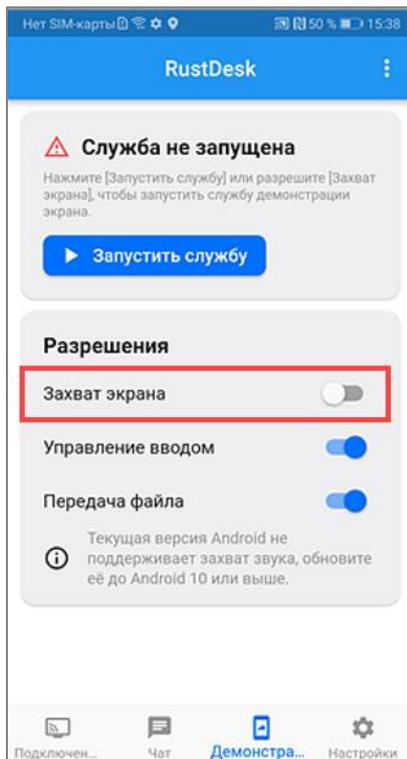


Рисунок 4.7

4) Выдать разрешение на захват экрана (применимо для ОС Android версий 7-9). Для этого необходимо:

– перевести переключатель «Захват экрана» в положение «Включено» (Рисунок 4.7);

АДМГ.20134-01 90 01-3

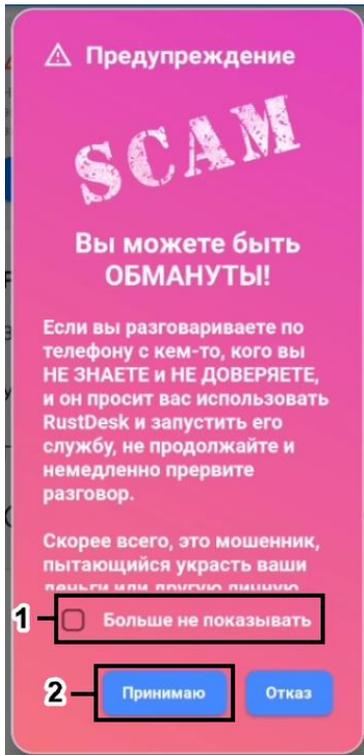


Рисунок 4.8

– ознакомиться с предупреждением о возможном мошенничестве (Рисунок 4.8);

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 4.8 [1]) и выбрать «Принимаю» (Рисунок 4.8 [2]);

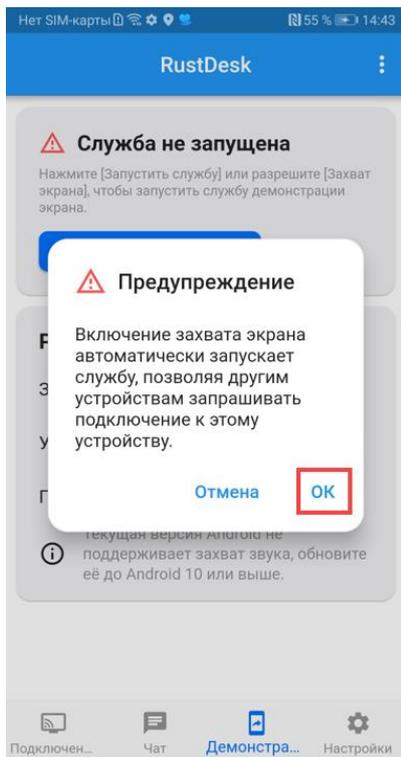


Рисунок 4.9

– ознакомиться с предупреждением, что включение захвата экрана автоматически запускает приложение RustDesk, и коснуться «ОК» (Рисунок 4.9);

АДМГ.20134-01 90 01-3

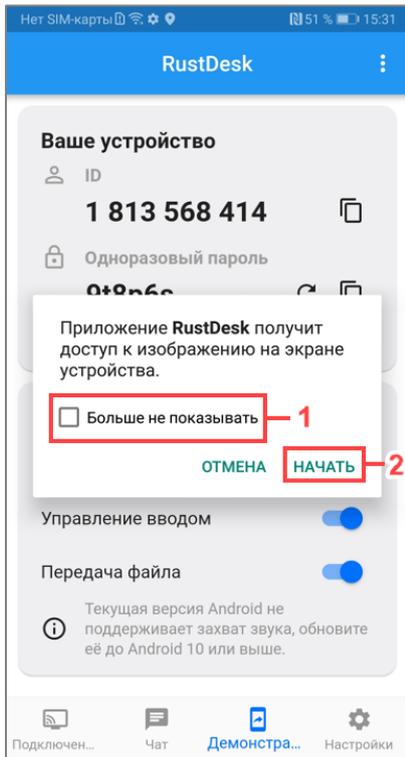


Рисунок 4.10

ПРИМЕЧАНИЯ:

- ✓ Включение захвата экрана и службы RustDesk выполняется при удаленном подключении к устройству из ПУ;
- ✓ На устройствах с ОС Android версии 10 и выше при каждом удаленном подключении к устройству из ПУ необходимо подтверждать включение захвата экрана и службы RustDesk (Рисунок 4.11).

Исключение: подключение без подтверждения пользователя будет происходить, если на устройстве установлена сборка, подписанная подписью производителя (подробнее в пп. 2.1.1.7).



Рисунок 4.11

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 4.10 [1]) и коснуться «Начать» (Рисунок 4.10 [2]).

В результате устройство будет готово к удаленному подключению.

Процесс сбора и отправки системных сообщений на Email

Последовательность этапов сбора и отправки системных сообщений приведена на рисунке (Рисунок 5.1) и указана цифрами.

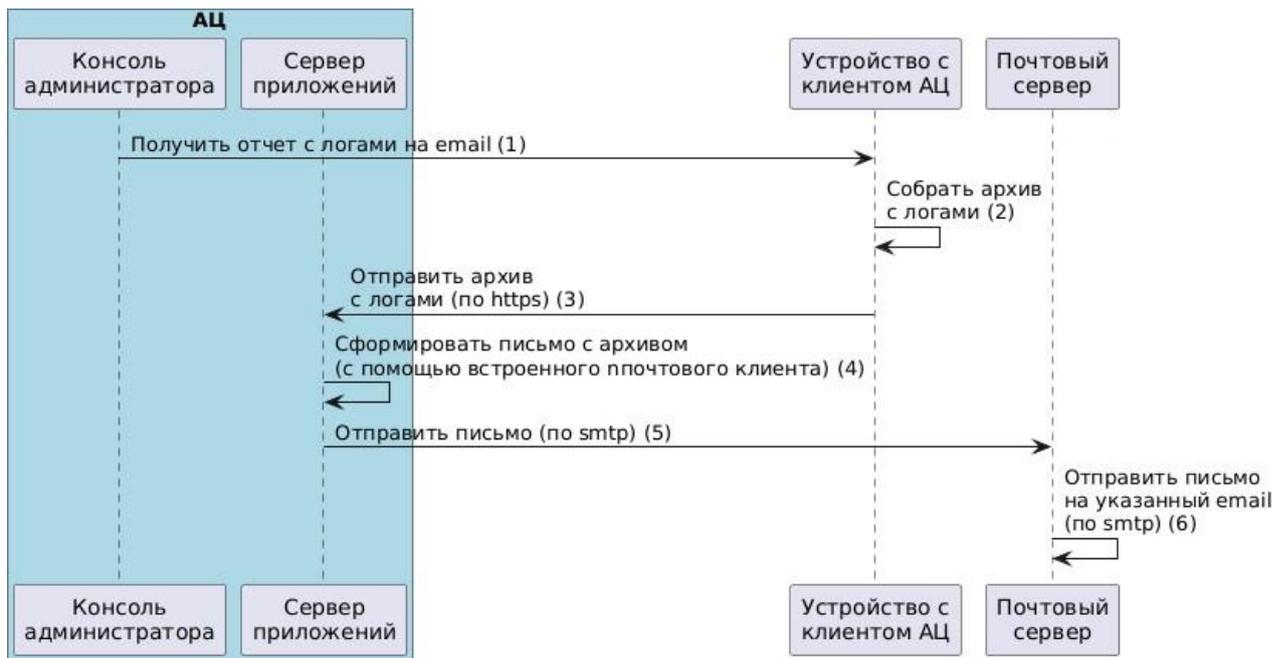


Рисунок 5.1

Описание процесса:

1) Администратор Платформы управления отправляет на устройство команду оперативного управления по сбору отчета с системными ошибками, в которой указывает email адресата;

2) Устройство получает команду, запускает сбор системных ошибок, помещает их в архив;

3) Устройство отправляет архив на сервер приложений;

4) Сервер приложений получает архив во временную область хранения, с помощью встроенного почтового клиента формирует письмо с архивом;

5) Сервер приложений пытается сразу же отправить его на почтовый сервер. Некоторая область памяти используется для пересылки, но дальше логи нигде не хранятся;

6) В случае:

- успешной отправки сервер приложений информирует приложение «Аврора Центр», что системные ошибки отправлены. Далее почтовый сервер пересылает письмо на email, который был указан в команде оперативного управления;

- неуспешной отправки сервер приложений информирует приложение «Аврора Центр» об ошибке загрузки. Далее системные ошибки никуда не уходят. Ошибка отправки фиксируется в системных ошибках устройства.

