ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Прикладное программное обеспечение «Аврора Центр» релиз 5.0.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Часть 3

Подсистема Платформа управления

Версия 1.2

Листов 270

2024

АННОТАЦИЯ

Настоящий документ является третьей частью руководства пользователя Прикладного программного обеспечения «Аврора Центр» (далее – ППО) релиз 5.0.0 и содержит описание функционирования подсистемы Платформа управления (ПУ), входящей в состав ППО.

ППО является прикладным программным обеспечением, предназначенным для:

– управления устройствами[1], а также приложениями[2] и их жизненным циклом;

– отправки push-уведомлений на устройства;

– (обновления операционной системы (ОС) Аврора) 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 Аврора и не гарантирует их успешного завершения.

ПРИМЕЧАНИЯ:

✓ Подробная информация о составе и назначении ППО, а также требования к условиям выполнения приведены в документе «Руководство администратора»;

✓ Подробная информация об особенностях резервного копирования приведена в документе «Рекомендации по резервному копированию».

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

– «Руководство пользователя. Часть 1. Подсистема безопасности»;

– «Руководство пользователя. Часть 2. Подсистема «Маркет»;

– «Руководство пользователя. Часть 3. Подсистема Платформа управления»;

– «Руководство пользователя. Часть 4. Подсистема управления тенантами»;

– «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений».

ПРИМЕЧАНИЕ. Состав разделов интерфейса ППО зависит от вариантов поставки[3].

Описание работы приложений приведено в документах:

– «Руководство пользователя. Часть 6. Приложение «Аврора Маркет» для операционной системы Аврора»;

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 8. Приложение «Аврора Маркет» для операционной системы Android»;

[1] Определение термина «Устройство» приведено в таблице (Таблица 53).

[2] Определение термина «Приложение» приведено в таблице (Таблица 53).

[3] Комплектность вариантов поставки определяется условиями Лицензионного договора.

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;

– «Руководство пользователя. Часть 10. Приложение «Аврора Маркет» для операционных систем семейства Linux»;

– «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

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 10
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 22
2.1. Общее описание карточек элементов управления 22
2.1.1. Работа с карточкой устройства 22
2.1.2. Работа с карточкой группы устройств 50
2.1.3. Работа с карточкой пользователя 54
2.1.4. Работа с карточкой группы пользователей 58
2.1.5. Работа с карточкой политики 62
2.1.6. Работа с карточкой офлайн-сценария 65
2.2. Подраздел «Устройства» 67
2.2.1. Добавление устройства в ПУ 69
2.2.2. Добавление группы устройств вручную 72
2.2.3. Добавление устройств или группы устройств с помощью CSV-файла 76
2.2.4. Добавление приглашения на самостоятельную регистрацию устройства 85
2.2.5. Экспорт списка устройств в CSV-файл 89
2.2.6. Привязка устройства к пользователю 90
2.2.7. Привязка устройств к группе устройств 92
2.2.8. Активация устройств 95
2.2.9. Применение оперативных команд 108
2.2.10. Отвязка (исключение) устройств из группы устройств 112
2.2.11. Архивирование устройства 114
2.2.12. Восстановление устройств из архива 117
2.2.13. Удаление группы устройств 119
2.2.14. Очистка устройств до заводских настроек 120
2.2.15. Вывод устройства из эксплуатации 120
2.3. Подраздел «Пользователи» 121
2.3.1. Добавление пользователя устройства вручную 123
2.3.2. Добавление группы пользователей вручную 124

2.3.3. Добавление пользователей или группы пользователей с помощью CSV-файла 126
2.3.4. Привязка пользователей к группе пользователей 135
2.3.5. Привязка пользователей к устройствам 139
2.3.6. Архивирование пользователя 141
2.3.7. Удаление группы пользователей 142
2.4. Подраздел «Политики» 143
2.4.1. Общее описание правил политик 150
2.4.2. Добавление политики вручную 172
2.4.3. Добавление политики на основе корпоративного шаблона 174
2.4.4. Добавление политики на основе существующей 177
2.4.5. Редактирование правила политики 178
2.4.6. Назначение политики на группы устройств или группы пользователей .. 181
2.4.7. Отвязка политики от группы устройств или группы пользователей 184
2.4.8. Удаление политики 186
2.5. Подраздел «Сценарии» 187
2.5.1. Добавление офлайн-сценария 190
2.5.2. Назначение офлайн-сценария на группы устройств или группы пользователей 194
2.5.3. Отвязка офлайн-сценарий от группы устройств/группы пользователей ... 197
2.5.4. Удаление офлайн-сценария 199
2.6. Подраздел «Файлы» 201
2.6.1. Добавление файла (скрипта) 201
2.6.2. Доставка файла и выполнение скрипта на устройстве с помощью ПУ 201
2.6.3. Удаление файла (скрипта) 202
3. Работа в разделе «Мониторинг» Консоли администратора ПУ 204
3.1. Подраздел «Индикаторы» 204
4. Работа в разделе «Администрирование» Консоли администратора ПУ 208
4.1. Подраздел «Настройки» 208
4.1.1. Доверенные сертификаты 209
4.1.2. Категории пользовательских сертификатов 211
4.1.3. Архивные устройства 214
4.1.4. Интеграция (информация о серверах) 214
4.1.5. Ссылка на приложение «Аврора Центр» для ОС Android 231
4.1.6. Территории 232
4.2. Подраздел «Орг.структура» 234
5. Сообщения об ошибках и ограничения 235
5.1. Сообщения об ошибках 235
5.2. Ошибки импорта 244
5.2.1. Ошибки импорта устройств 244
5.2.2. Ошибки импорта пользователей 246
5.3. Ограничения 249

Перечень терминов и сокращений..... 257
Приложение 1..... 259
Приложение 2..... 261
Приложение 3..... 264
Приложение 4..... 265

1. ПОДГОТОВКА К РАБОТЕ

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

✓ Наличие веб-браузера с поддержкой технологий: TLS, CSS3, HTML5, ECMAScript 5 и Cookie. Рекомендуется использовать веб-браузер Chrome версии 90 или выше;

✓ Разрешение экрана монитора 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, 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».

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).

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».

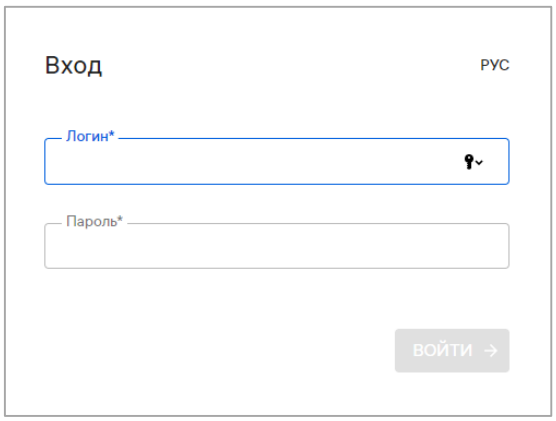

Рисунок 1

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».

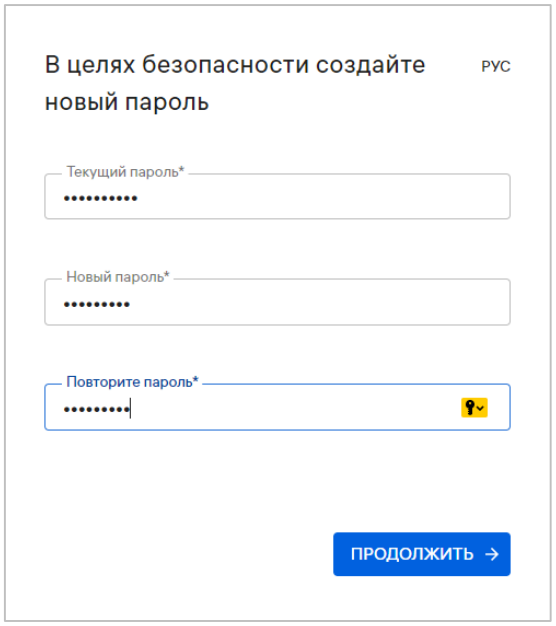

Рисунок 2

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 2 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.

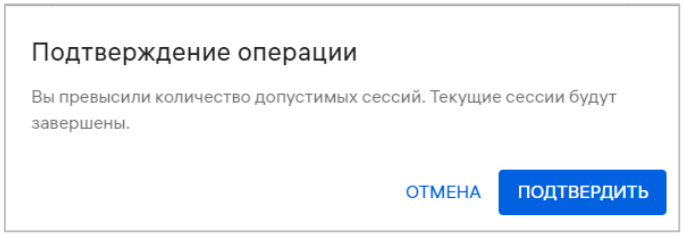

Рисунок 3

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 поставки[4] ППО состав разделов верхней панели интерфейса ППО может отличаться.

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

[4] Комплектность вариантов поставки определяется условиями Лицензионного договора.

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 3.1);

– «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);

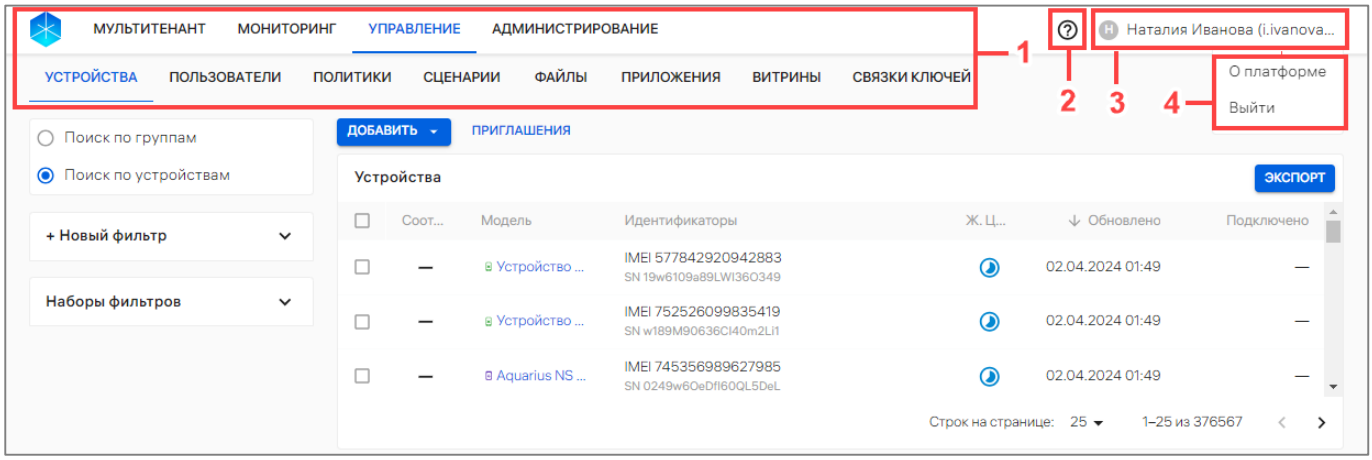

Рисунок 4

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

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

– имя;

– фамилия;

– Email;

4) Выбирать соответствующие пункты из раскрывающегося списка нажатием значка[5] в меню пользователя (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 «Закрыть» (Рисунок 5 [3]) для выхода из раздела «О платформе»;

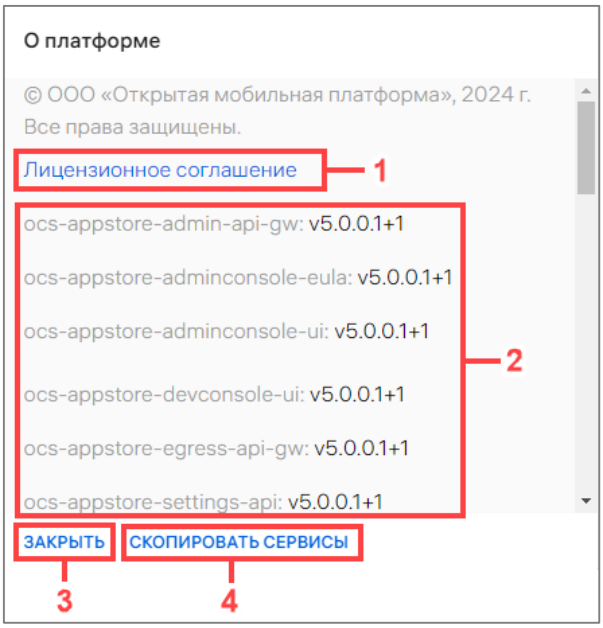

Рисунок 5

– «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);

– 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;

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

– 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.

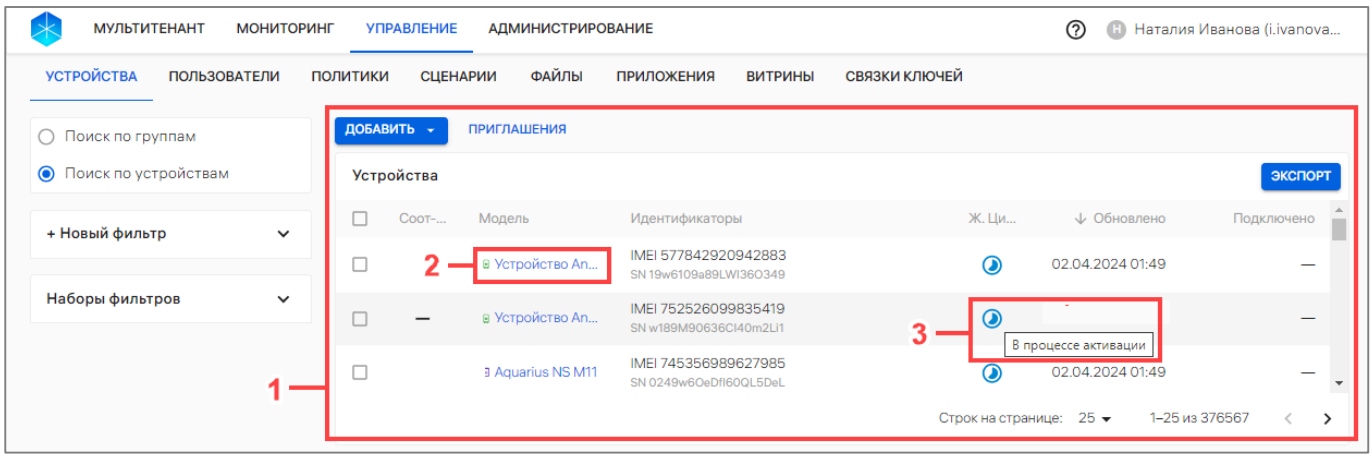

Рисунок 6

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. 2.2.6.1
		Привязать устройства к группам	пп. 2.2.7.1
		Активация устройств	пп. 2.2.8.2
		Архивировать	пп. 2.2.11.1
Группы устройств			
ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам»		Активация устройств (активация помощью JSON-файла)	пп. 2.2.8.4
Пользователи			
-		Привязать пользователей к группам	пп. 2.3.4.1
		Привязать устройства к пользователям	пп. 2.3.5.1
		Архивировать пользователя	п. 2.3.6
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. 2.6.3

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

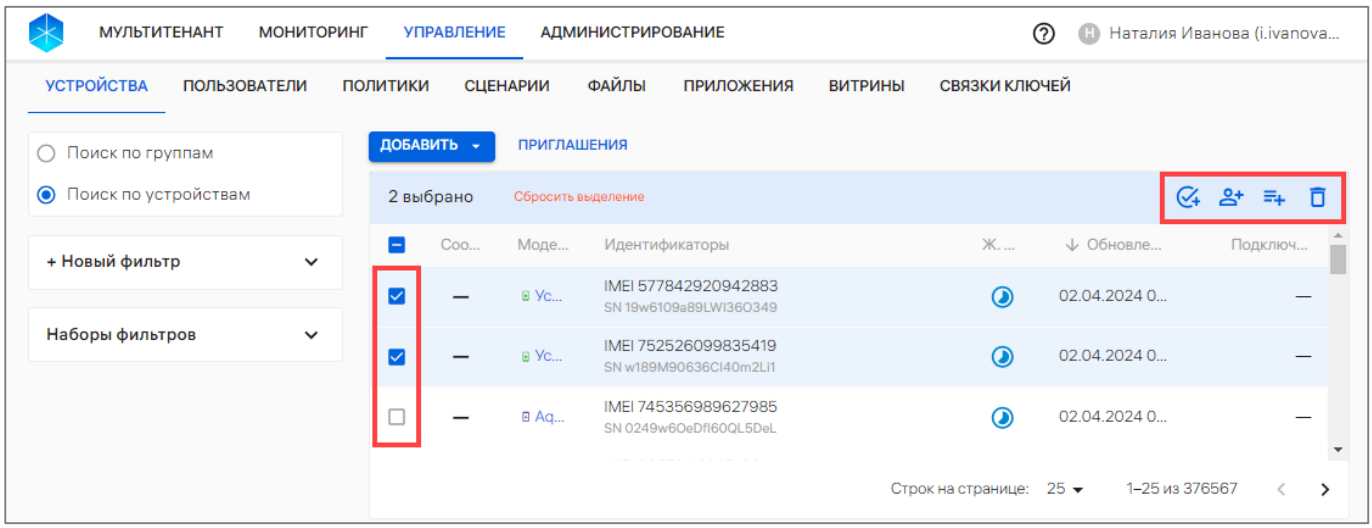

Рисунок 7

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 по каждому из подразделов раздела «Управление».

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	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»;

Подраздел	Фильтры	Доступные значения
конкретную группу)		– «По сетевому имени компьютера» - поиск по сетевому имени компьютера (hostname). 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»
	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

Подраздел	Фильтры	Доступные значения
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» → «Поиск по группам»	По названию	Поиск группы устройств по названию. Ввод значения с клавиатуры
	По принципу добавления	Поиск группы устройств по принципу добавления в группу. ПРИМЕЧАНИЕ. После применения фильтра в списке отображаются только динамические группы по выбранным критериям. Выбор значения из раскрывающегося списка: – «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»;

Подраздел	Фильтры	Доступные значения
		– «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»
	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, входящее 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

Подраздел	Фильтры	Доступные значения
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
	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 37)

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).

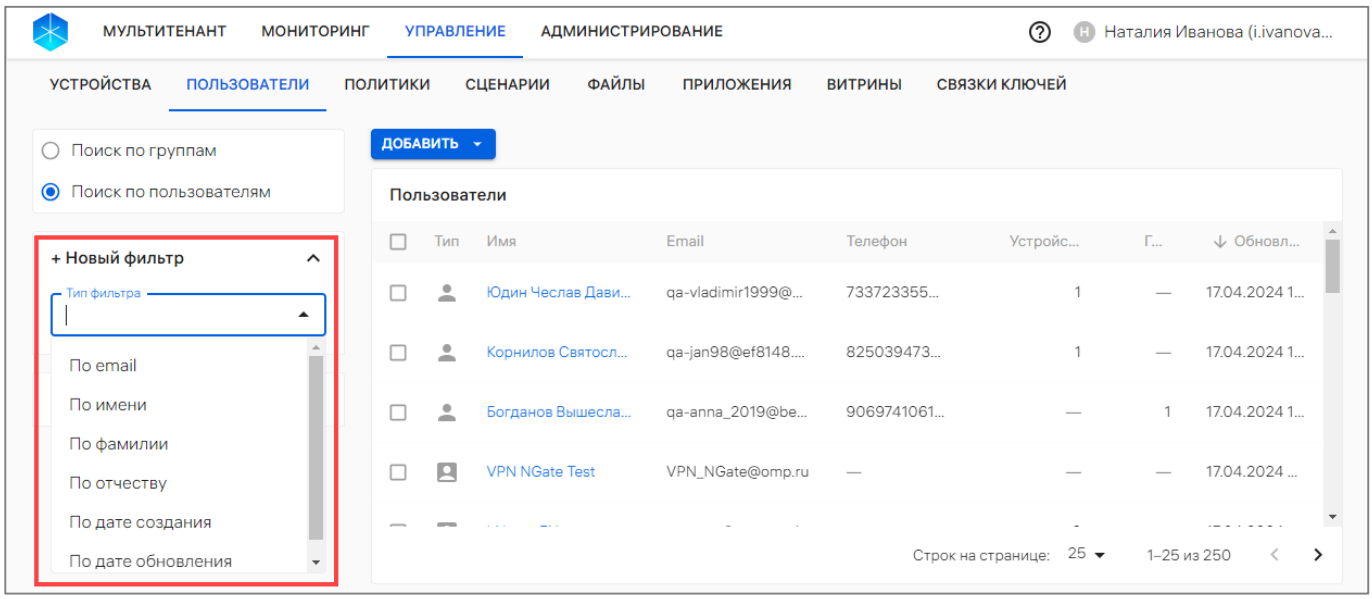

Рисунок 8

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]);

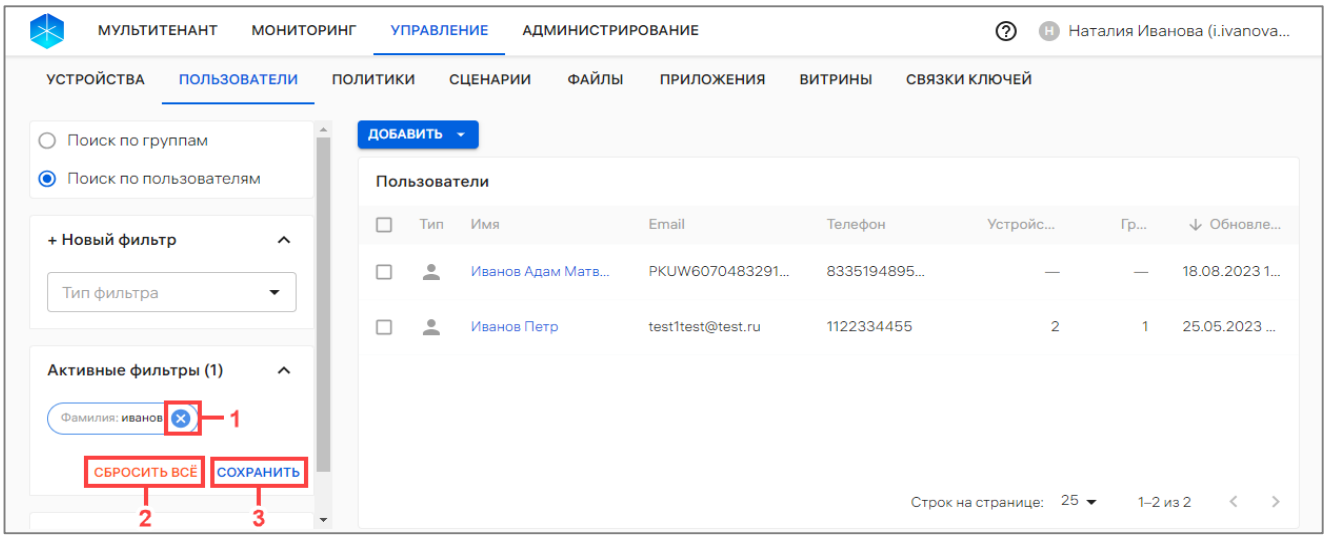

Рисунок 9

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

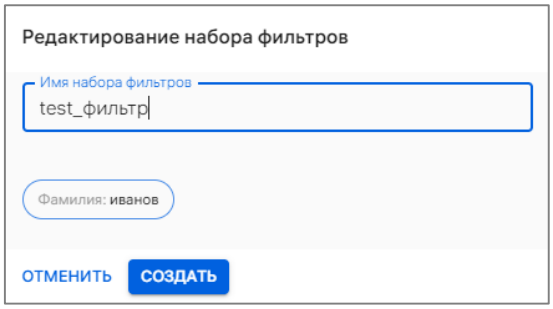

Рисунок 10

– 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 ✎.

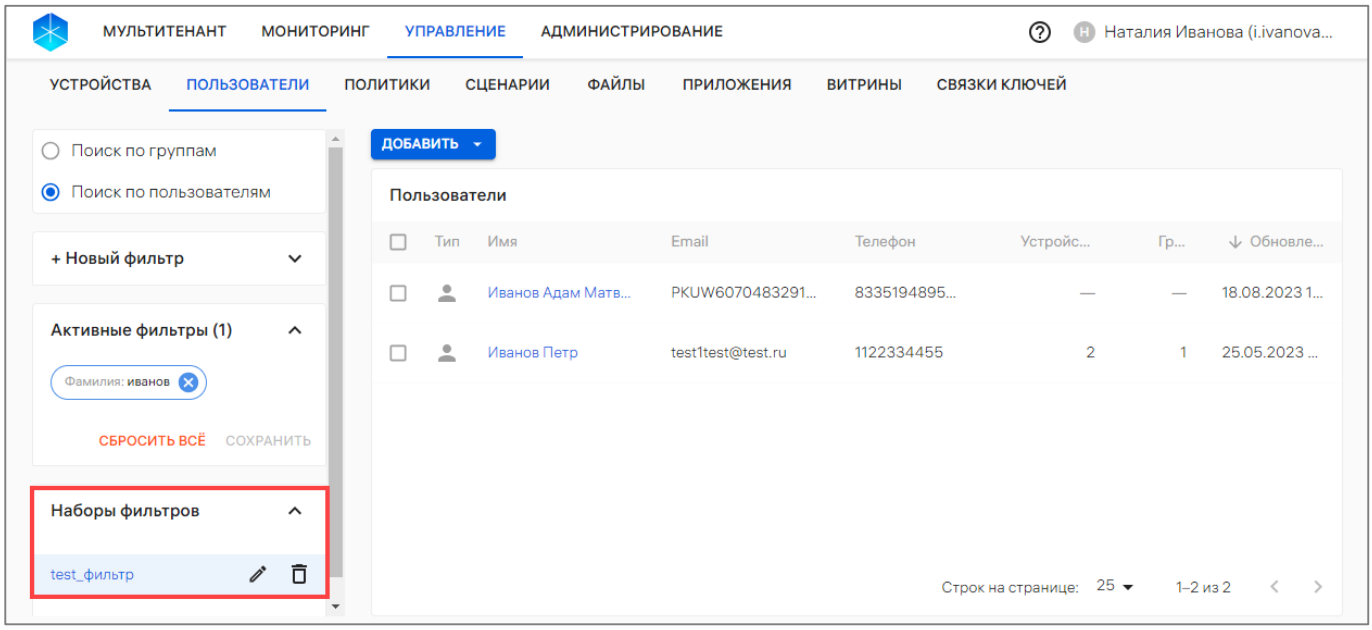

Рисунок 11

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
Ethernet MAC	MAC-адрес Ethernet устройства, который можно скопировать, нажав значок
SN	Серийный номер устройства, который можно скопировать, нажав значок
WLAN MAC	MAC-адрес WLAN устройства, который можно скопировать, нажав значок
Сетевому имени	Сетевому имени компьютера, которое можно скопировать, нажав на значок

Параметр	Описание
Статус	Статус жизненного цикла устройства/соответствия политике
Клиент Аврора Центр	Версия приложения «Аврора Центр» подсистемы ППО, которое установлено на устройство
Клиент Аврора Маркет	Версия приложения «Аврора Маркет» подсистемы ППО, которое установлено на устройство
Создано	Дата и время добавления устройства
Обновление	Дата и время последнего обновления информации об устройстве
Подключение	Дата и время последнего подключения устройства
Комментарий к устройству	Дополнительная информация об устройстве (заполняется при необходимости)

– оперативное управление (Рисунок 12 [4]), применение которого приведено в п. 2.2.9;

– 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:

– «Платформа»;

– «Модель устройства»;

– «Комментарий».

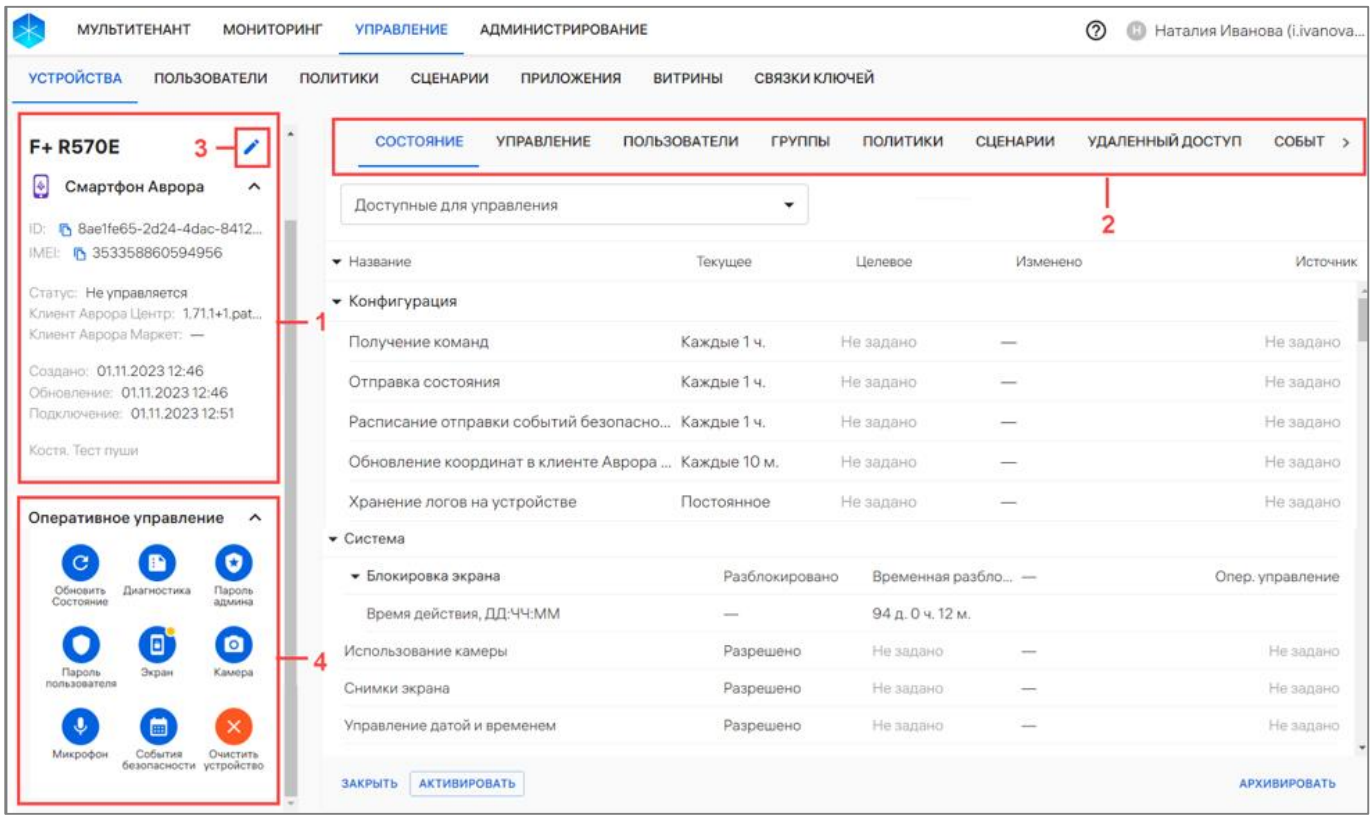

Рисунок 12

2.1.1.1. Вкладка «Состояние»

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

– активировать устройство, нажав кнопку «Активировать» (пп. 2.2.8.1);

– удалить устройство из списка устройств, нажав кнопку «Архивировать» (пп. 2.2.11.2);

– 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 поля состояния;

– «Доступные для управления» — отображаются поля, значения которых могут задаваться политиками, оперативным управлением, офлайн-сценариями (значение выставлено по умолчанию);

– «Под управлением» — отображаются поля, значения которых заданы политиками, оперативным управлением, офлайн-сценариями.

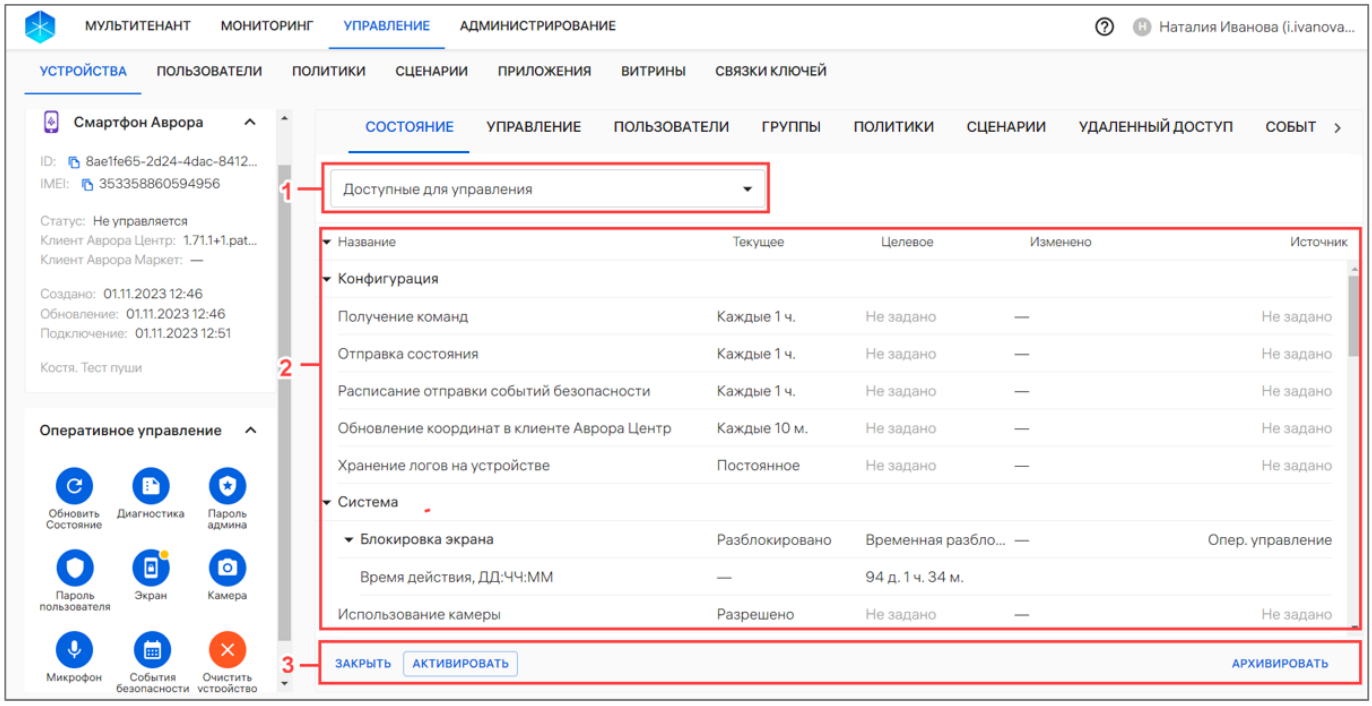

Рисунок 13

Для получения данных о состоянии активированного устройства в любом статусе необходимо создать и назначить на устройство политику отправки состояния или отправить оперативную команду «Обновление состояния». 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 назначения (изменения) политики или оперативной команды;

– «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.

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).

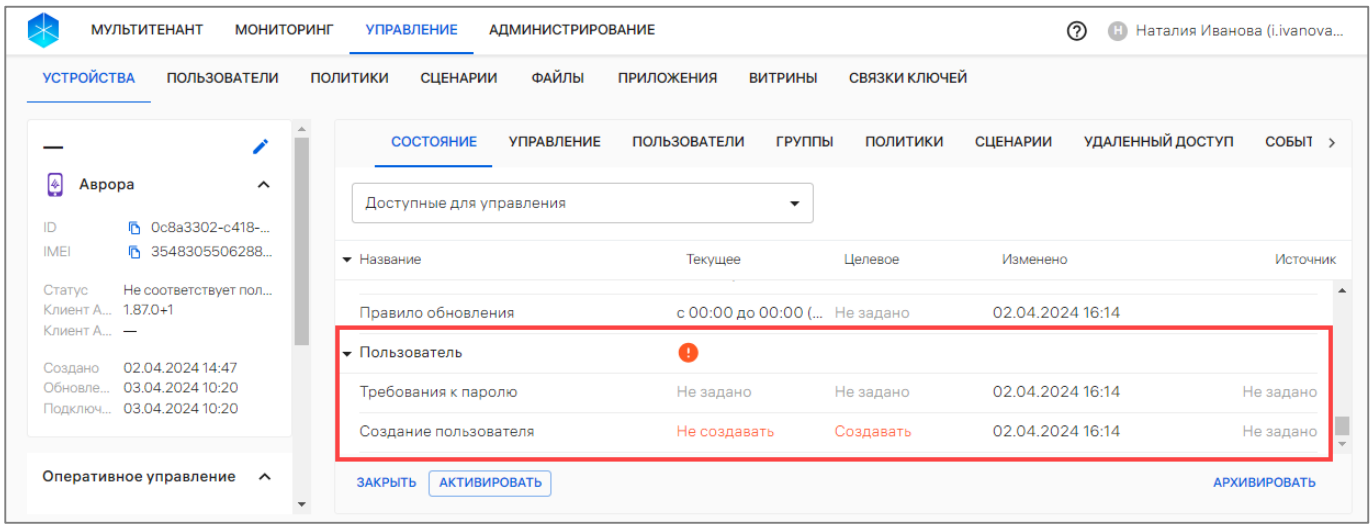

Рисунок 14

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	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Свойства					
Серийный номер	Серийный номер, присвоенный устройству производителем	Пример: YY220331000763	+	+	-
Производитель	Компания-производитель устройства	Пример: Mashtab	+	+	-
Модель	Модель устройства	Пример: mashtab_t1	+	+	-
Настройки Сервиса уведомлений Аврора					
ID приложения	Идентификатор приложения, с которым приложение «Аврора Центр» регистрируется в ПСУ	Пример: `int_mobile_buggmfjginaqssnmf07g`	+	+	-
Адрес	Адрес Сервиса уведомлений Аврора для приложения «Аврора Центр»	Пример: `ocs-dev.ompcloud.ru`	+	+	-
Порт	Номер порта для подключения приложения «Аврора Центр»	Пример: 989	+	+	-
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 значения «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	Пример: 86400	+	+	-
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 значения «Не задано»	+	+	-

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
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 значения «Не задано»	+	+	-
Настройки LDAP					
OIDC Клиент	Идентификатор клиента, необходимый для аутентификации в LDAP	`user-mobility-management`	+	+	-
Настройки проверки подключения к сети					
Адрес IPv4	Адрес IPv4 для проверки доступа к сети Интернет у устройства	Пример: http://ipv4.omprussia.ru/return_204	+	-	-
Адрес IPv6	Адрес IPv6 для проверки доступа к сети Интернет у устройства	Пример: http://ipv6.omprussia.ru/return_204	+	-	-
Настройки сервера времени					
Адреса	Список адресов серверов времени NTP	Пример: `ntp.nict.jp, time.google.com, pool.ntp.org`	+	-	-
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, которые не будут отправляться в Аврора Центр	Пример: «Информационное»	+	-	-
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»	+	-	-
Корневые сертификаты (количество сертификатов)					

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Название сертификата	В столбце «Текущее»/«Целевое» отображается цифровой отпечаток (Fingerprint) доверенного сертификата	Пример: 1a245f158147714f93d04428a6b5593fc0ea88de	+	+	-
Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат	Пример: ОМР	+	+	-
Дата выпуска	Дата выпуска сертификата	Пример: 09.04.2021	+	+	-
Срок действия, до	Срок действия сертификата	Пример: 07.06.2031	+	+	-
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		+	+	-
Управление датой и временем	Разрешение или запрет на внесение изменений в настройки даты и времени		+	+	-
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		+	+	-
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)	Пример: host-129	-	-	+
Тип устройства	Тип устройства – ПК/Ноутбук/Other	Пример: Other	-	-	+
Объем жестких дисков	Общий объем жестких дисков на устройстве	Пример: 39.63 ГБ	-	-	+
Объем оперативной памяти	Общий объем оперативной памяти на устройстве	Пример: 938,35 МБ	-	-	+
Процессор					
Название	Название модели процессора	Пример: AMD Ryzen 9 5900X 12-Core Processor	-	-	+

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Частота	Частота процессора	Пример: 3693.06 MHz	-	-	+
Количество ядер	Количество ядер процессора	Пример: 1	-	-	+
Звуковые устройства (Список названий звуковых устройств ЭВМ)					
Название	Название звукового устройства ЭВМ	Пример: Intel 82801AA AC97 Audio	-	-	+
Мониторы (список названий мониторов, подключенных к устройству)					
Название	Название монитора, подключенного к устройству		-	-	+
Память (список хранилищ устройств)					
Название	Название хранилища	Пример: /apex/com.android.media	+	+	+
Общий объем	Общий объем модуля памяти устройства	Размер в МБ/ГБ Пример: 64,00 ГБ	+	+	+
Доступный объем	Доступный для пользователя объем модуля памяти		+	+	+
Свободно	Свободный объем модуля памяти устройства		+	+	+
Батарея					
Уровень заряда	Уровень заряда аккумулятора устройства	Пример: 80%	+	+	+
Заряжается	Заряжался ли аккумулятор устройства в момент отправки состояния	Возможные значения: – «Да»; – «Нет»	+	+	+
Управление соединениями					
Управление авиарежимом	Разрешение или запрет на использование авиарежима	Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Управление точкой доступа WLAN	Разрешение или запрет на изменение настроек мобильной точки доступа		+	+	-
Использование браузера	Разрешение или запрет возможности использования браузера на устройстве		+	+	-
Передача данных MTP	Разрешение или запрет возможности передачи данных по протоколу MTP		+	+	-
Сетевые интерфейсы					
Название	Название сетевого интерфейса	Пример: wlan0	+	+	+
Тип	Тип сетевого интерфейса	Пример: ETHERNET	+	+	+
MAC	MAC-адрес сетевого интерфейса	Пример: 00:0C:29:8C:E0:28	+	+	+
WLAN					
Работа WLAN	Разрешение или запрет на использование сети WLAN	Возможные значения: – «Включен»;	+	+	-

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
		– «Выключен»			
Управление WLAN	Разрешение или запрет изменения состояния адаптера сети WLAN	Возможные значения: – «Разрешено»; – «Запрещено»	+	+	-
Название WLAN	Название сети WLAN, к которой подключено устройство	Пример: WLAN_1	+	+	-
MAC-адрес роутера	MAC-адрес роутера, к которому подключено устройство	Пример: 00:26:57:00:1f:02	+	+	-
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»	+	+	-
Хеш пароля	Хеш-значение пароля беспроводной сети. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA2	Пример: s2YaBGWeY4MRyDrqh60nNc6l4yEBtgLGxukl7dylV8	+	+	–
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	Пример: WI-FI-сеть	+	+	-
Идентификатор	Идентификатор пользователя для подключения к беспроводной сети. **ПРИМЕЧАНИЕ**. Отображается для сети с WPA-EAP	Пример: ivanov@omp.ru	+	+	-
VPN					
Подключения (подключения VPN, созданные на устройстве с помощью политики)					
Название (тип подключения)	Название подключения VPN. В скобках указывается тип подключения:	Пример: Test	+	+	-

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	– для устройств с ОС Аврора - КриптоПро NGate R2; – для устройств с ОС Android - Cisco AnyConnect/ КриптоПро NGate R2				
Адрес сервера	Адрес сервера VPN	Пример: 1.1.1.1	+	+	-
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	Пример: `adcs-moscow-cert`	-	+	-
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	Пример: `ivanivanov`	+	+	-
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	Пример:12121-32324-31434-33333-32222b	+	+	-
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»	+	+	-
Геопозиция					
Режим работы	Режим работы геопозиционирования	Возможные значения: – «Не задано»; – «Выключено»; – «Пользовательские настройки»;	+	+	-

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
		– «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»; – «Выключен»	+	+	-
GPS-координаты	Географические координаты устройства (широта и долгота)	Пример: 55.739604, 37.496983	+	+	-
Время получения координат	Дата и время фиксации координат	Пример: 25.1.2023 19:10	+	+	-
SIM-карты					
Слот SIM1 (то же для Слот SIM2)					
IMEI	Уникальный номер SIM-карты	Пример: 35-419002-389644-3	+	+	-
ICCID	Уникальный серийный номер SIM-карты	Пример: 8901260232714958936F	+	+	-
Активен	Активность SIM-карты	Возможные значения: – «Да»; – «Нет»	+	+	-
Защищена PIN-кодом	Защита SIM-карты PIN-кодом		+	+	-
Голосовые вызовы	Разрешение или запрет голосовых вызовов	Возможные значения: – «Разрешена(ны)»; – «Запрещена(ны)»	+	+	-
Мобильная передача данных	Разрешение или запрет на мобильную передачу данных		+	+	-
Внешние накопители					
Использование USB-накопителей	Разрешение или запрет использования USB-накопителей	Возможные значения: – «Разрешено»; – «Запрещено»	+	-	-
Использование SD-карт	Разрешение или запрет использования SD-карт		+	-	-
Управление приложениями					

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Установка приложений	Разрешение или запрет установки приложения на устройства	Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»	+	+	+
Приложения (сгруппированы по названиям приложения)					
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	+	+	+
Автозапуск	Определяет включение автозапуска приложения	Возможные значения: – «Не задано»; – «Да»; – «Нет»	+	+	-

Название группы политик/состояний		Описание	Доступные значения	Версии ОС		
				ОС Аврора	ОС Android	ОС семейства Linux
Управление файлами						
	Файлы (сгруппированы по названиям файлов)					
	Директория	Директория на устройстве, в которую должен быть помещен файл	Пример: `/home/omp/`	-	+	+
	Размер	Размер файла	Пример: 76 Байт	-	+	+
	Комментарий	Комментарий к файлу	Пример: comment test	-	+	+
	Хэш файла	Хэш содержимого файла	Пример: i5BAARxvCOdJkz51xL+pj6Svds3qIrU/EQjQI+Vc+ok	-	+	+
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)	Пример: test_result	-	+	+
	Последнее успешное выполнение	Дата и время последнего успешного выполнения скрипта	Формат: [дд].[мм].[гг] [чч]:[мм]	-	+	+
Дистрибутив ОС						
ОС		Название ОС	Пример: Аврора	+	+	+
Версия ОС		Номер версии ОС	Пример: 3.2.3.15	+	+	+
Вариант ОС		Название варианта ОС	Пример: omp	+	+	+
Обновление ОС		Разрешение или запрет обновления ОС Аврора	Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Правило обновления		Период обновления на новую версию ОС	Пример: с 22:00 до 06:00 (3.0.2.20)	+	-	-

Название группы политик/состояний	Описание	Доступные значения	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Пользователь					
Требования к паролю	Информация о требованиях к следующим параметрам пароля: – сложность; – длина; – срок истечения	Возможные значения: 1) Обычный: сложность – обычная (цифры), длина – от 7 до 10 символов; 2) Сложный: сложность – высокая (цифры, буквы, символы, знаки пунктуации), длина – от 8 до 12 символов); 3) 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»	+	-	+
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	Пример: OCSEMM	+	+	-
Фингерпринт	Цифровой отпечаток (Fingerprint) сертификата	Пример: 1a245f158147714f93d04428a6b5593fc0ea88de	+	+	-
Хэш-алгоритм запроса	Алгоритм хэширования	Пример: sha512	+	+	-
Тип шифрования и длина ключа	Алгоритм шифрования приватного ключа	Пример: rsa2048	+	+	-
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		+	+	**-**
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	Пример: 11223344	-	+	-
Приложения	Названия пакетов приложений, которые будут доступны пользователю в режиме киоска	Пример: com.android.chrome	-	+	-
Ярлыки веб-страниц			-	+	-

Название группы политик/состояний		Описание	Доступные значения	Версии ОС		
				ОС Аврора	ОС Android	ОС семейства Linux
	Название ярлыка	Названия ярлыка веб-страницы	Пример: omp	-	+	-
	URL	Электронный адрес сайта/веб-страницы в формате URL	Пример: https://www.omp.ru/	-	+	-
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		-	+	-

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]).

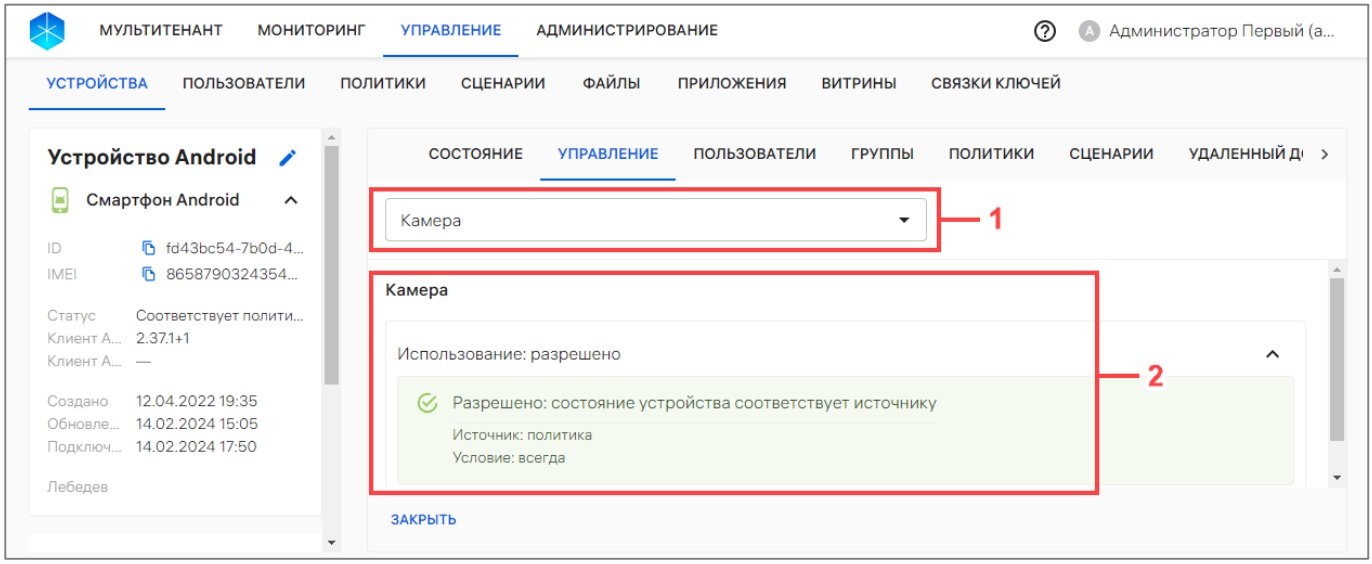

Рисунок 15

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. 2.2.6.2.

Список пользователей сортируется по дате обновления информации о пользователях устройства.

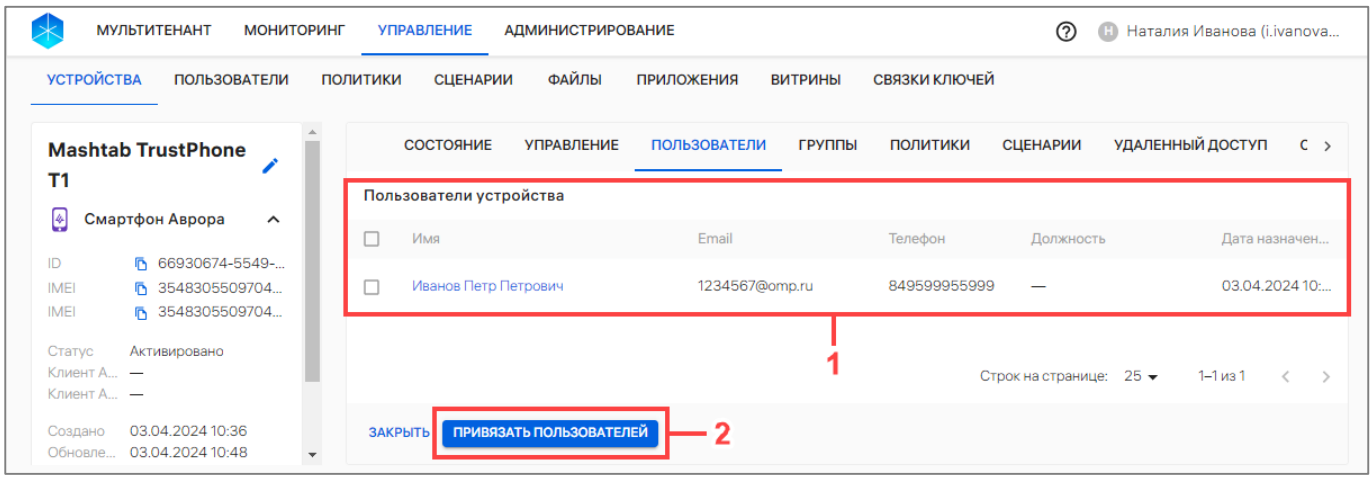

Рисунок 16

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 пользователя
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. 2.2.7.2.

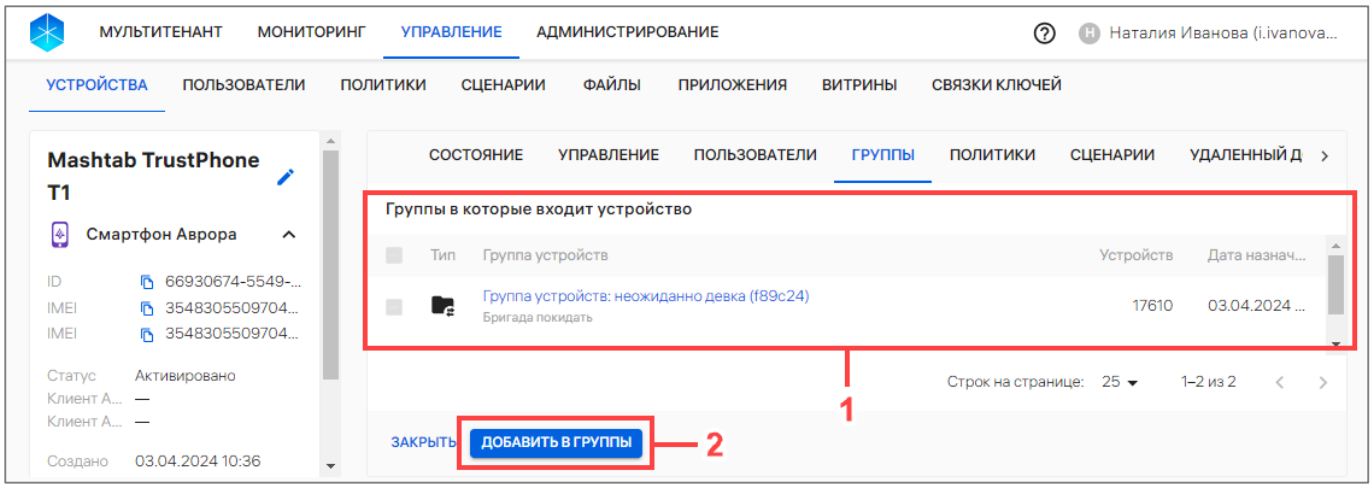

Рисунок 17

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 его правил (Рисунок 18), а при его отсутствии 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.

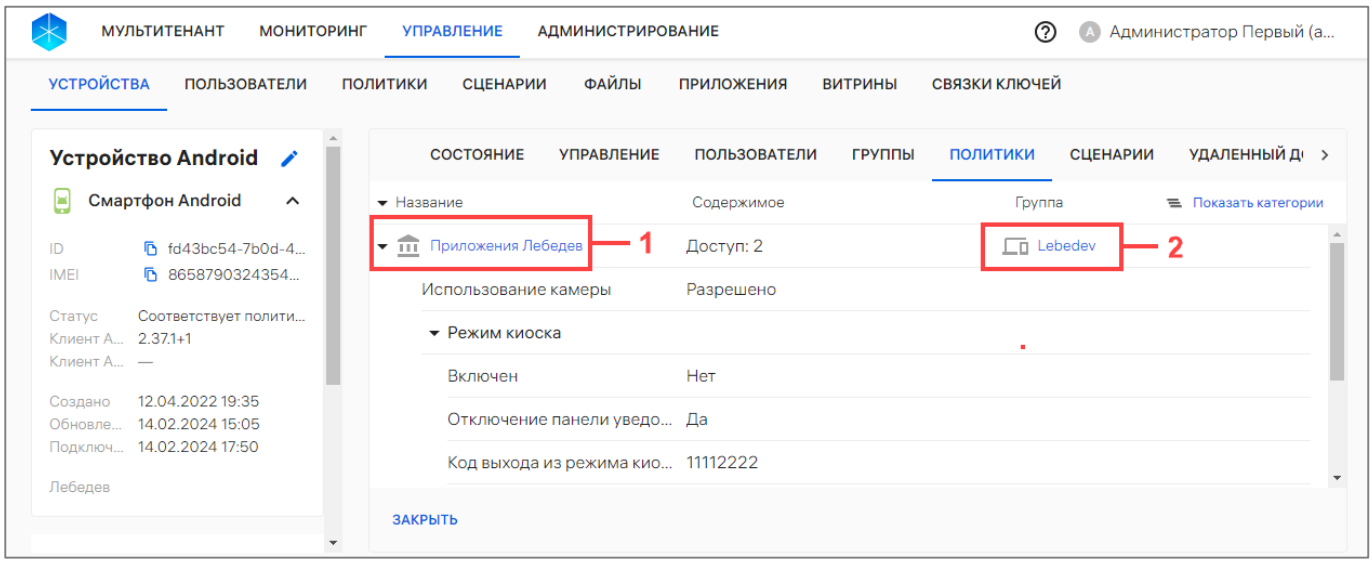

Рисунок 18

При отсутствии политик, назначенных на группу устройств/пользователей, в которую входит данное устройство, необходимо выполнить действия, приведенные в п. 2.4.6.

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. 2.2.14) 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.

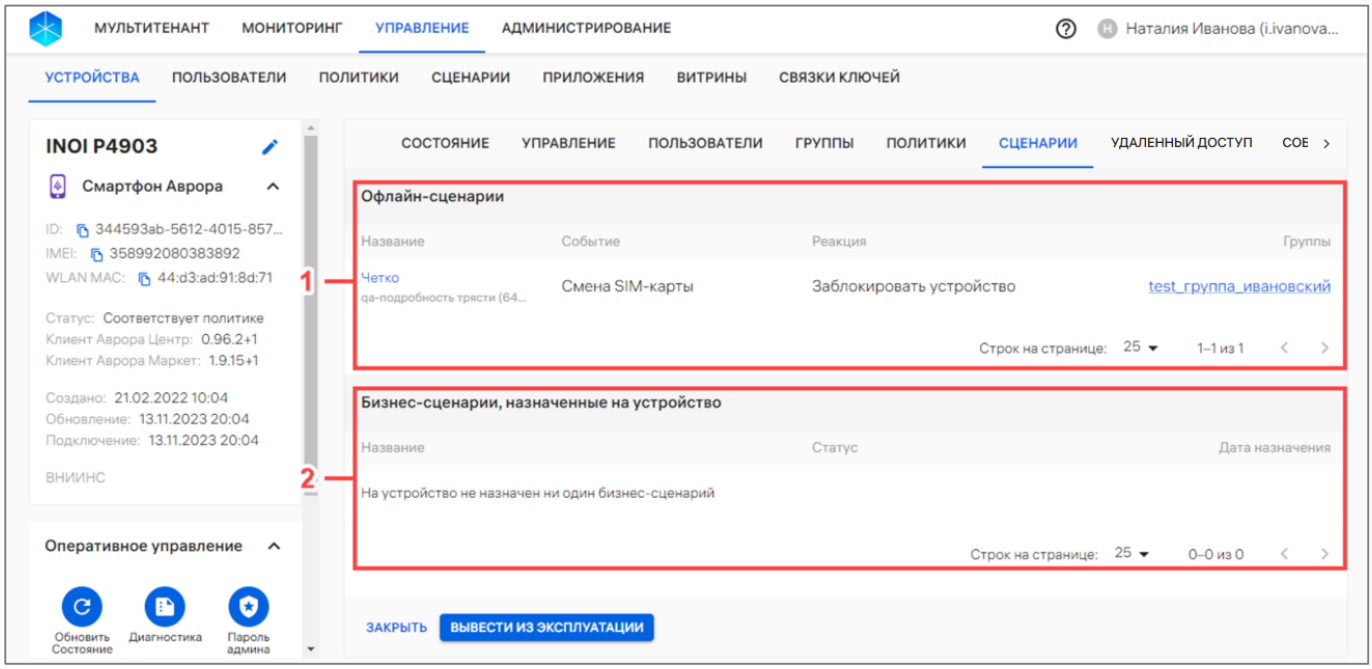

Рисунок 19

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.

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

1) Установить сервер RustDesk.

ПРИМЕЧАНИЯ:

✓ Инструкция по установке расположена на официальном сайте: https://rustdesk.com/docs/ru/self-host/rustdesk-server-oss/install/;

✓ Рекомендуется использовать версию сервера RustDesk 1.1.8.

В результате установки сервера RustDesk будут доступны следующие настройки: адрес и ключ;

2) Задать настройки сервера RustDesk (адрес и ключ) в конфигурационном файле ПУ `(/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml)`;

3) Установить и настроить desktop-клиент RustDesk на ЭВМ администратора.

Для этого необходимо:

– скачать на официальном сайте: https://github.com/rustdesk/rustdesk/releases дистрибутив desktop-клиента RustDesk и установить его на ЭВМ.

ПРИМЕЧАНИЕ. Рекомендуется использовать desktop-клиент RustDesk версии 1.2.3;

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

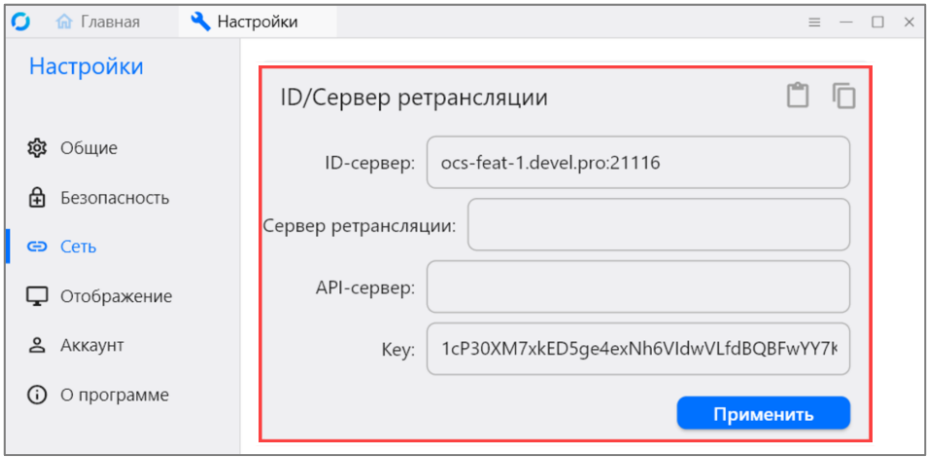

Рисунок 20

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;

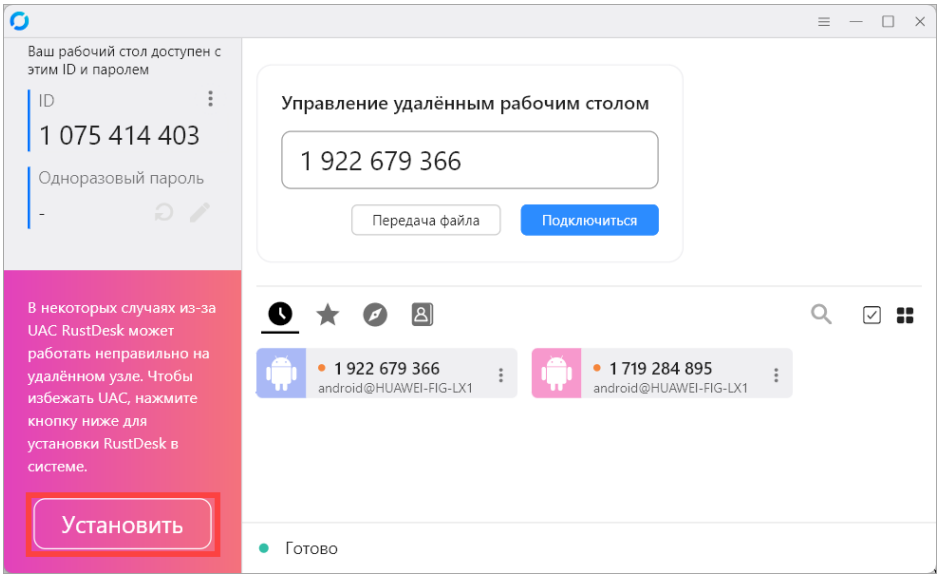

Рисунок 21

4) Установить и настроить приложение RustDesk на устройствах:

– ОС Android версии 7-11 (подготовка устройства к удаленному подключению приведена в приложении (Приложение 4);

– ОС Альт Linux версии p10.

ПРИМЕЧАНИЯ:

✓ Необходимые установочные файлы входят в состав дистрибутива ППО;

✓ Рекомендуется установить приложение RustDesk, назначив политику через ПУ;

5) 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 (Рисунок 26).

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

ПРИМЕЧАНИЕ. 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.

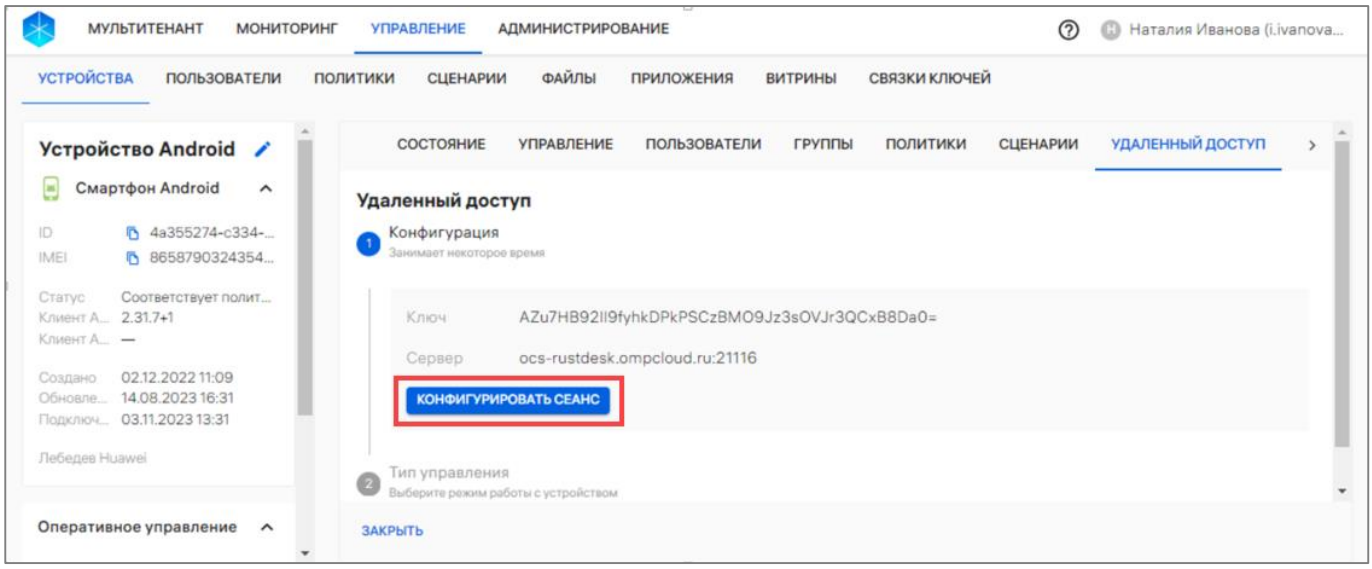

Рисунок 22

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 устройстве вручную запустить службу RustDesk и выдать требуемые разрешения (Приложение 4).

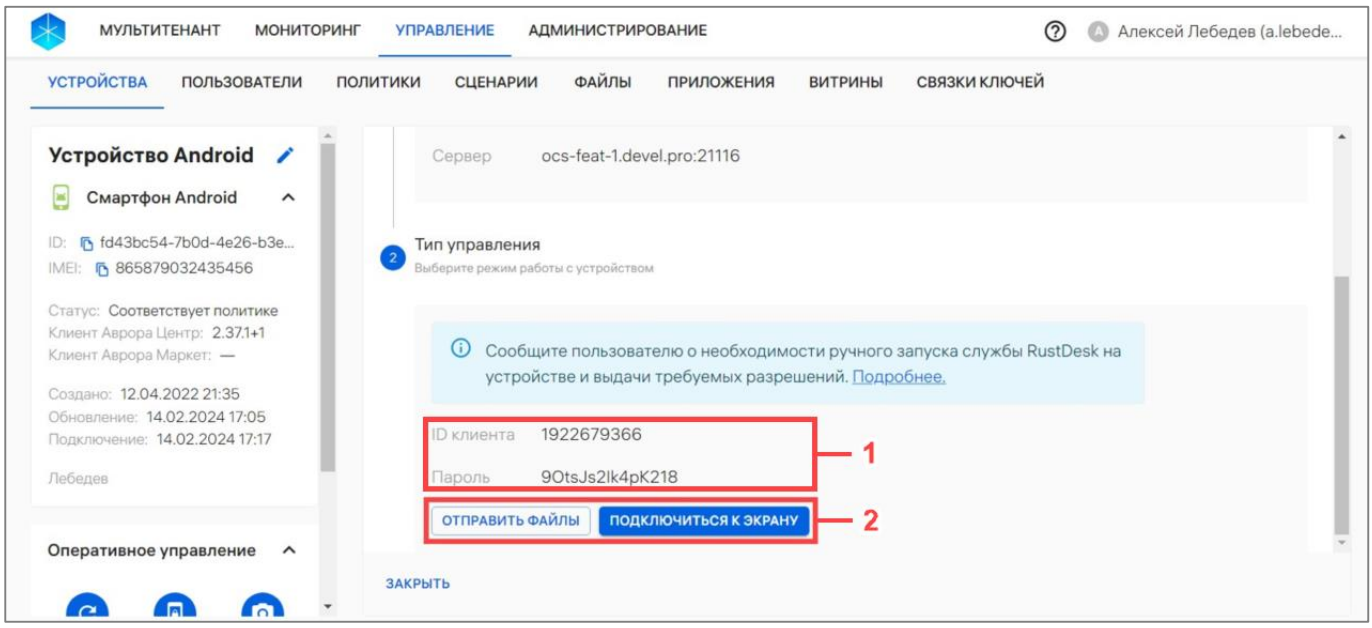

Рисунок 23

Если необходимо:

– подключиться к рабочему столу пользователя устройства, необходимо нажать кнопку «Подключиться к экрану» (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» (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. 2.2.9) или политикой с правилом «Конфигурация/Расписание отправки событий безопасности» (пп. 2.4.6.2).

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

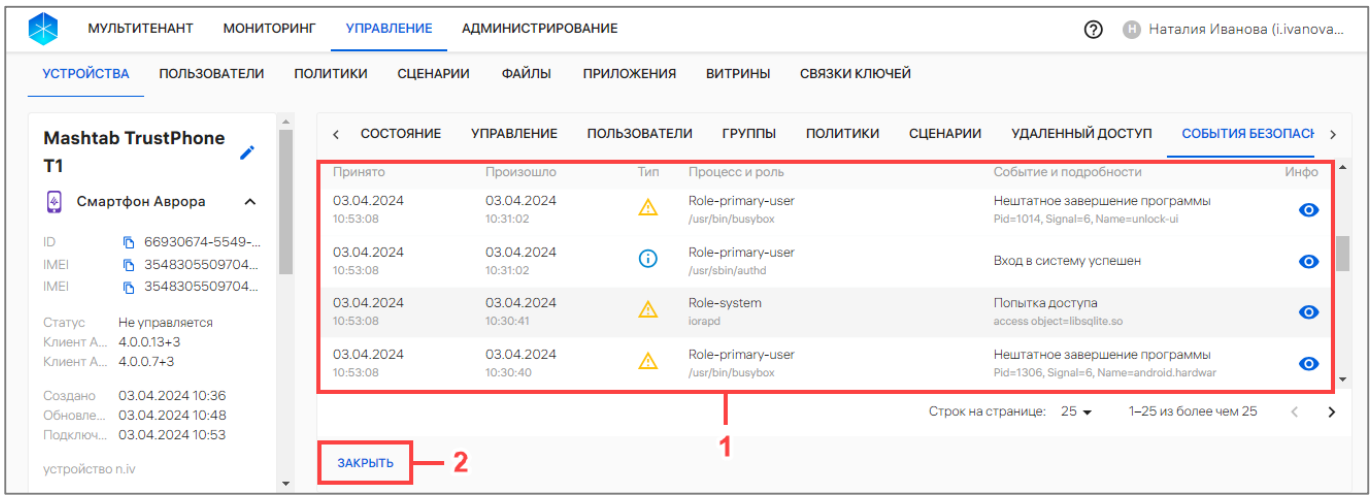

Рисунок 24

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»

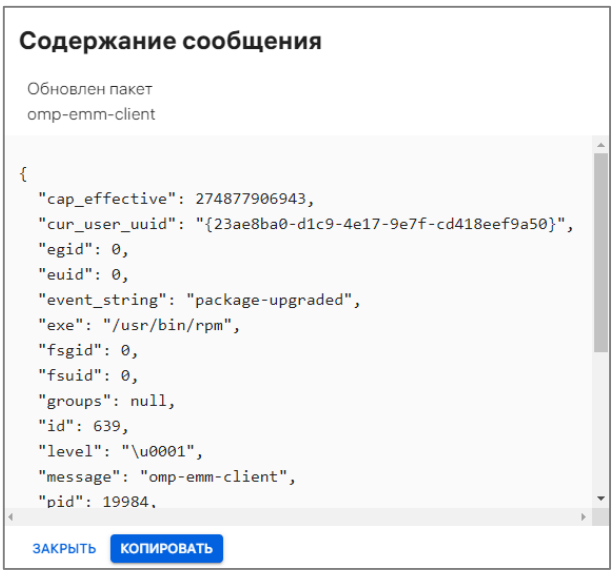

Рисунок 25

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

2.1.1.9. Вкладка «Приложения»

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

ПРИМЕЧАНИЕ. Данные о всех установленных приложениях отправляют только устройства с ОС Аврора и ОС Android. Устройства на базе ОС семейства Linux передают информацию только об установленном приложении «Аврора Центр».

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	Определяет включение автозапуска приложения. Возможные значения: – ⊘ - Выключено; – ✓ - Включено. **ВНИМАНИЕ!** Автозапуск можно установить только для приложений с ОС Аврора. **ПРИМЕЧАНИЕ.** Если информация об автозапуске не была получена (например, автозапуск приложений отсутствует на устройстве на базе ОС Android), то ячейка не заполняется

Параметр	Описание
Разрешения	Автоматическое применение разрешений. Определяет, выдано ли приложению автоматическое применение требуемых разрешений. Возможные значения: – «Выключено»; – «Включено». **ПРИМЕЧАНИЕ.** Если информация о выданных разрешениях не была получена (например, для системных приложений в ОС Android), то ячейка не заполняется
Политика	Название политики, по правилу которой было установлено приложение. Название политики выделено цветом и представляет собой активную ссылку (Рисунок 26 [2]), при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5). При отсутствии политик с правилом установки приложения отображается значок «—»
Инфо	Отображение названия пакета приложения (Рисунок 27) при нажатии значка «Дополнительная информация» (Рисунок 26 [3])

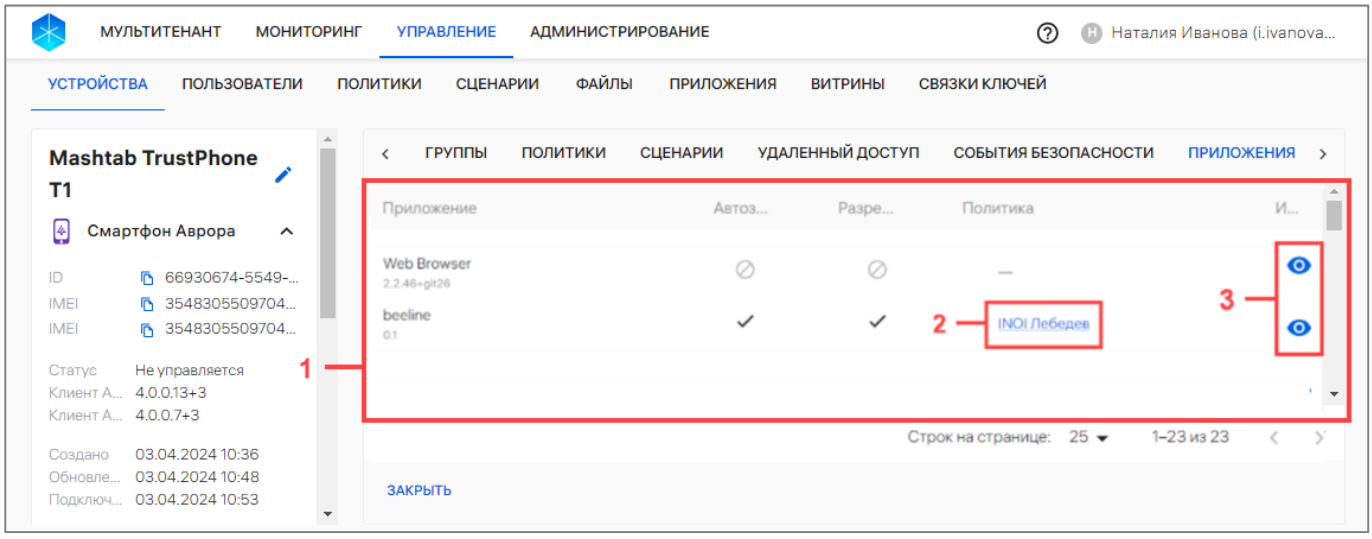

Рисунок 26

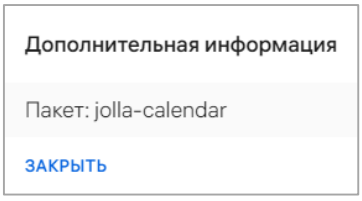

Рисунок 27

2.1.1.10.Вкладка «Карта»

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

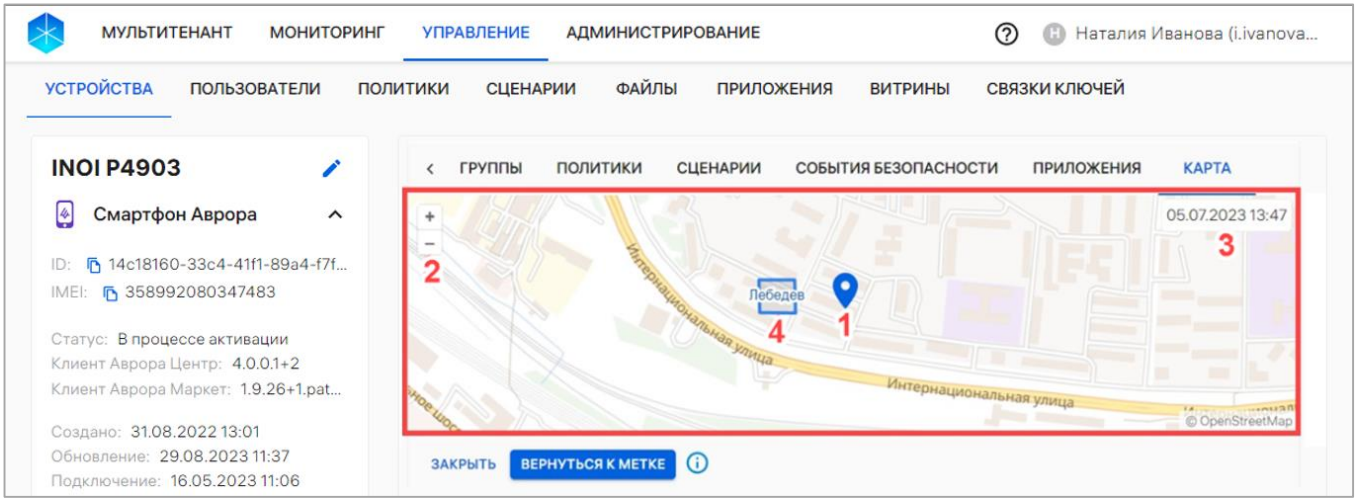

Рисунок 28

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;
– дату актуальности координат;
– режим работы геопозиционирования.

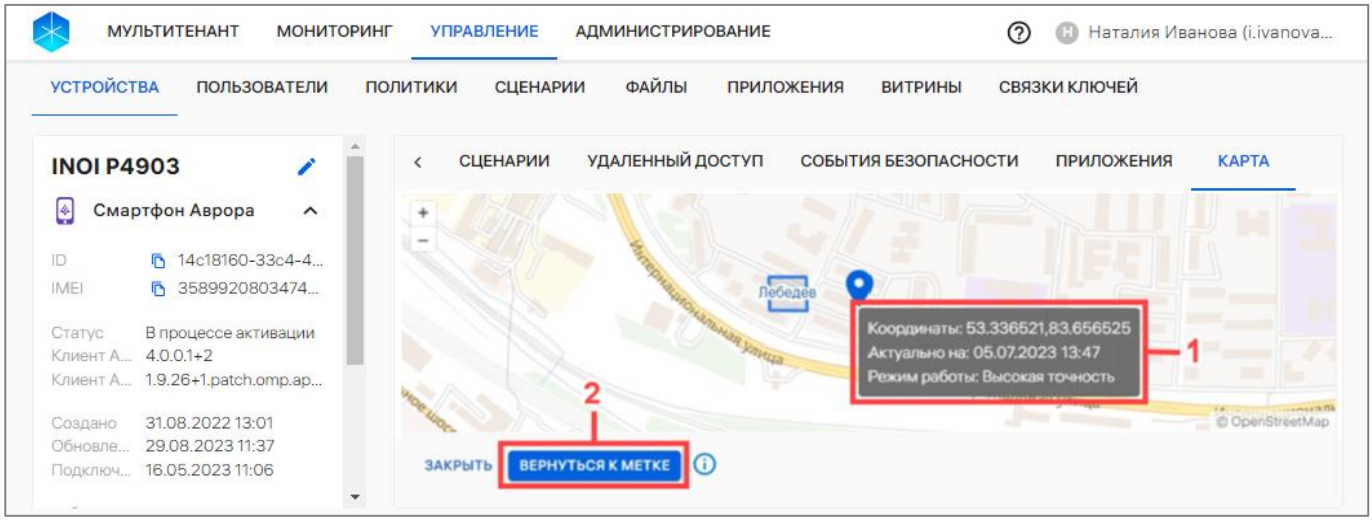

Рисунок 29

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).

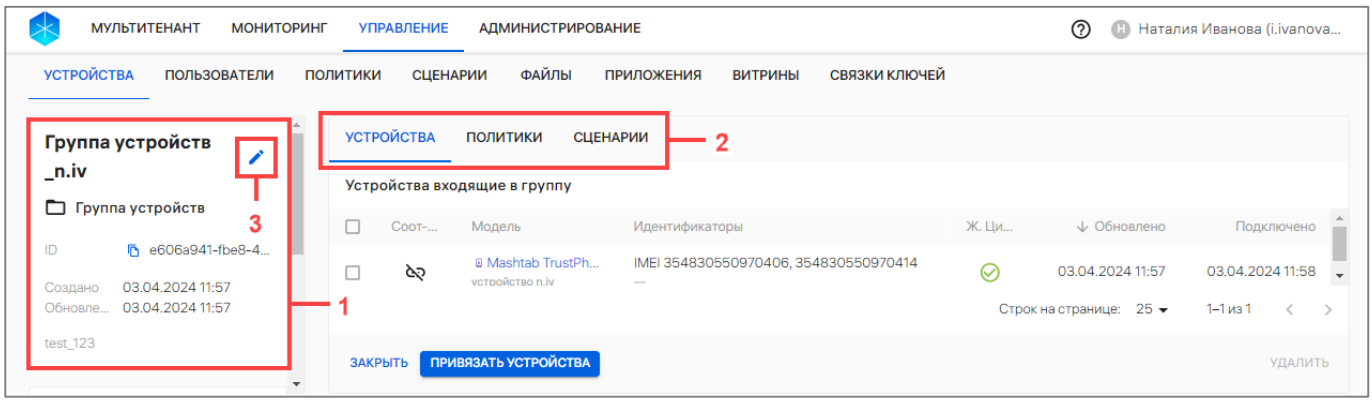

Рисунок 30

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. 2.2.7.3.

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

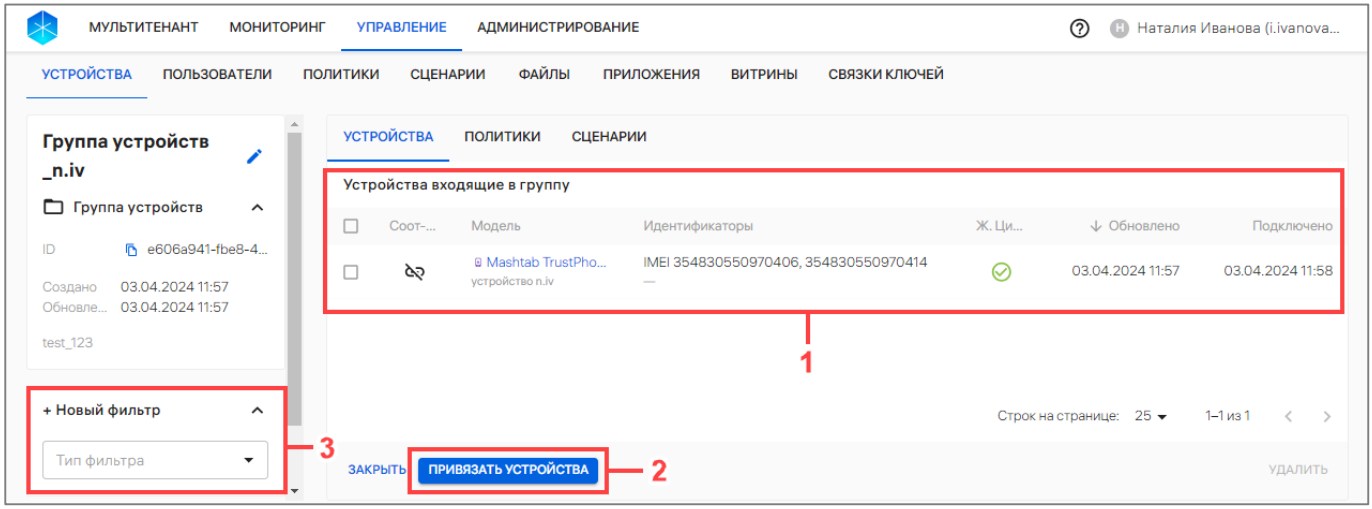

Рисунок 31

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

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

Таблица 11

Параметр	Описание
Соответствие	Соответствие назначенной политике (Приложение 1)
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
Подключено	Дата и время последнего подключения ПУ к Серверу приложений ПУ

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 выполнив действия, приведенные в пп. 2.4.6.2.

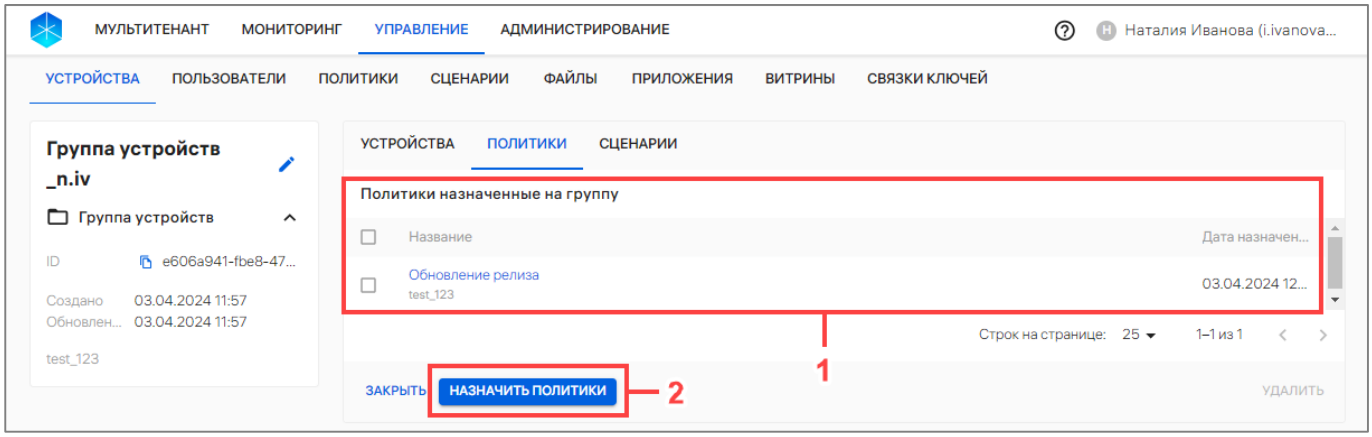

Рисунок 32

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.

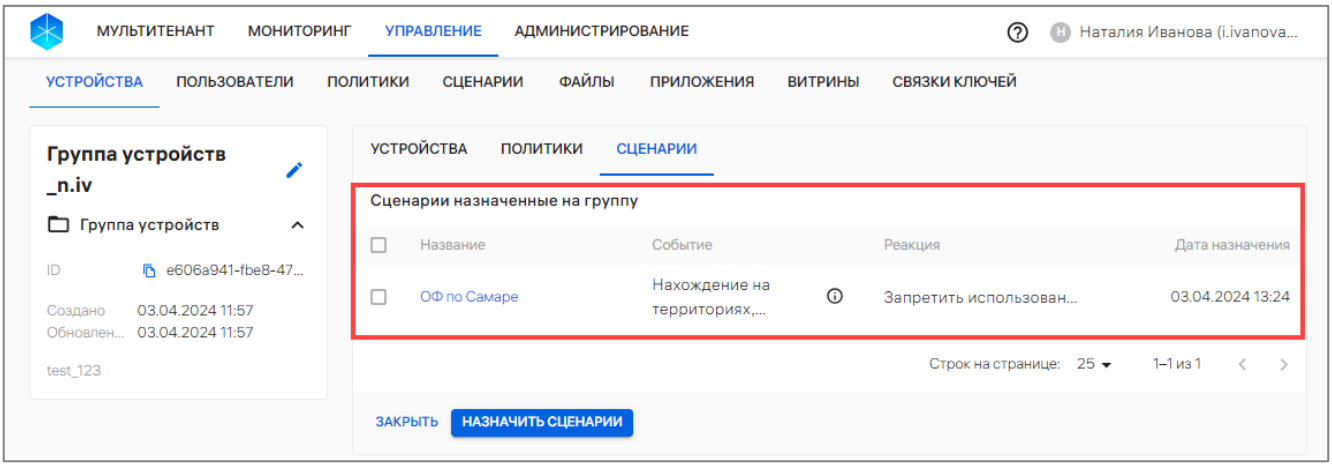

Рисунок 33

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 40)

Параметр	Описание
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).

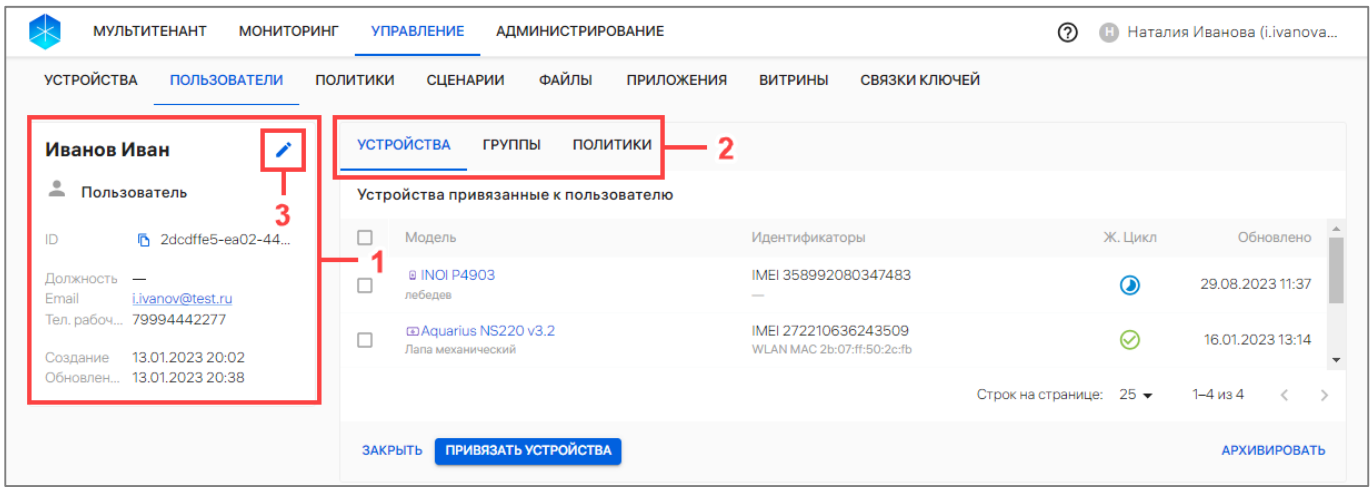

Рисунок 34

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.

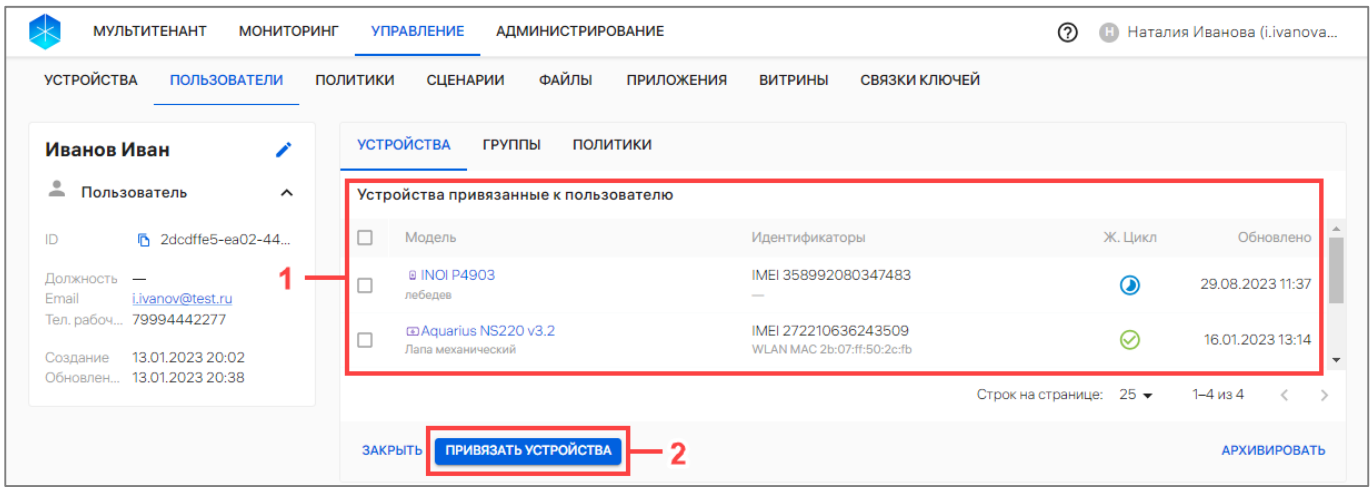

Рисунок 35

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.

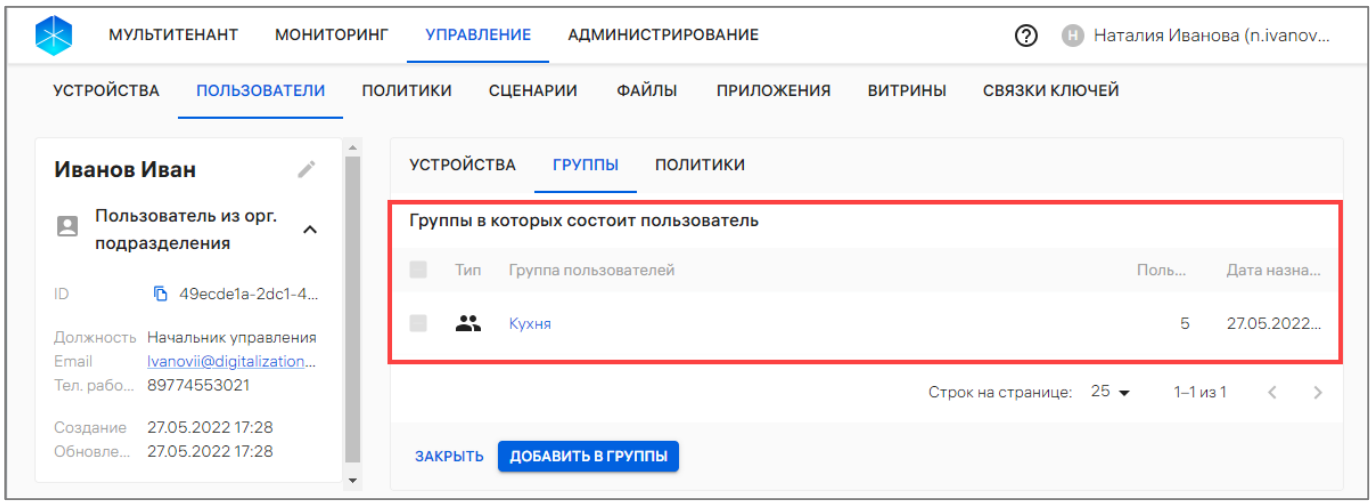

Рисунок 36

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

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

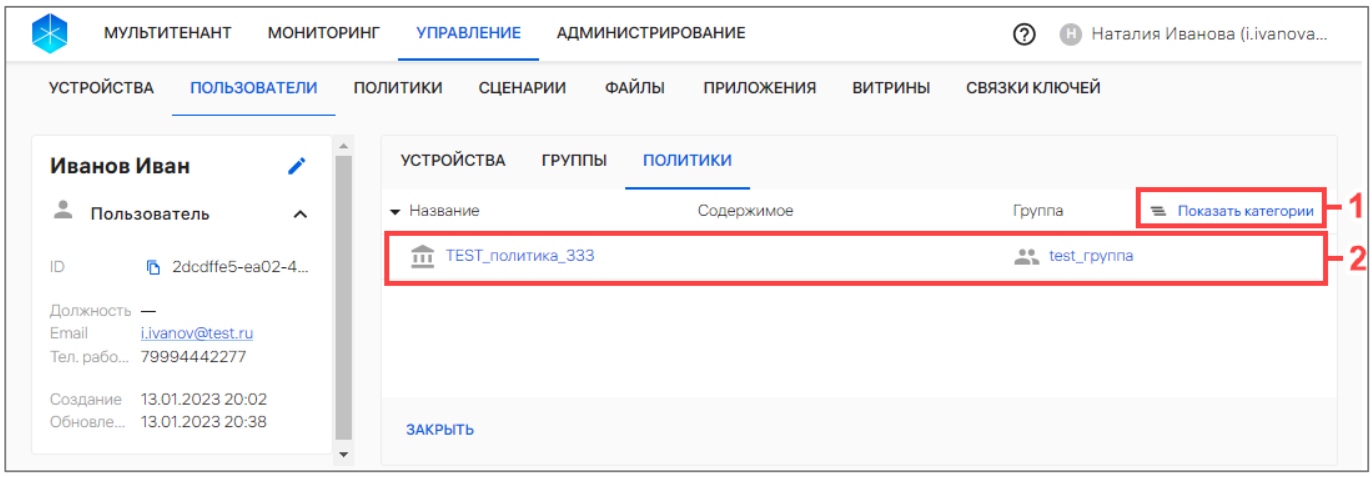

Рисунок 37

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).

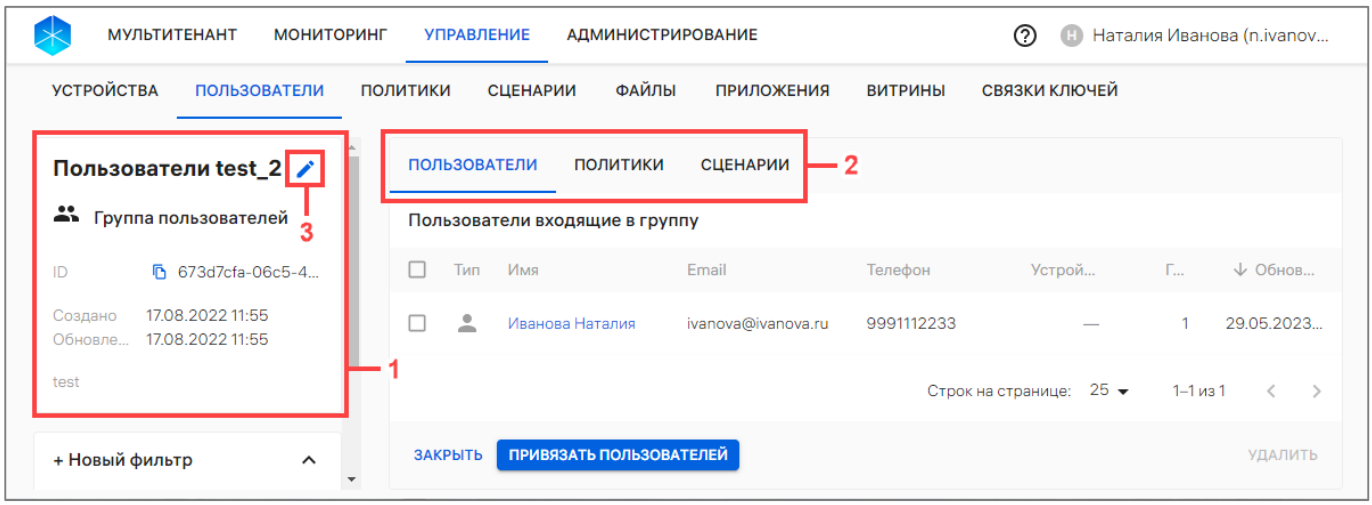

Рисунок 38

Для редактирования данных группы с типом «Группа пользователей» необходимо нажать на значок «Редактировать» (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 их отсутствии 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.

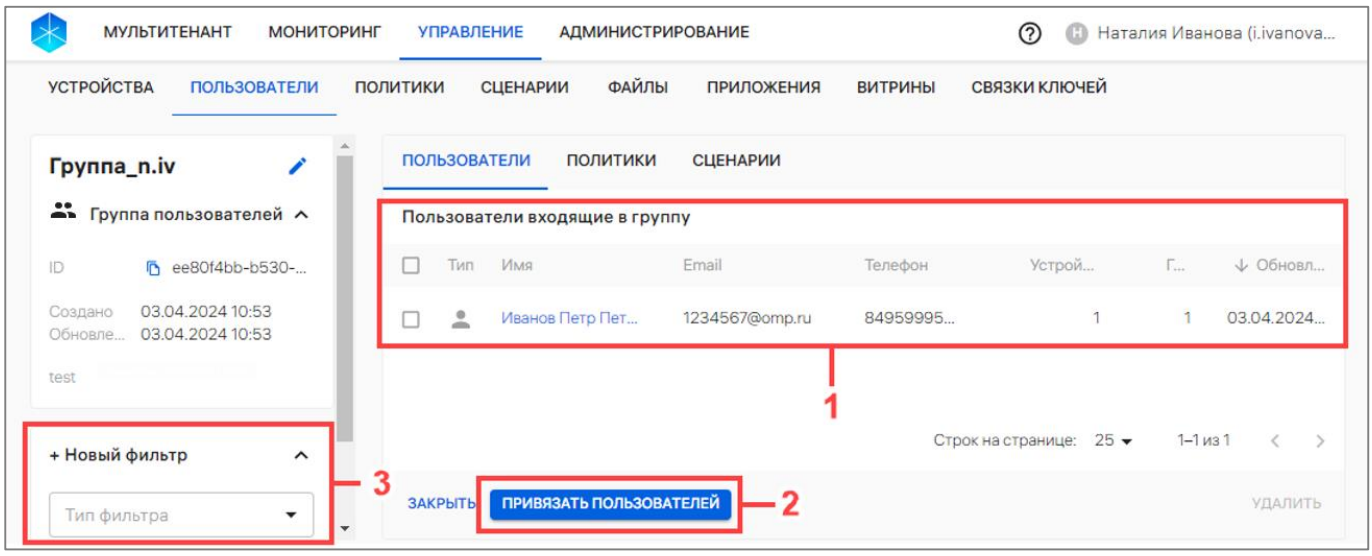

Рисунок 39

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. 2.4.6.3.

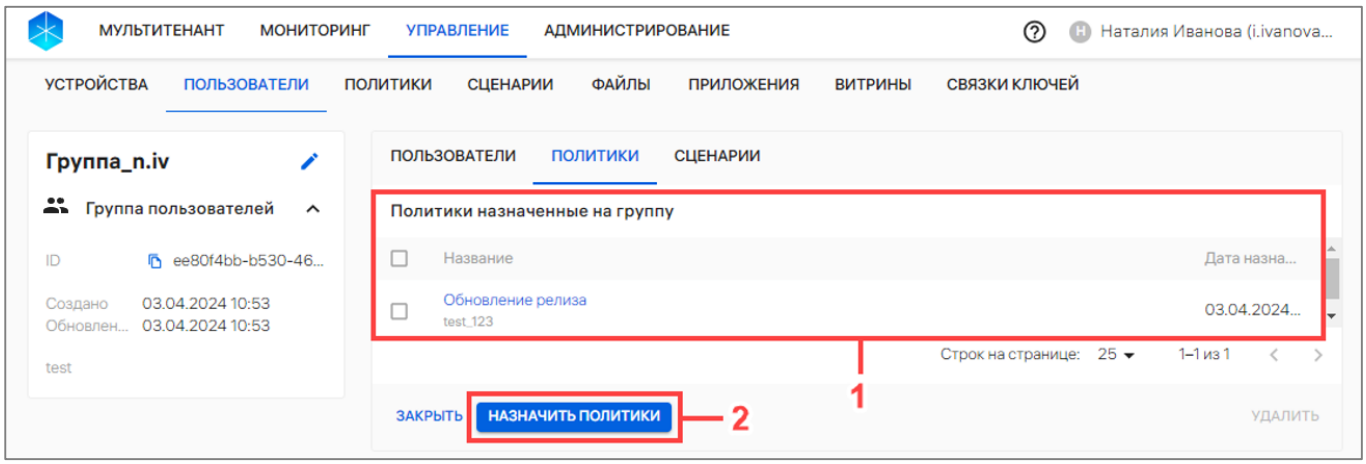

Рисунок 40

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 п. 2.5.2.4 и п. 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.

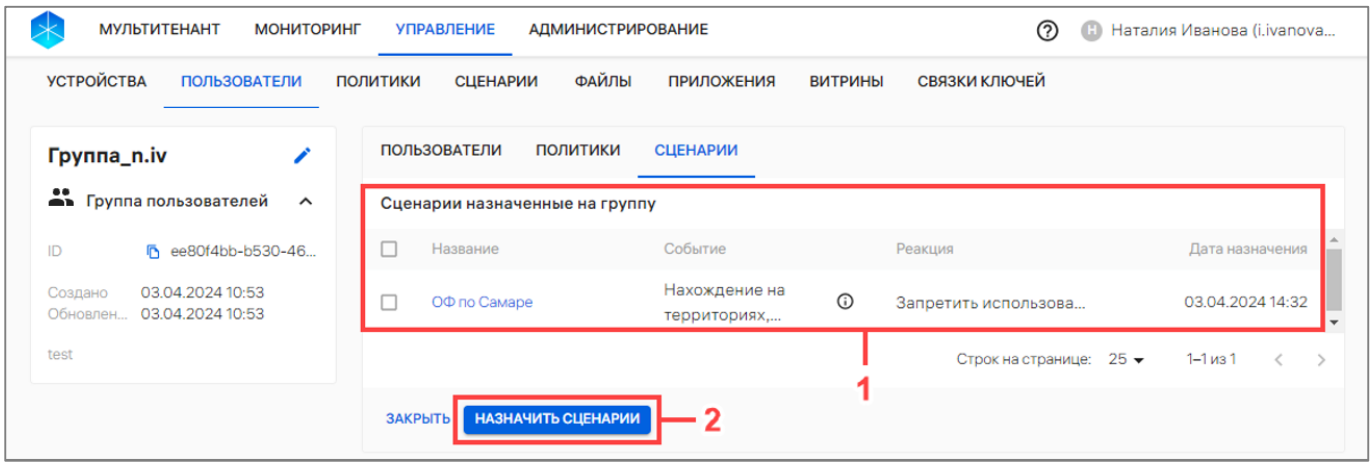

Рисунок 41

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 40)
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).

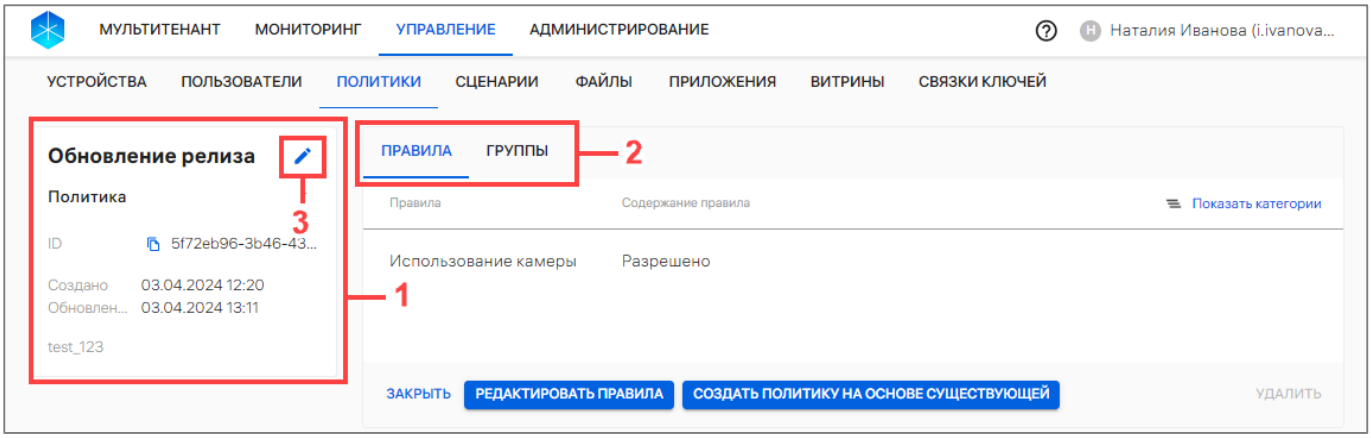

Рисунок 42

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).

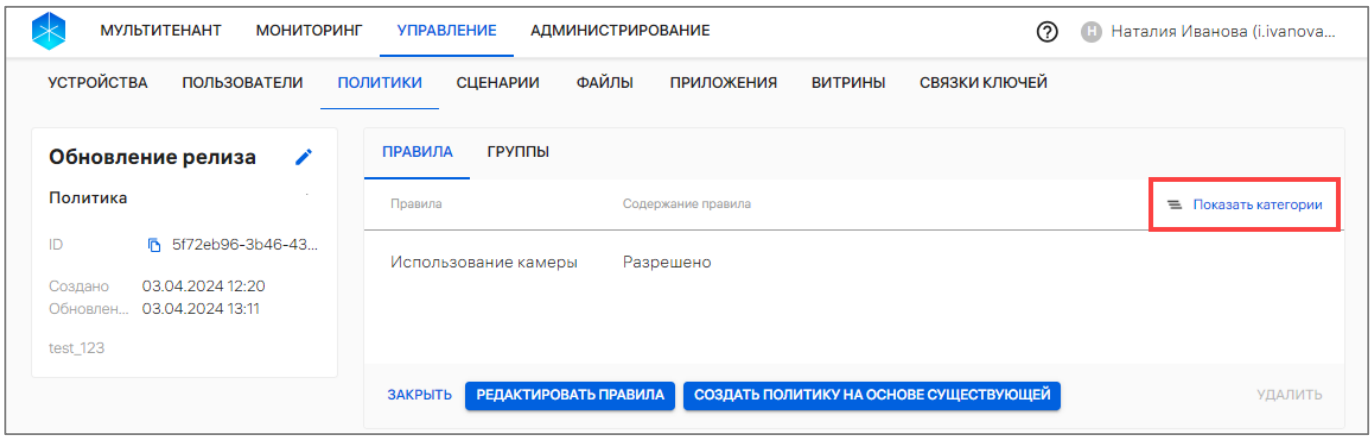

Рисунок 43

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]).

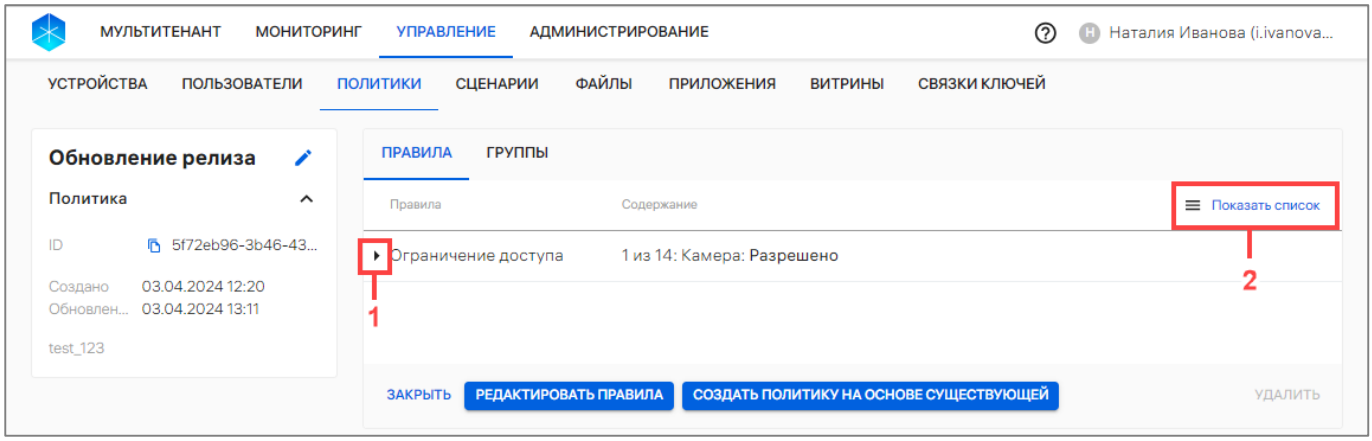

Рисунок 44

Набор правил политики подлежит редактированию. Процесс редактирования приведен в п. 2.4.5.

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. 2.4.6.1 и п. 2.4.7.1.

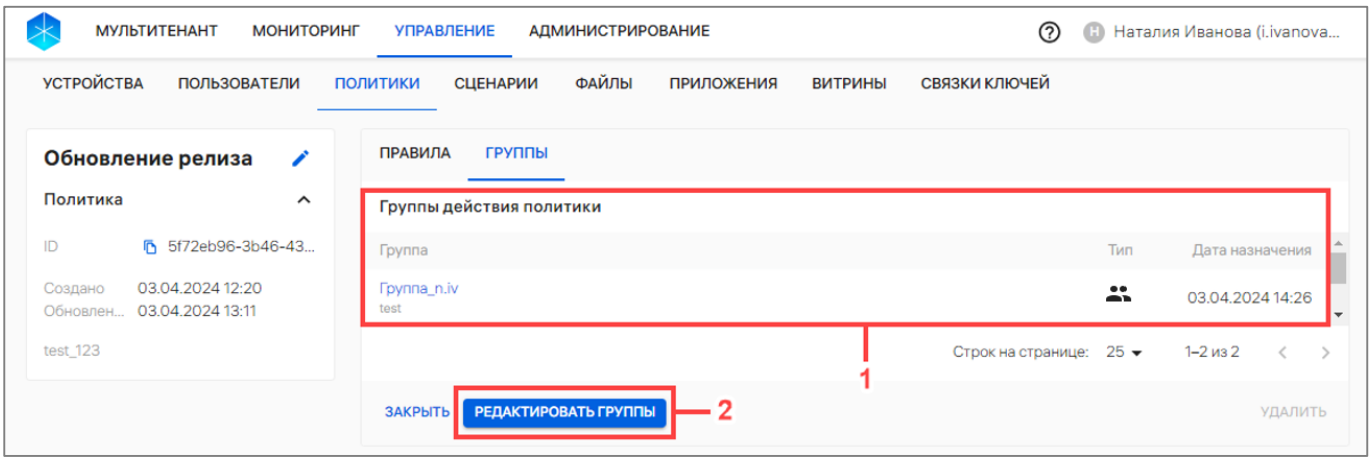

Рисунок 45

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 40)
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»
Реакция	Доступные значения приведены в таблице (Таблица 40)
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]).

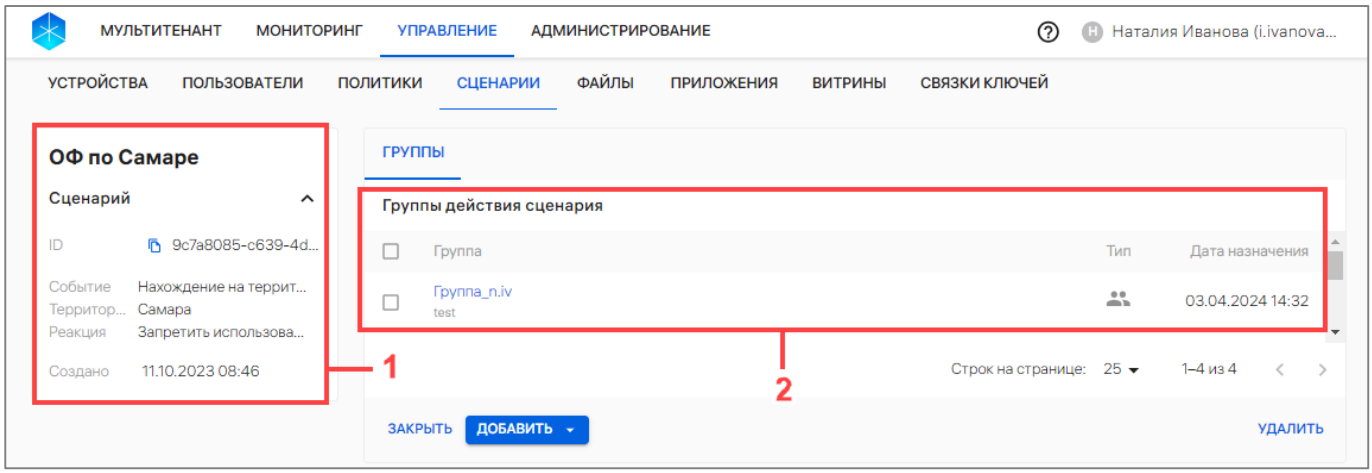

Рисунок 46

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

2.2. 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 47 [2]).

ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 47 [1]).

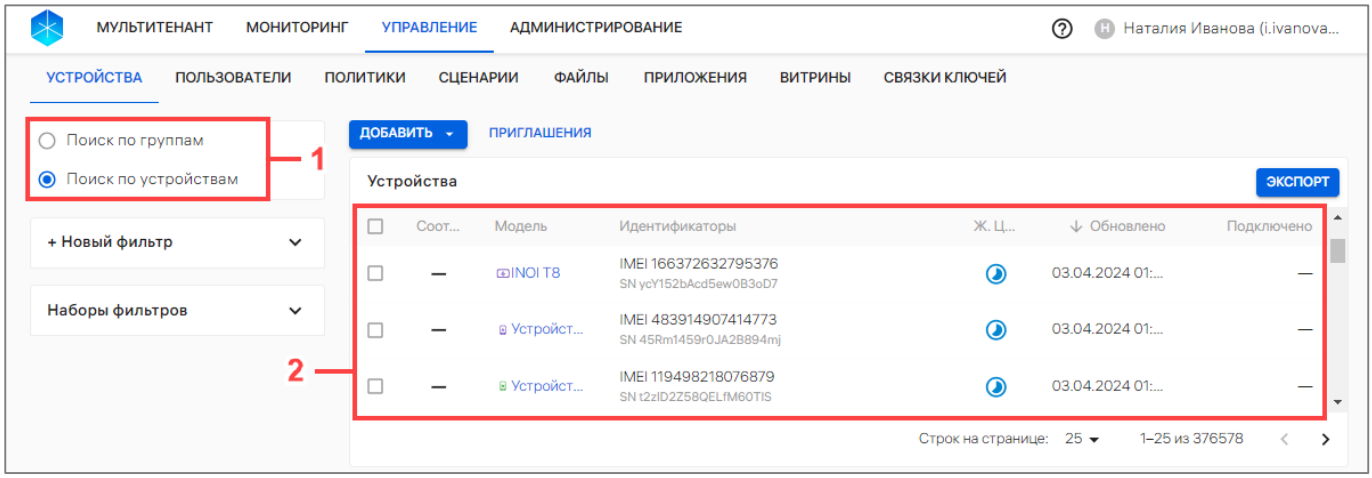

Рисунок 47

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, приведенных в таблице (см. Таблица 11), а при отсутствии добавленных об устройствах или групп устройств отображается сообщение «Нет данных».

При выборе в области фильтров «Поиск по группам» (Рисунок 48 [1]) информация о группах устройств в рабочей области отображается в столбцах (Рисунок 48 [2]), приведенных в таблице (Таблица 24).

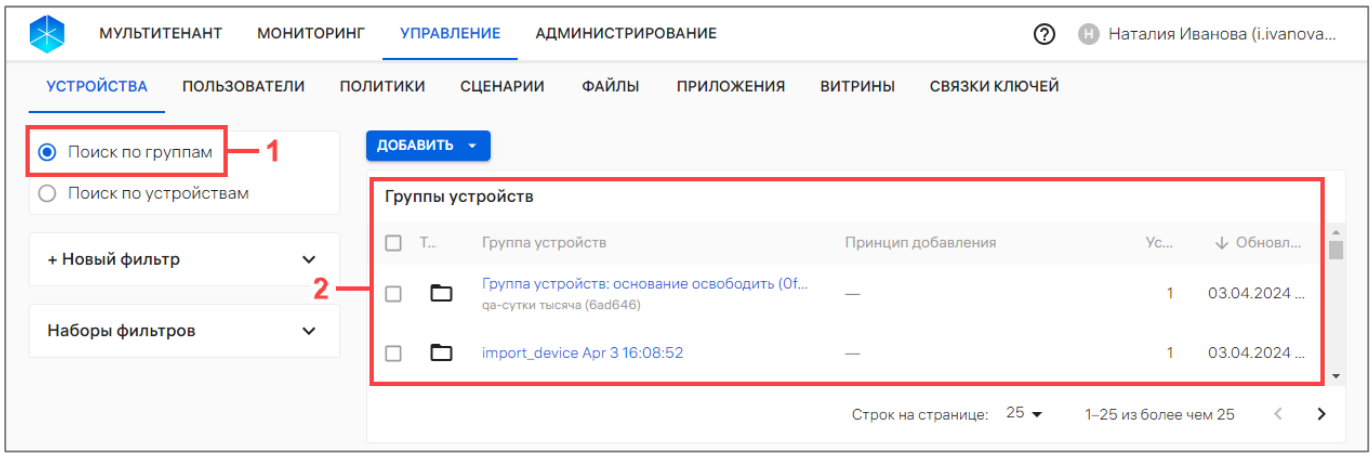

Рисунок 48

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

Таблица 24

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	Значения, 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 п. 2.2.1.1 и 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 49);

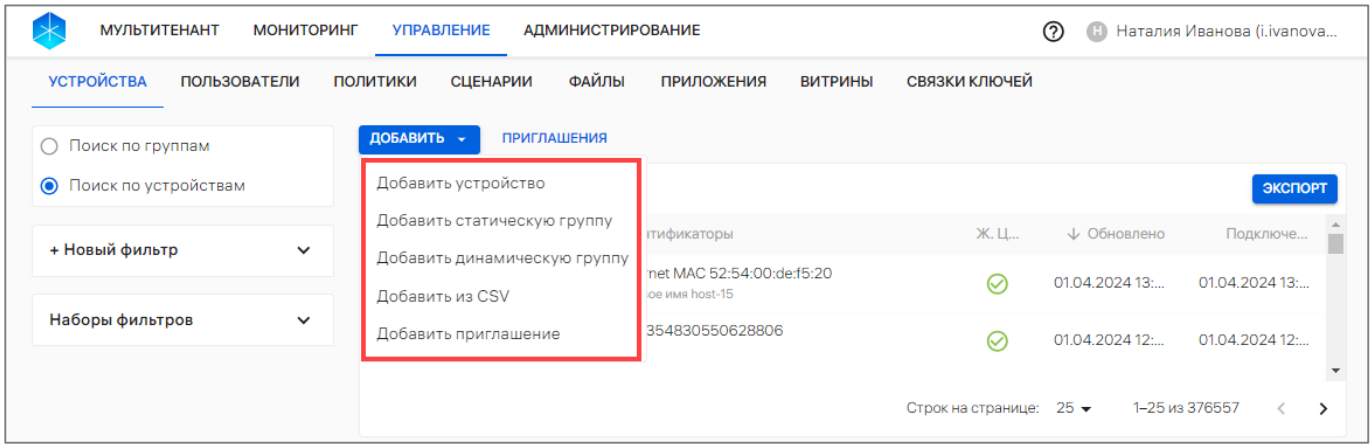

Рисунок 49

– в открывшемся окне (Рисунок 50) заполнить поля, приведенные в таблице (Таблица 25).

ПРИМЕЧАНИЕ. Для отображения полей «IMEI», «Серийный номер», «Ethernet MAC», «WLAN MAC» необходимо установить галочку в чекбоксе напротив требуемого параметра. После ввода значения необходимо нажать Enter на клавиатуре и при необходимости добавить второй для полей «IMEI», «Ethernet MAC», «WLAN MAC». Если необходимо удалить параметр, то нажать на значок справа от значения, а для полной очистки нажать на значок «Очистить» в правом конце поля;

– после ввода значений необходимо подтвердить либо отменить действия.

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

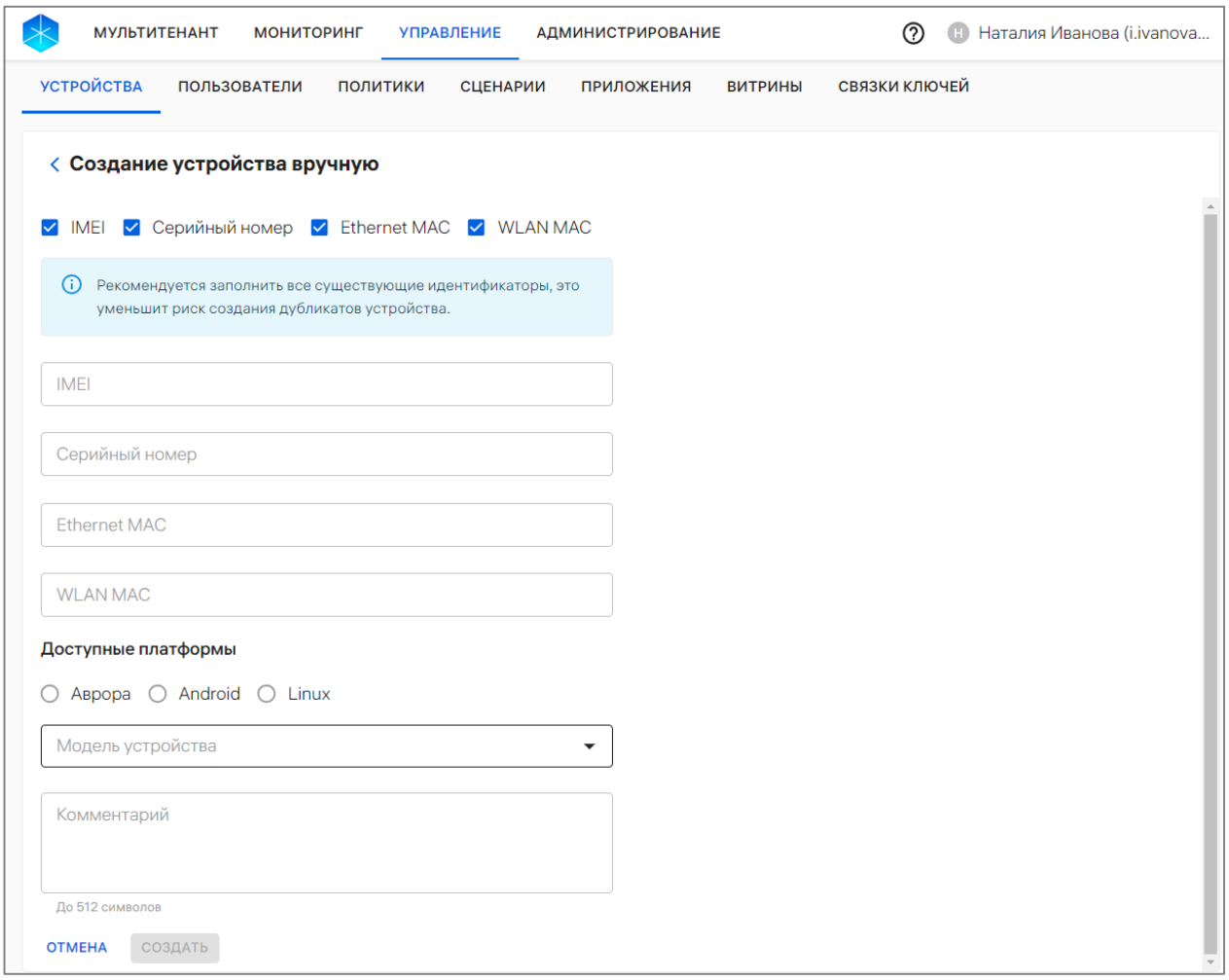

Рисунок 50

Таблица 25

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 производителем. Может содержать от 1 до 20 символов.	

Параметр	Значения	Описание
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
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 устройство в ПУ и активировать его.

ВНИМАНИЕ! Для успешного прохождения процесса необходимо, чтобы устройство не было добавлено и активировано в ПУ.

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 следующих документах:

- «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;
- «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;
- «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux»;

– не переименовывая приглашения (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 завершение 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 49);

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

– подтвердить либо отменить действия.

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

Таблица 26

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

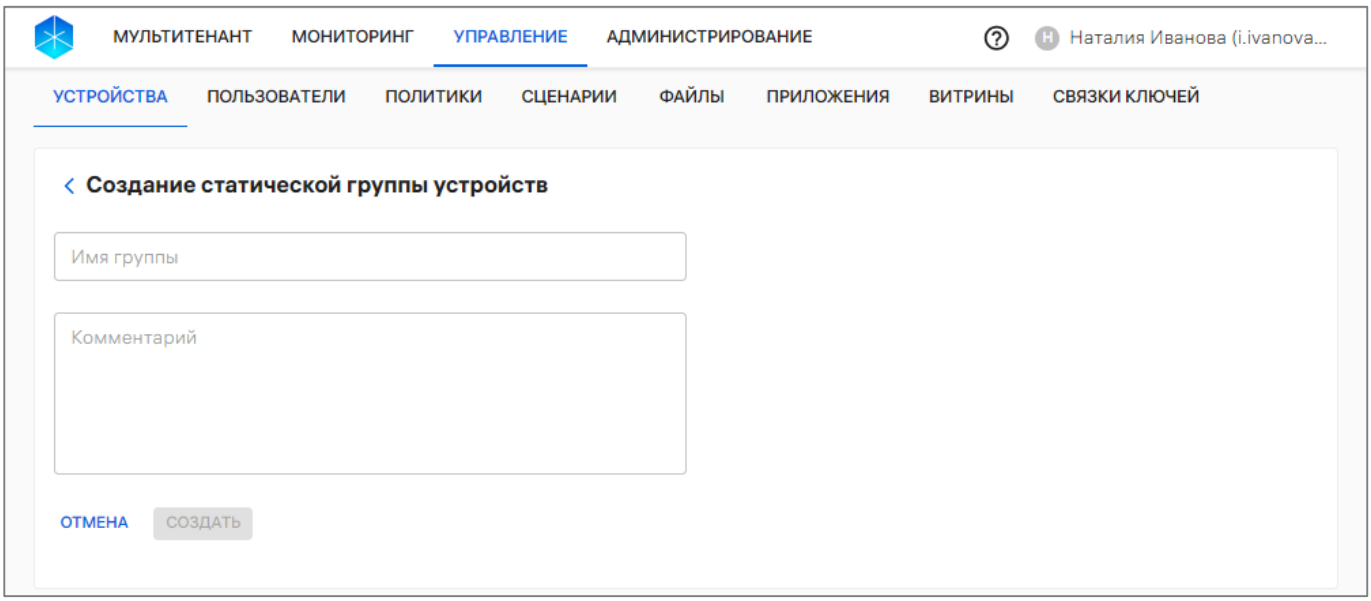

Рисунок 51

2.2.2.2. Добавление динамической группы устройств

Динамическая группа устройств — это группа с заданными условиями, при соблюдении которых устройства 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).

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 49);

– в открывшемся окне (Рисунок 52 [1]) заполнить поля, приведенные в таблице (см. Таблица 26);

– задать значения параметров, приведенных в таблице (Таблица 27) по которым устройства будут добавлены в динамическую группу (Рисунок 52 [2]);

– подтвердить либо отменить действия.

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.

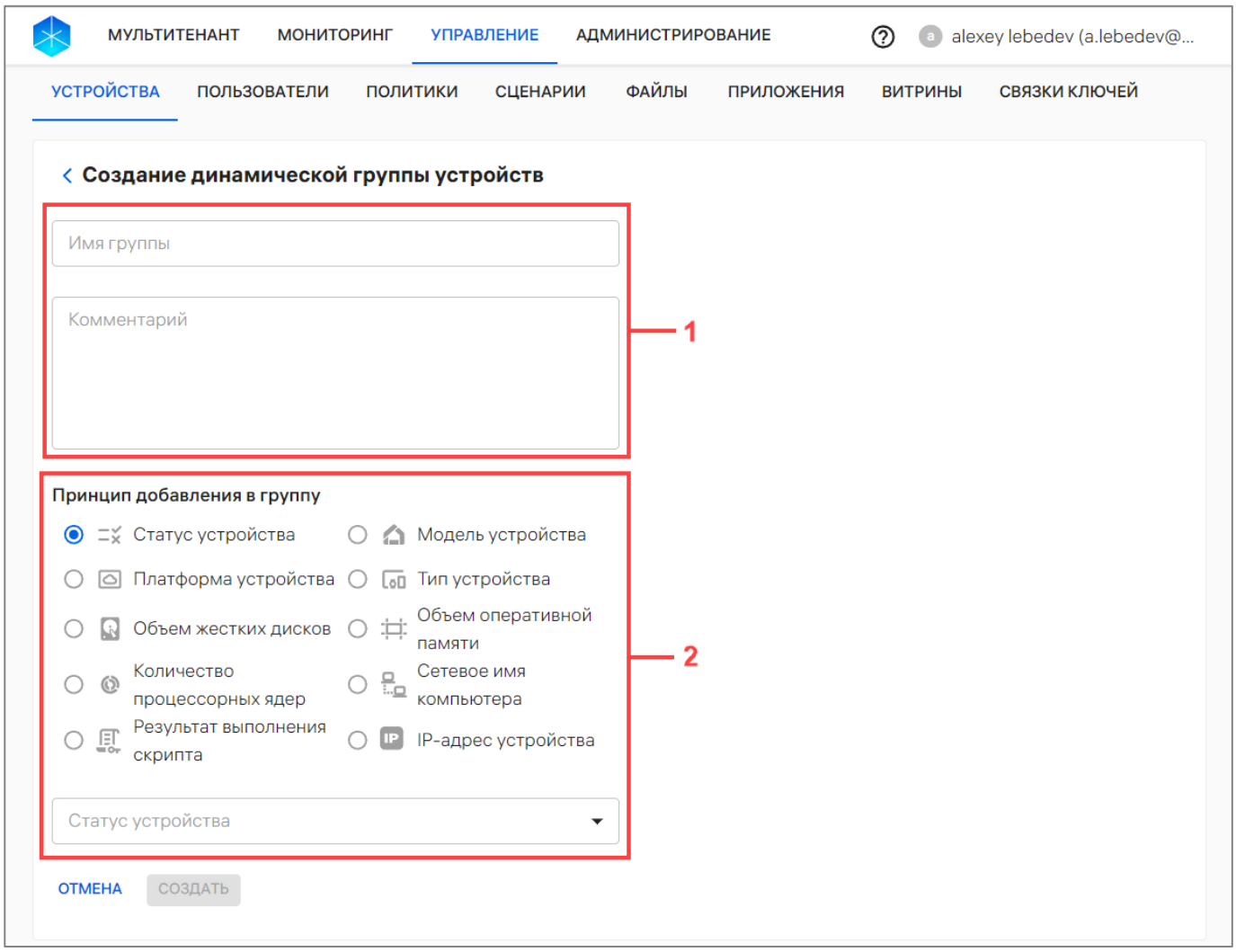

Рисунок 52

Таблица 27

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
Платформа устройства	Выбор значения из раскрывающегося списка: – Аврора; – Android; – Linux

Параметр	Значение
Объем жестких дисков. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Указать объем жесткого диска устройств в формате: – «От» (МиБ); – «До» (МиБ). **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал
Количество процессорных ядер. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Указать количество процессорных ядер устройств в формате: – «От»; – «До». **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал
Результат выполнения скрипта. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС Android и ОС семейства Linux	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 `OMP_SCRIPT_RESULT_FILE`. Подробнее в приложении (Приложение 3)
Модель устройства	Выбор устройства из раскрывающегося списка
Тип устройства	Выбор типа устройства из раскрывающегося списка: – Планшет; – КПК; – Смартфон; – Неизвестный тип устройства; – ПК
Объем оперативной памяти. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Указать объем оперативной памяти устройств в формате: – «От» (МиБ); – «До» (МиБ). **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал
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 (.).

Параметр	Значение
	Максимальная длина 253 символа, а длина от начала строки до первой точки не должна превышать 63 символа. Если необходимо вести маску сетевого имени, необходимо ограничить ее звездочкой (*) в начале, внутри и/или в конце части сетевого имени
IP-адрес устройства	Указать интервал IP-адресов: – «Начальный адрес»; – «Конечный адрес». **ПРИМЕЧАНИЕ.** Конечный адрес не включается в интервал

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 49);

– в открывшемся окне нажать «Шаблон .CSV » (Рисунок 52), в результате чего шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 28).

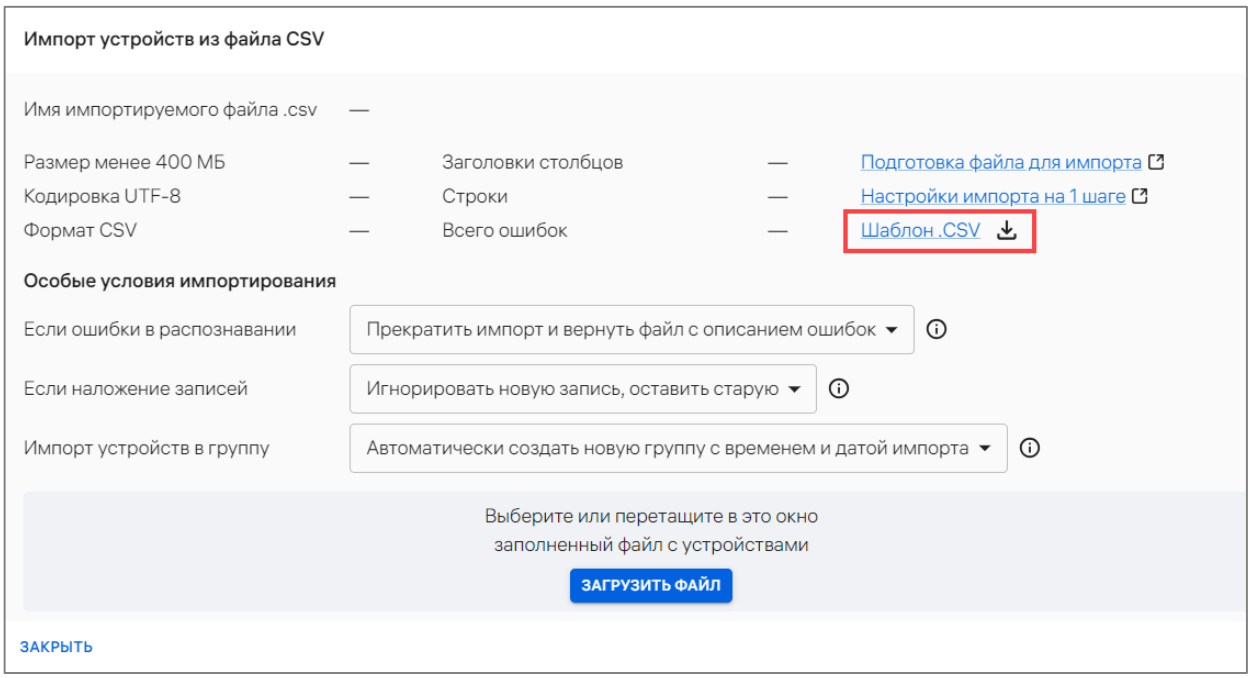

Рисунок 52

Пример заполненного CSV-файла:

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

Также возможно заполнить CSV-файл в табличном виде (Рисунок 53).

Пример:

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

Рисунок 53

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 рекомендуется иметь 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;

– 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 COMMENT может быть добавлен необязательный столбец STRATEGY. Он заполняется в случае необходимости 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 (0xFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «a».

Описание требований к значениям параметров приведены в таблице (Таблица 28).

Таблица 28

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. **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

Параметр	Описание	Примечание
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. **ПРИМЕЧАНИЕ.** Если поле MAC WLAN не заполнено, то после успешной активации значение MAC WLAN отобразится в карточке устройства автоматически
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
STRATEGY	Правило разрешения конфликтующих записей. Доступные значения: – **SKIP** или **S** – в результате конфликтующая запись не будет перезаписана. Если файл содержит несколько одинаковых записей об устройстве, но с разными группами,	Параметр не обязателен для заполнения. Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта

Параметр	Описание	Примечание
	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 отвязано от всех групп, в которых оно состояло ранее в системе, и привязано ко всем группам из файла	

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 49);

– в открывшемся окне задать особые условия импорта, приведенные в таблице (Таблица 29);

Таблица 29

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 54 [1]): – **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:	В поле содержится подсказка, доступная для 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

Наименование полей	Описание	Примечание
	• файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств	
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 54 [2]): – **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. **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	
Импорт устройств в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 54 [3]):	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ. В результате отобразится текст

Наименование полей	Описание	Примечание
	– **Автоматически создать новую группу с временем и датой импорта** – в результате будет создана новая группа устройств (с типом «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	подсказки следующего содержания: в процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую

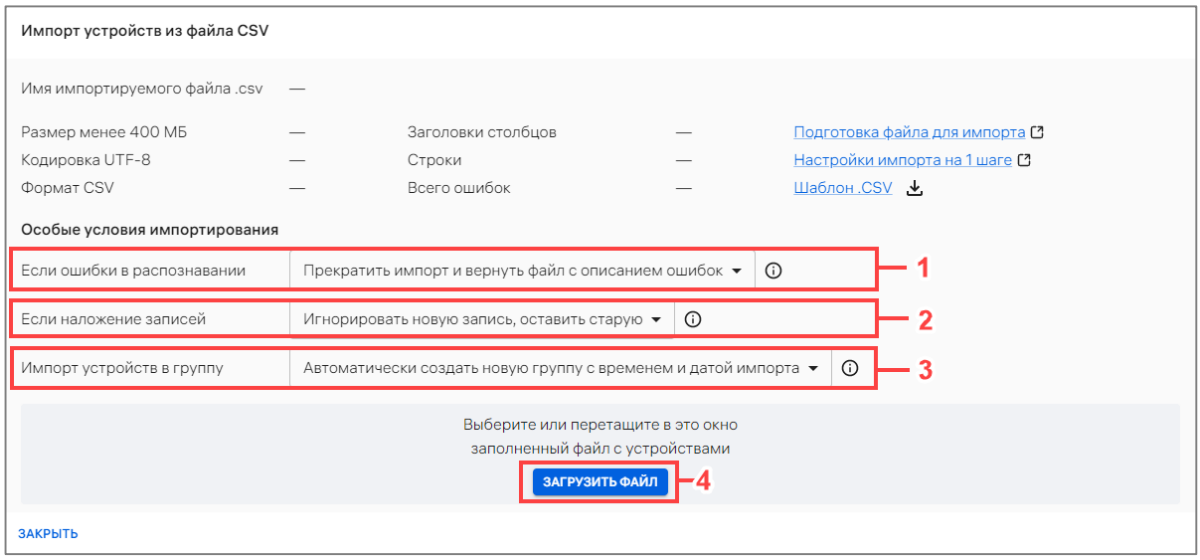

Рисунок 54

– далее необходимо загрузить CSV-файл одним из способов:
  - переместить CSV-файл в область загрузки;
  - нажать кнопку «Загрузить файл» (см. Рисунок 54 [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 55).

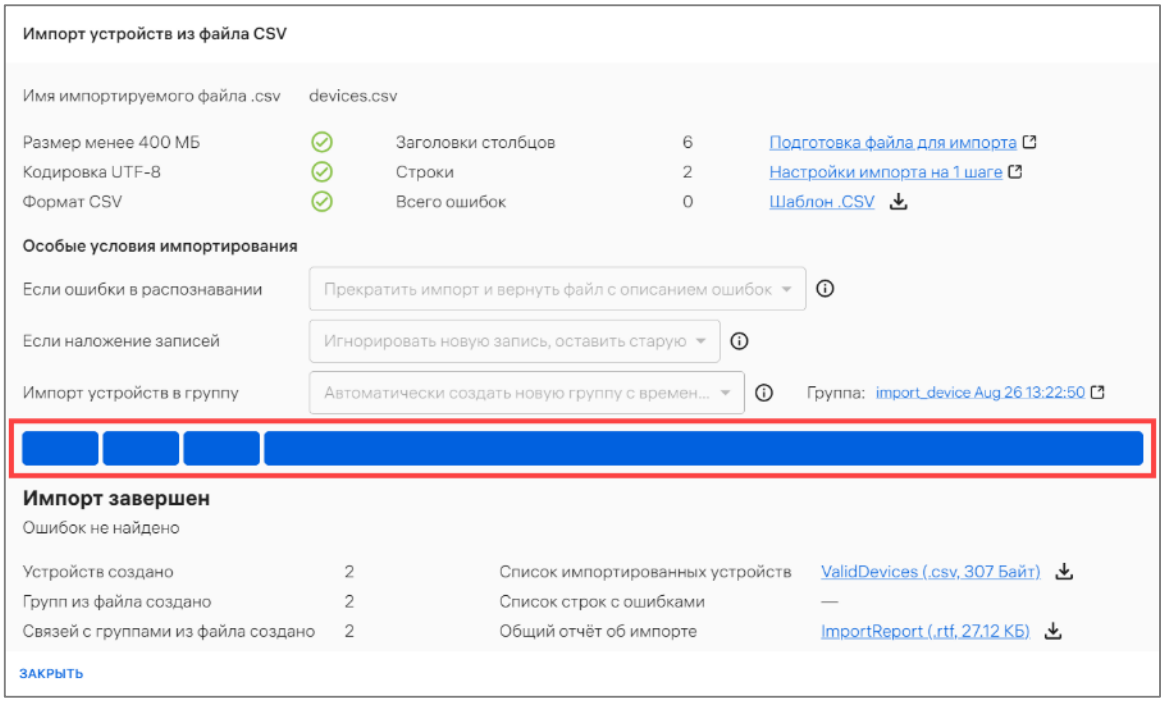

Рисунок 55

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 56 [6]).

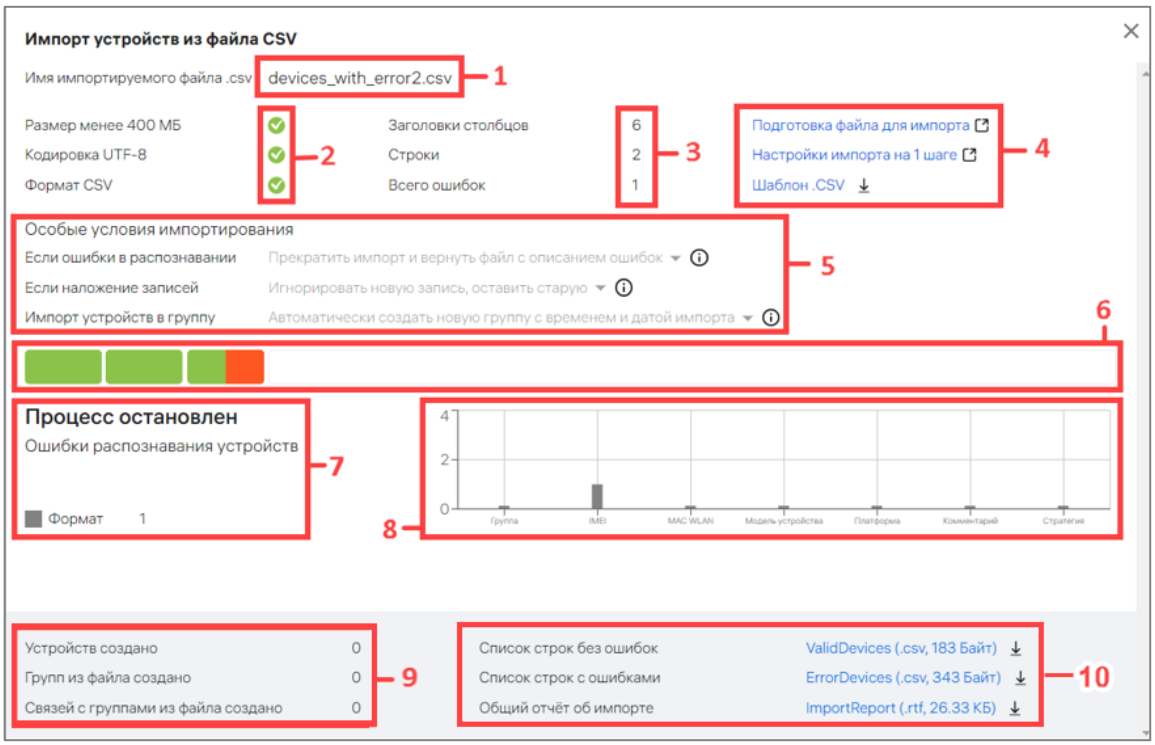

Рисунок 56

В окне с результатами импорта устройств отображается следующая информация:

– название импортируемого файла (см. Рисунок 56 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 56 [2]);

– количество столбцов, всех импортируемых строк и ошибок в файле (Рисунок 56 [3]);

– ссылки (см. Рисунок 56 [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 56 [5], см. Таблица 29);

– шкала прогресса импорта (см. Рисунок 56 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (см. Рисунок 56 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (см. Рисунок 56 [8]);

– количество добавленных устройств, групп устройств и их связей (см. Рисунок 56 [9]);

– ссылки на скачивание отчетов (см. Рисунок 56 [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 3.1.

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 49);

2) Перейти в список приглашений, нажав на кнопку «Приглашения» (Рисунок 57), и на отобразившейся странице нажать на кнопку «Добавить приглашение» (Рисунок 58).

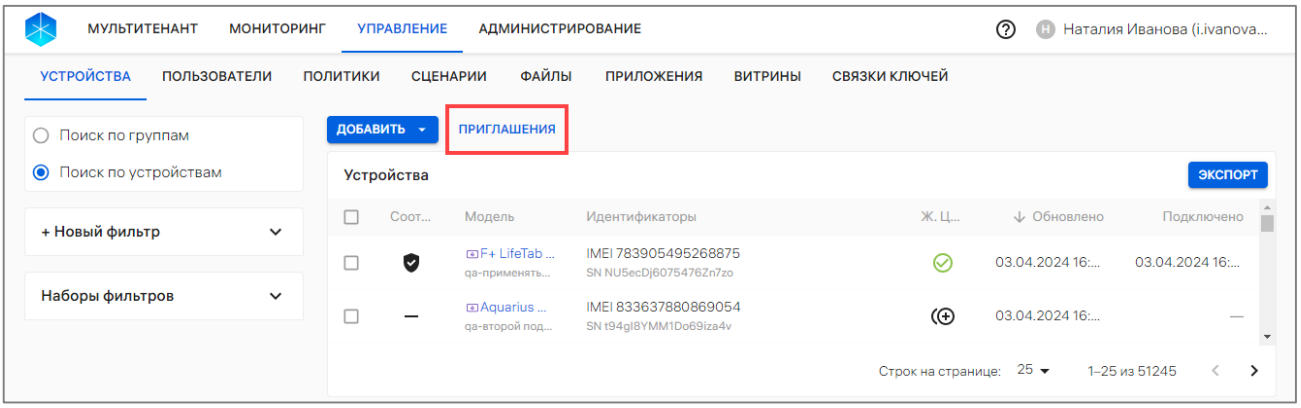

Рисунок 57

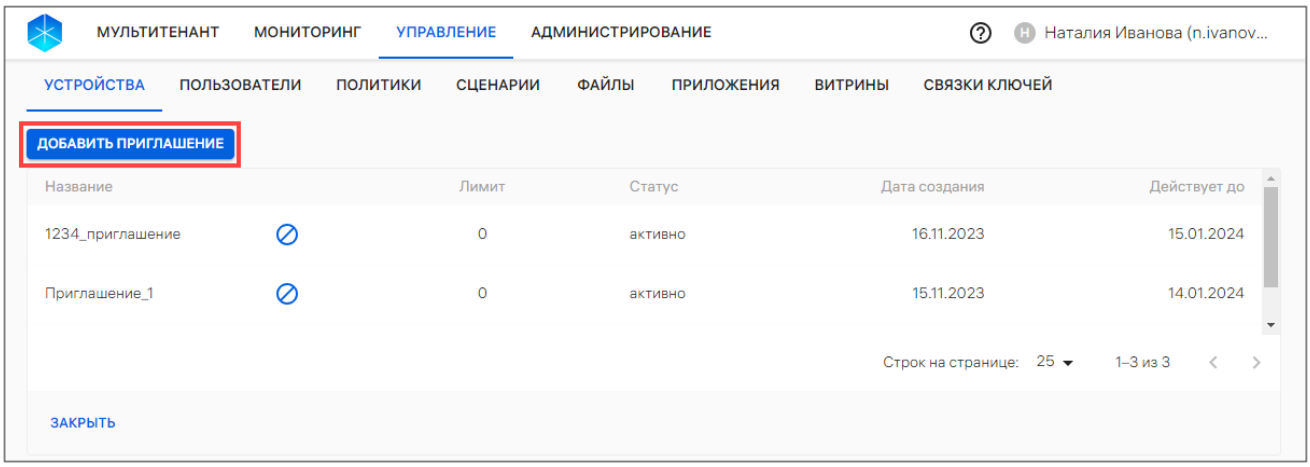

Рисунок 58

В результате в отобразившемся окне (Рисунок 59) необходимо заполнить поля:

– «Название». Ввод значения с клавиатуры. Может содержать от 1 до 50 символов;

– «Лимит переиспользования приглашения в сутки». Ввод значения с клавиатуры. Может быть от 0 до 1 000 000.

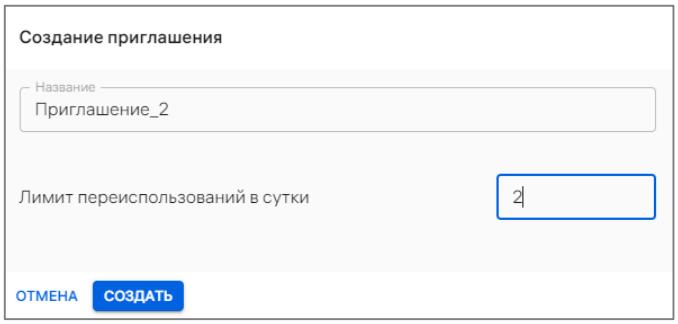

Рисунок 59

После выполнения указанных действий необходимо подтвердить или отменить действие.

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

– лимит переиспользования приглашения в сутки (Рисунок 60 [1]);

– QR-код (Рисунок 60 [2]), 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-файл» (см. Рисунок 60 [3]), 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 60 [4]), при нажатии на которую отобразится предупреждающее сообщение (Рисунок 61), где необходимо подтвердить или отменить действие.

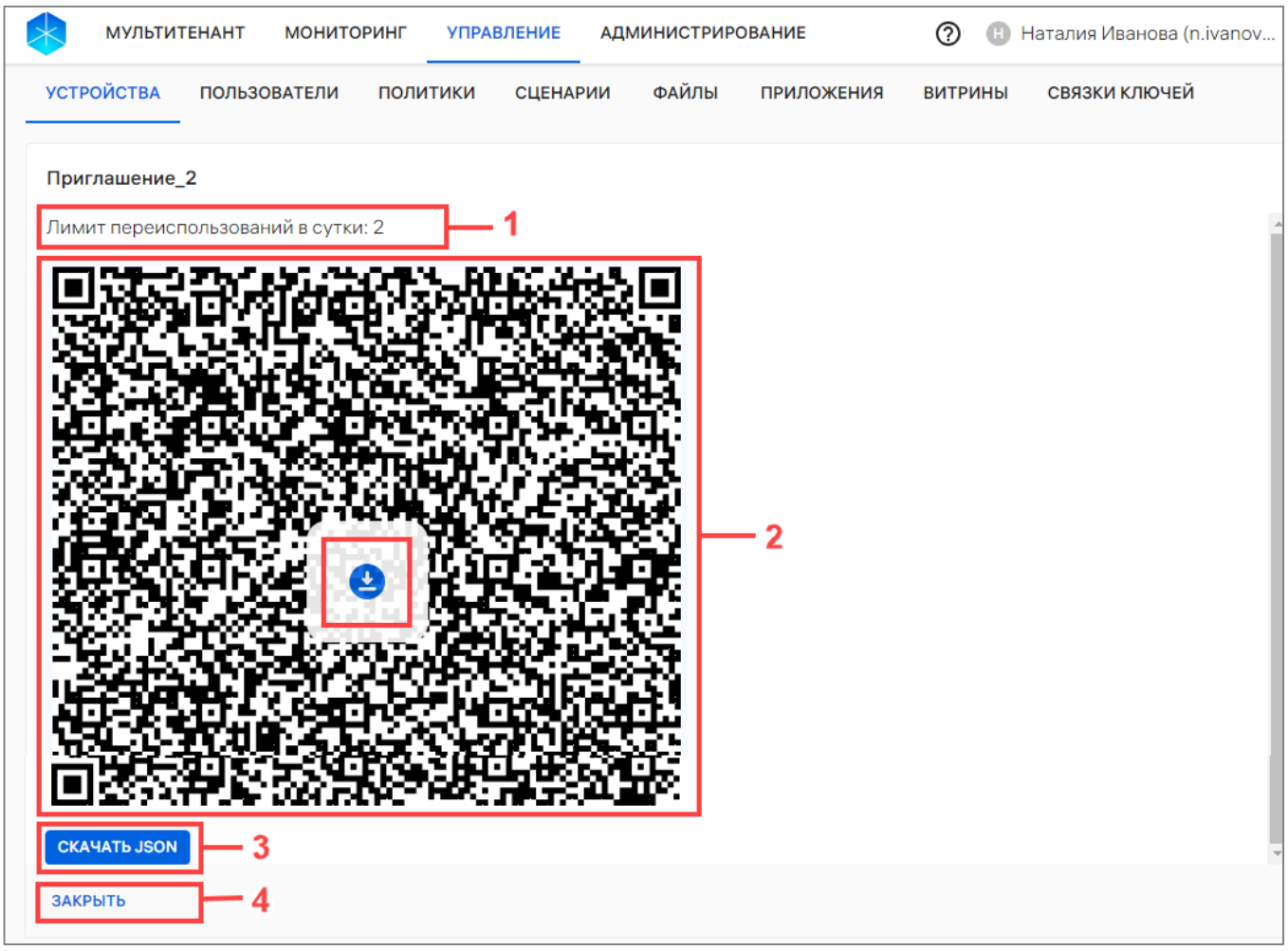

Рисунок 60

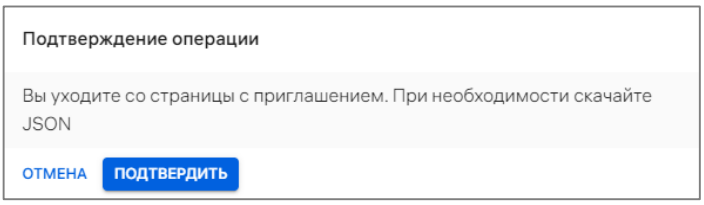

Рисунок 61

Приглашение имеет название `invite.json`.

Пример содержания JSON-файла:

{"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{"accessToken":"ed776WJVIKVTocq78","inviteTakeupURL":"http://ocs.ompcloud.ru/emm/mobile/api/deviceInvites/897eae828/takeUp","trustedCerts":""},"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.ompcloud.ru/emm/mobile/clientDownload","android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"bZ41Av7s6nrQpXjB2Pg5oKfKL5xPxhLevsESkkVLfg4","android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true}

ВНИМАНИЕ!

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

✓ Не рекомендуется изменять название и форматировать сгененированный 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.

При выходе из карточки приглашения осуществится переход на страницу со списком приглашений, на которой доступно отозвать созданное приглашение, нажав на значок ⊘ «Отозвать» (Рисунок 62 [1]), а также возможно просмотреть информацию о каждом приглашении, которые отображаются в следующих столбцах (Рисунок 62 [2]):

– «Название» - название приглашения;

– «Лимит» - лимит переиспользований приглашения в сутки;

– «Статус» - статус активности приглашения. Возможные значения:

- «Активно»;
- «Приостановлено»;
- «Отозвано»;

– «Дата создания» - дата создания приглашения;

– «Действует до» - дата, до которой действует токен доступа, соответствующий приглашению.

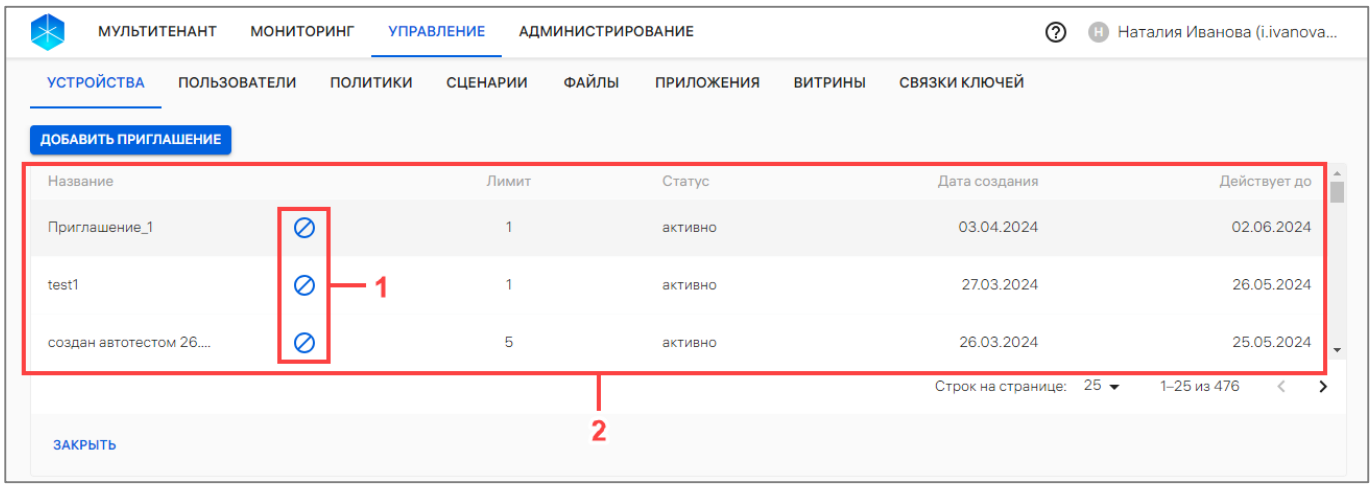

Рисунок 62

2.2.5. 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 63);

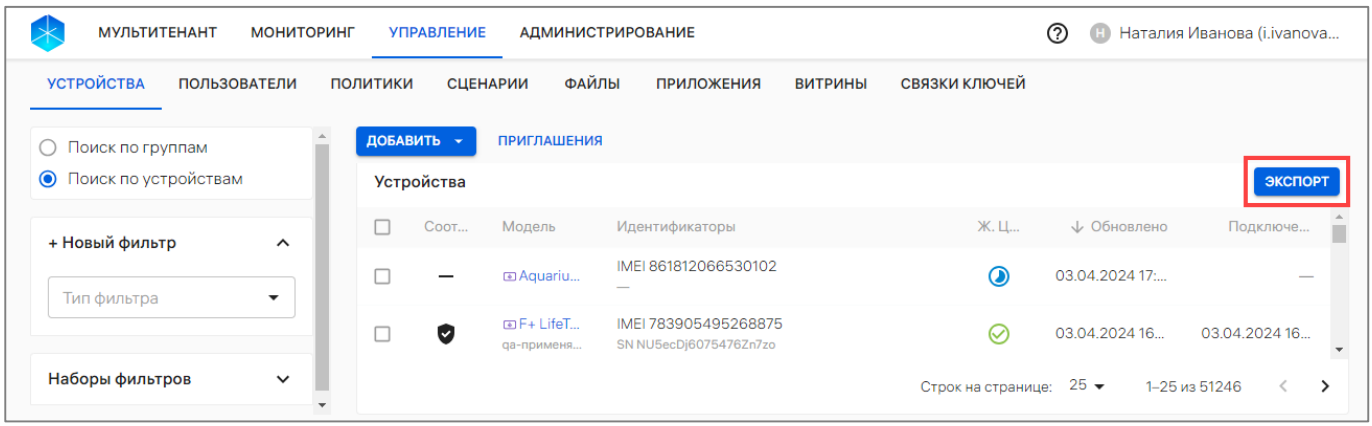

Рисунок 63

– в отобразившемся окне подтверждения экспорта устройств подтвердить либо отменить действия (Рисунок 64).

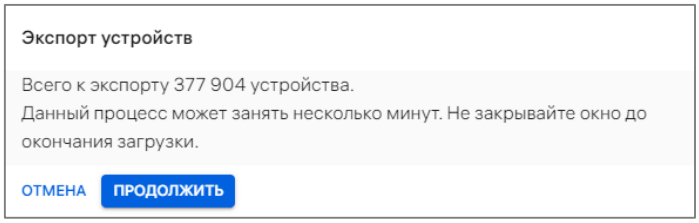

Рисунок 64

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;

– **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).

2.2.6. 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. 2.2.6.1);
– с помощью быстрых действий в списке пользователей (пп. 2.3.5.1);
– вручную через карточку устройства (пп. 2.2.6.2);
– 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.

2.2.6.1. 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 65 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям» (Рисунок 65 [2]);

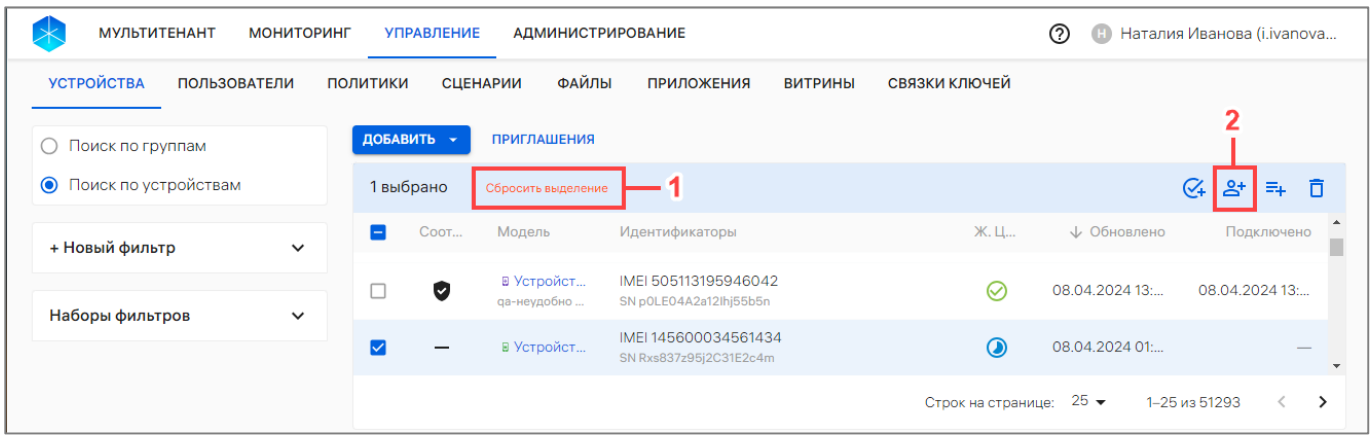

Рисунок 65

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте либо телефону пользователя (Рисунок 66 [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 66 [3]);

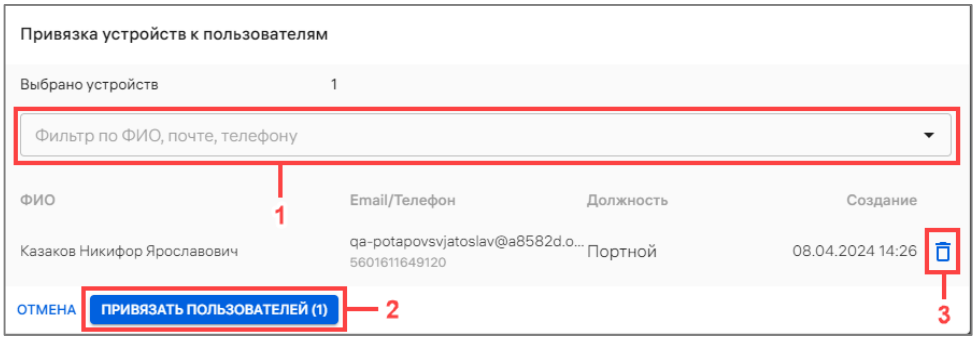

Рисунок 66

– нажать кнопку «Привязать пользователей» (см. Рисунок 66 [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).

2.2.6.2. Привязка устройства к пользователю из карточки устройства

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

– 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 66) выполнить действия, описанные в пп. 2.2.6.1.

2.2.7. Привязка устройств к группе устройств

В Консоли администратора ПУ предусмотрены 2 типа групп устройств:

– динамическая – это 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 – это группа, созданная Администратором Платформы управления. Состав группы изменяется Администратором Платформы управления.

Осуществить привязку устройств к статической группе можно с помощью:

– списка быстрых действий (пп. 2.2.7.1);

– карточки устройства (пп. 2.2.7.2);

– карточки группы устройств (пп. 2.2.7.3);

– 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).

2.2.7.1. 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 67 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к группам» (Рисунок 67 [2]);

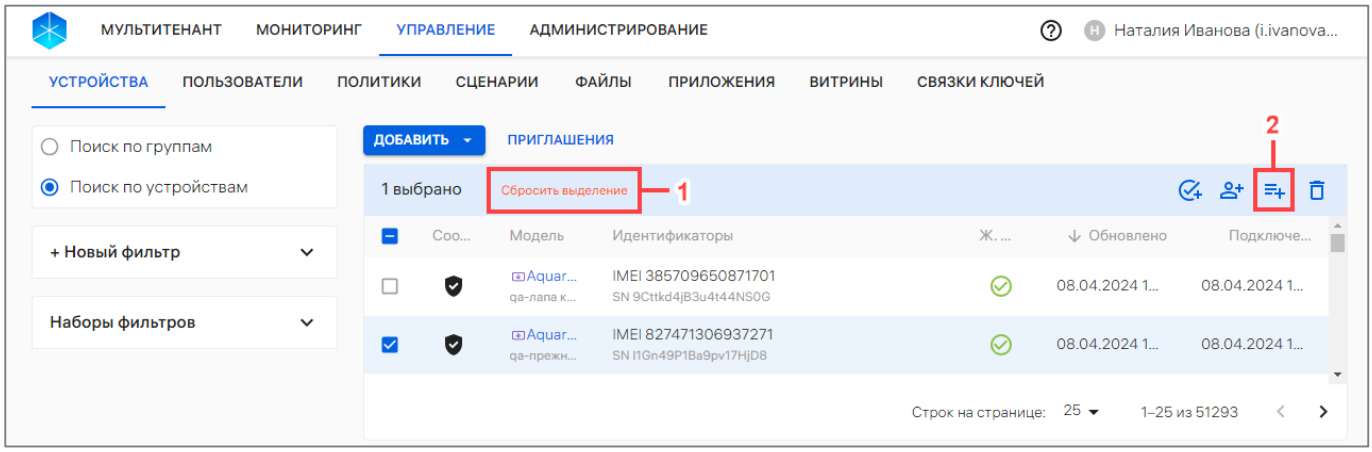

Рисунок 67

– в отобразившемся окне выбрать необходимую группу устройств из раскрывающегося списка (Рисунок 68 [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 68 [3]);

Рисунок 68

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 69 [1]) и нажав кнопку «Создать статическую группу» (Рисунок 69 [2]);

Рисунок 69

– нажать кнопку «Добавить в группы» (Рисунок 68 [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.

2.2.7.2. 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. 2.2.7.1.

В результате успешной привязке устройства к группе отобразится соответствующее сообщение.

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

2.2.7.3. 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. 2.2.7.1.

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

2.2.8. Активация устройств

Для активации устройств в Консоли администратора ПУ необходимо сгенерировать QR-код, после чего статус устройств 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.

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 документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;

– «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

Активация устройств возможна следующими способами:

– вручную (пп. 2.2.8.1), если необходимо самостоятельно активировать 1 устройство;

– с помощью списка быстрых действий (пп. 2.2.8.2), если необходимо активировать несколько устройств;

– с помощью отправки QR-кода на Email (пп. 2.2.8.3), если необходимо, чтобы пользователи активировали свои устройства самостоятельно;

– с помощью загрузки JSON-файла (пп. 2.2.8.4), 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».

2.2.8.1. 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 70).

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

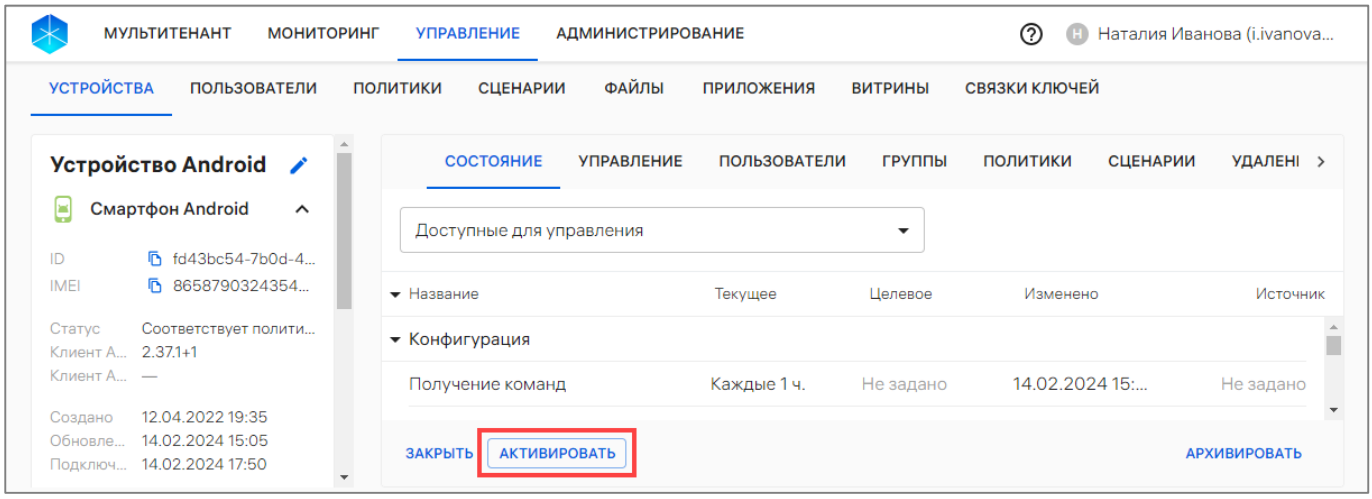

Рисунок 70

– отобразится окно активации устройств (Рисунок 71);

– 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 71 [1]) и нажать кнопку «Дальше» (Рисунок 71 [2]);

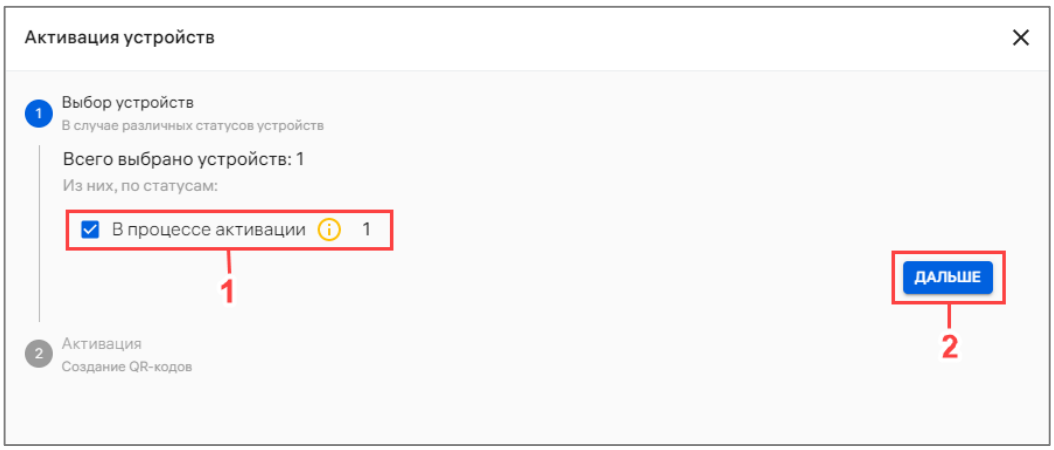

Рисунок 71

– откроется окно, где необходимо нажать кнопку «Активация вручную» (Рисунок 72);

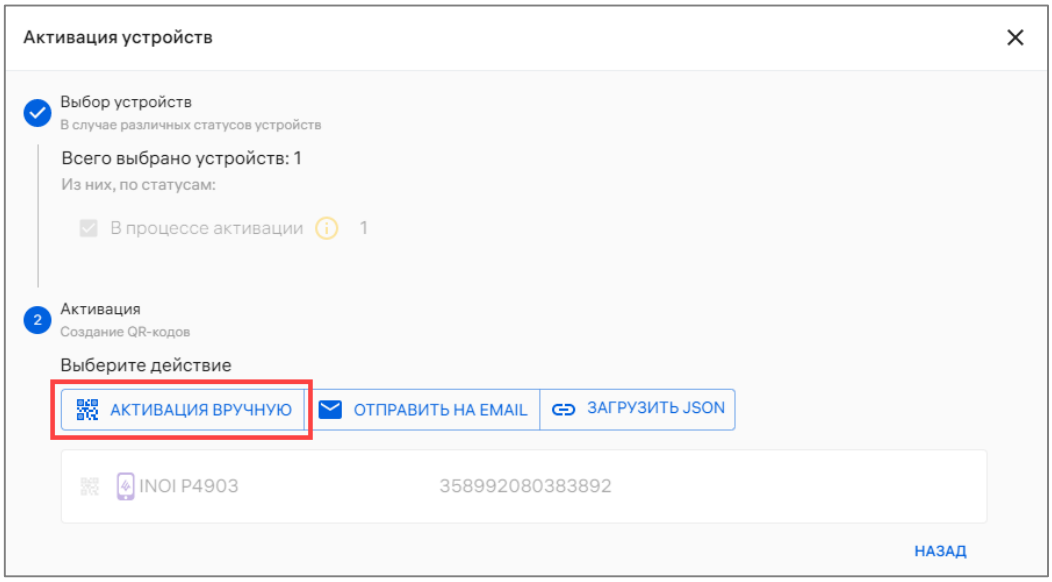

Рисунок 72

– в результате отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (Рисунок 73).

Рисунок 73

В результате успешного создания QR-кода будет отображена следующая информация (Рисунок 74):

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

– пароль, присваиваемый созданной учетной записи устройства;
– дата истечения QR-кода;
– адрес процесса - адрес сервера для процесса активации устройства;
– контрольная сумма MD5;
– название компонента (актуально для устройств с ОС Android);
– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр» (актуально для устройств с ОС Android).

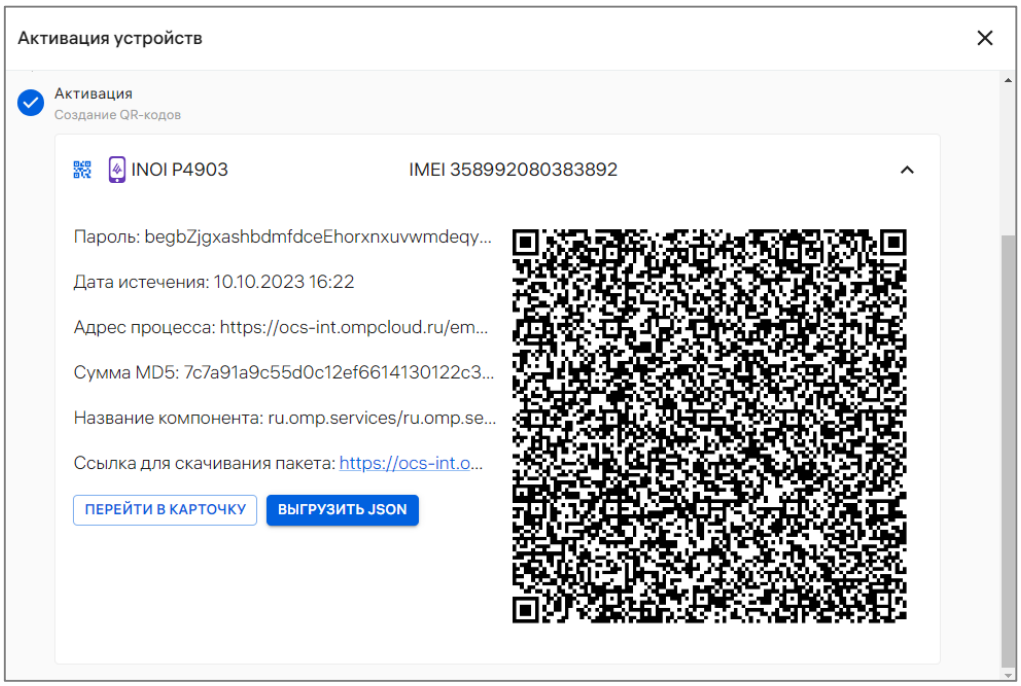

Рисунок 74

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.

2.2.8.2. 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 75 [1]);

– в списке быстрых действий выбрать значок «Активация устройств» (Рисунок 75 [2]).

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

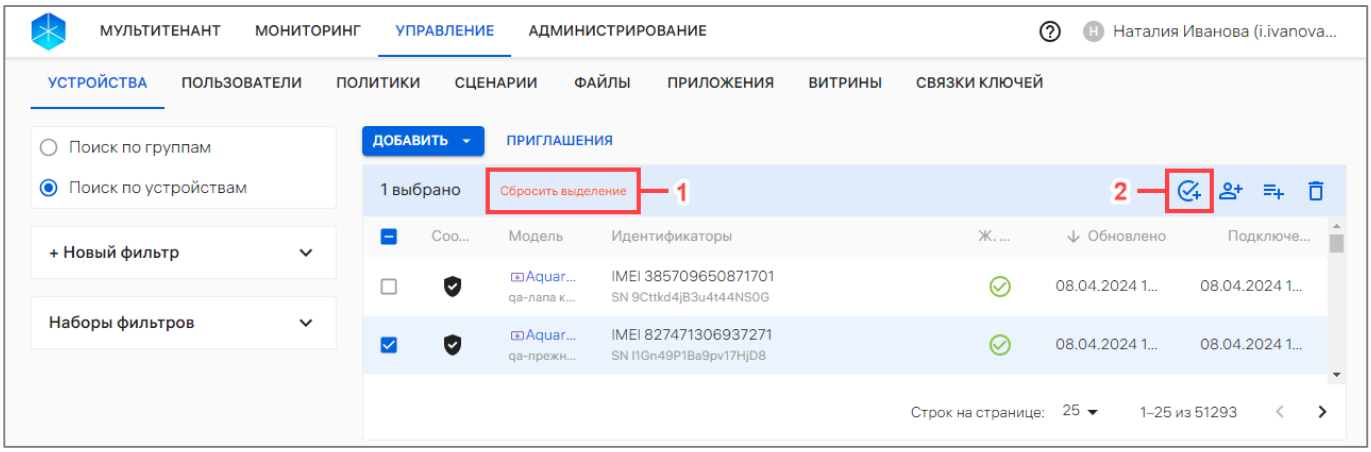

Рисунок 75

– отобразится окно активации устройств (см. Рисунок 71);

– 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 71 [1]) и нажать кнопку «Дальше» (см. Рисунок 71 [2]);

– в открывшемся окне необходимо нажать кнопку «Активация вручную» (см. Рисунок 72);

– отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (см. Рисунок 73).

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 76 [1], Рисунок 76 [2]), который необходимо отсканировать в приложении «Аврора Центр» на каждом устройстве;

– пароль, присваиваемый созданной учетной записи устройства;

– дата истечения QR-кода;

– адрес процесса - адрес сервера для процесса активации устройства;

– контрольная сумма MD5;

– название компонента (актуально для устройств с ОС Android);

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр» (актуально для устройств с ОС Android).

ПРИМЕЧАНИЕ. Установка приложения «Аврора Центр» и активация устройства будут автоматически выполняться при первоначальной настройке устройства с ОС Android (подробнее в документе «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android») и при корпоративной привязке устройства с ОС Аврора (подробнее в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора») к ПУ. В остальных случаях QR-код можно использовать только для активации устройства.

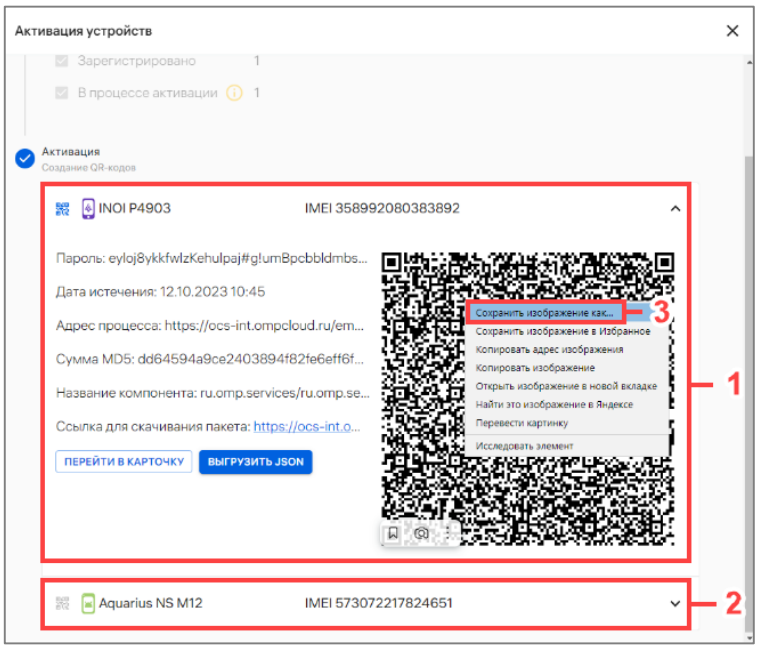

Рисунок 76

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».

QR-код можно скопировать, нажав на него правой кнопкой мыши, и выбрать из списка пункт «Сохранить картинку как...» (см. Рисунок 76 [3]), 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 документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.8.3. 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 75 [1]);

– в списке быстрых действий выбрать значок «Активация устройств» (см. Рисунок 75 [2]).

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

– отобразится окно активации устройств (см. Рисунок 71);

– 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 71 [1]) и нажать кнопку «Дальше» (см. Рисунок 71 [2]);

– откроется окно, где необходимо нажать кнопку «Отправить на Email» (Рисунок 77);

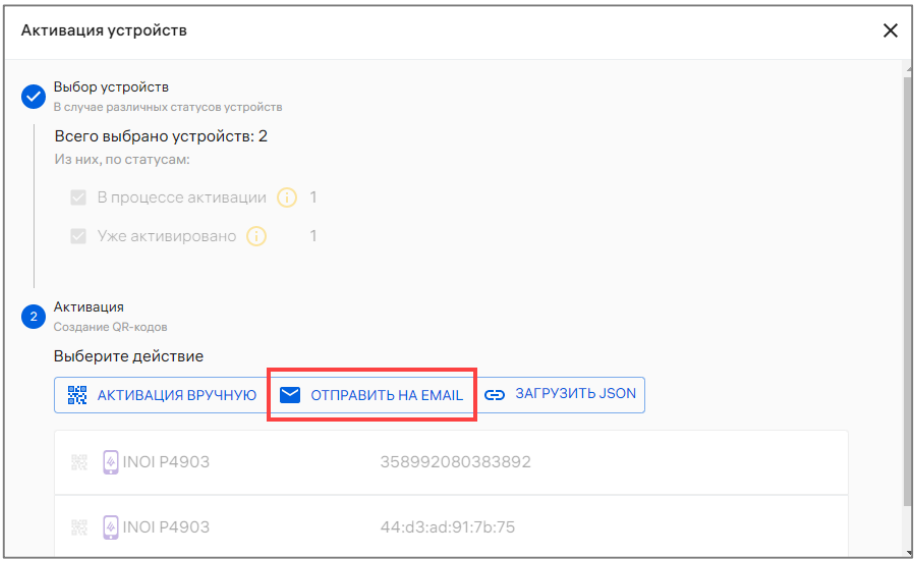

Рисунок 77

– в результате отобразится окно отправки QR-кода на Email, где необходимо ввести Email для писем с активацией (Рисунок 78 [1]);

– нажать кнопку «Отправить» (Рисунок 78 [2]).

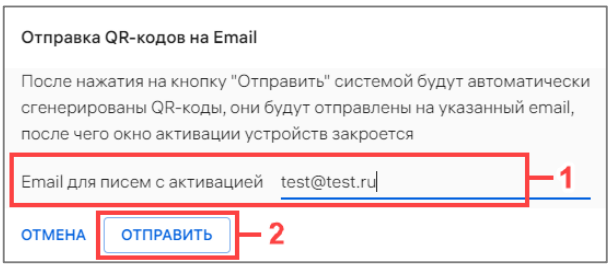

Рисунок 78

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 документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

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.

2.2.8.4. Активация группы устройств с помощью JSON-файла

Для активации устройств с помощью JSON-файла необходимо подготовить (пп. 2.2.8.4.1) и загрузить (пп. 2.2.8.4.2) 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».

Если первоначальная настройка устройств была выполнена, необходимо отсканировать QR-код, сгенерированный для группы устройств, в которую входят устройства. Подробное описание приведено в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.8.4.1. 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. 2.2.8.2, до этапа отображения окна активации устройств, где будет отображена следующая информация:

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

– пароль, присваиваемый созданной учетной записи устройства;

– дата истечения QR-кода;

– адрес процесса - адрес сервера для процесса активации устройства;

– контрольная сумма MD5;

– название компонента (актуально для устройств с ОС Android);

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр» (актуально для устройств с ОС Android).

ПРИМЕЧАНИЕ. Установка приложения «Аврора Центр» и активация устройства будут автоматически выполняться при первоначальной настройке устройства с ОС Android (подробнее в документе «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android») и при корпоративной привязке устройства с ОС Аврора (подробнее в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»») 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 79).

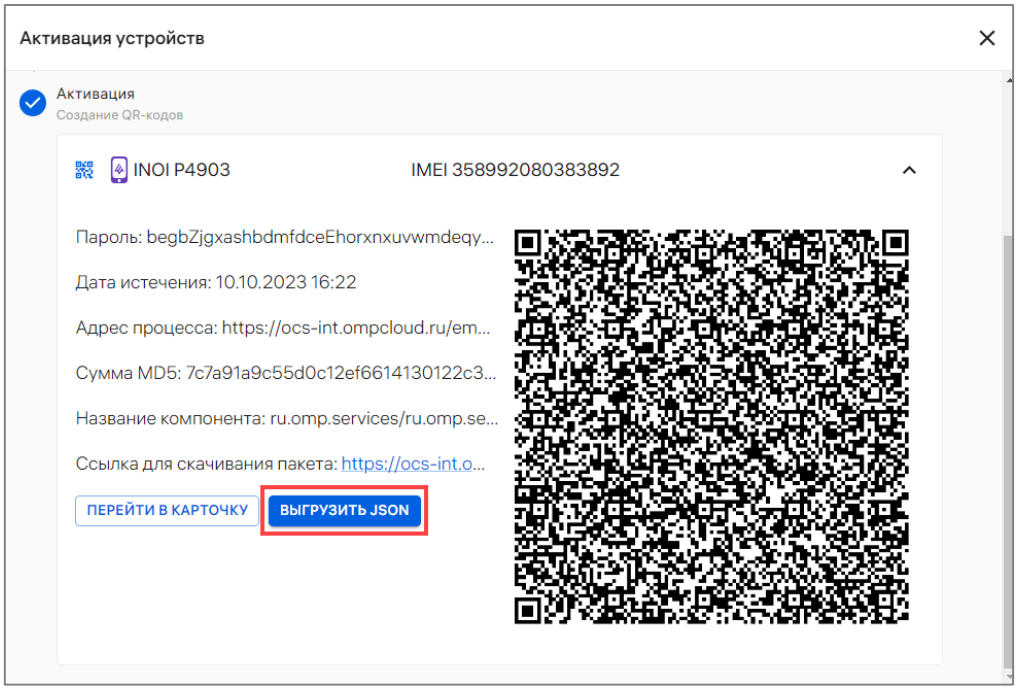

Рисунок 79

В результате на ЭВМ будет выгружен JSON-файл.

Пример содержания JSON-файла:

{"accountDomain":"","android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"accountDomain":"","clientID":"aurora-mobility-management","gatewayURI":"http://ocs-dev.ompcloud.ru/emm/mobile","password":"dtthtsgdoh5v"},"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"ru.omp.se ru.omp.services.AdminReceiver","android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATIO ocs-dev.ompcloud.ru/emm/mobile/clientDownload","android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"bZ41Av7s6nr","android. mobility-management","enrollmentID":"beefbeef","expiredAt":"2023-10-20T14:21:47+03:00","gatewayURI":"http://
ocs-dev.ompcloud.ru/emm/mobile","password":"dtthtsgdoh5v"}

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:

– **accountDomain**. Доменное имя аккаунтов учетных записей устройств, созданных в выбранном тенанте;

– **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;
  - 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.** Идентично параметру `accountDomain` выше;
- **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;

– **clientID**. Идентично параметру `clientID` выше;

– **enrollmentID**. Идентификатор созданной активации. Если QR-код создан через загрузку JSON-файла, данное поле принимает стандартное значение для всех выбранных устройств;

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

– **gatewayURI**. Идентично параметру `gatewayURI` выше;

– **password**. Идентично параметру `password` выше.

2.2.8.4.2. 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 80 [1]);

– в списке быстрых действий выбрать значок «Активация устройств» (Рисунок 80 [2]);

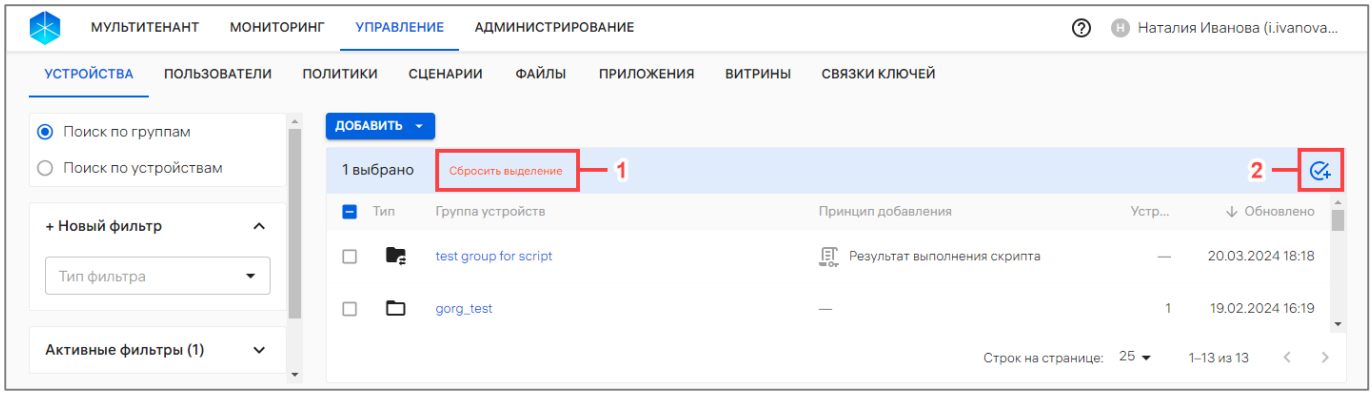

Рисунок 80

– перенести сгенерированный или подготовленный самостоятельно JSON-файл из файлового менеджера в поле загрузки (Рисунок 81);

Рисунок 81

– отобразится информация о загруженном JSON-файле, где необходимо нажать кнопку «Активация вручную» (Рисунок 82 [1]). Для удаления загруженного JSON-файла необходимо нажать кнопку «Удалить JSON» (Рисунок 82 [2]);

Рисунок 82

– 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 83), 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.

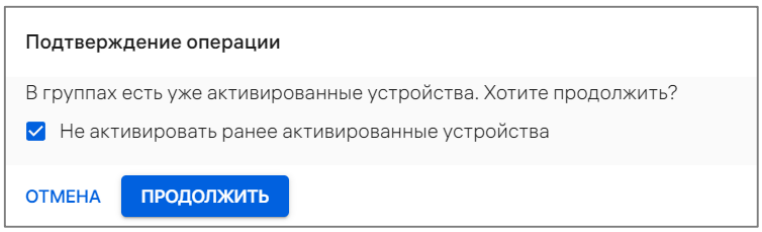

Рисунок 83

В результате JSON-файл будет загружен, и отобразится QR-код для активации группы устройств (Рисунок 84).

Рисунок 84

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»;

– 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 85). При нажатии на индикатор отобразится подробная информация об активации устройств: RequestID активации и количество готовых к активации устройств.

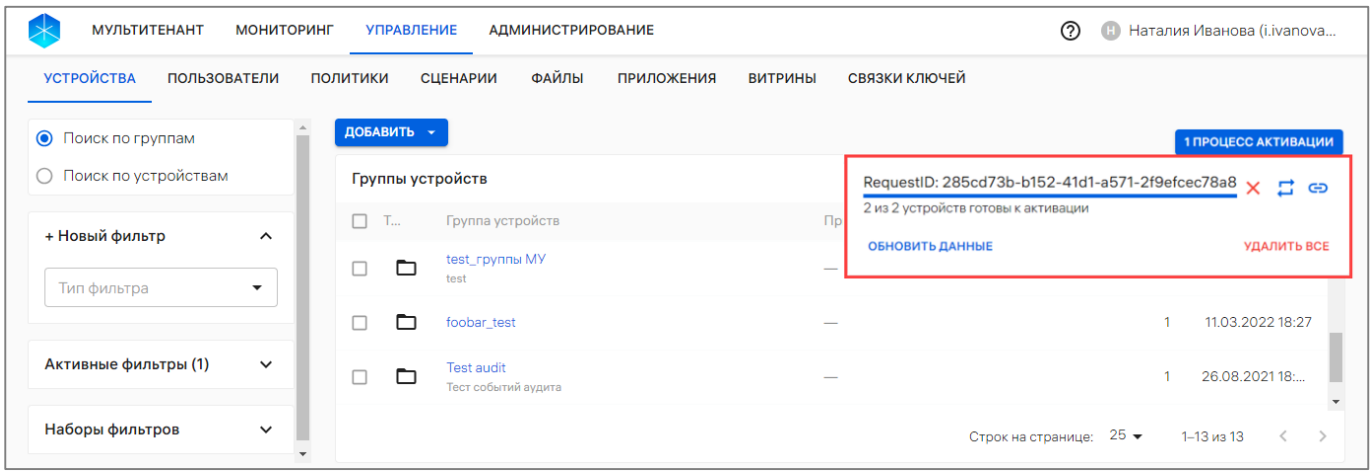

Рисунок 85

Для копирования ссылки процесса необходимо нажать значок «Скопировать ссылку процесса» (Рисунок 85). 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».

2.2.9. Применение оперативных команд

ВНИМАНИЕ! Применение оперативных команд доступно только для активированных устройств.

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 86 [1]), задать необходимые значения согласно таблице (Таблица 30) и далее подтвердить или отменить действия.

ПРИМЕЧАНИЕ. Действующие оперативные команды выделены цветным индикатором у соответствующего значка (Рисунок 86 [2]).

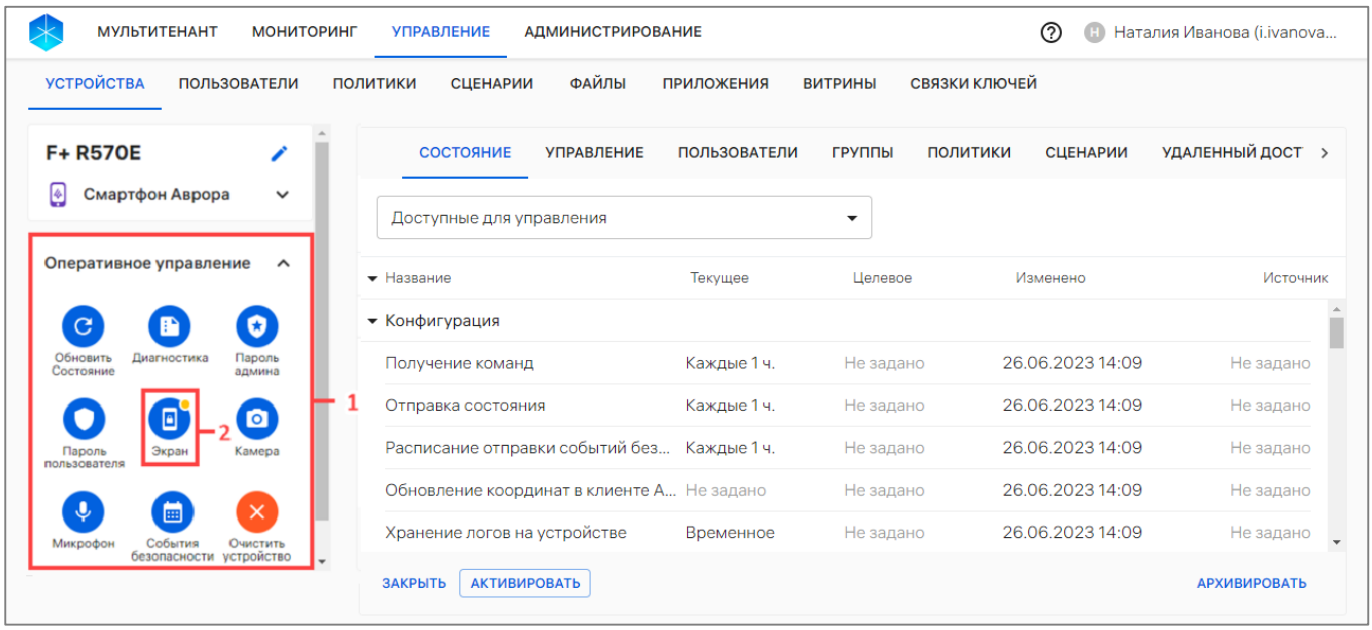

Рисунок 86

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 30

Оперативная команда	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Обновить состояние	Установка расписания обновления состояния устройства. Информация о состоянии устройства будет получена, если устройство находится в сети	+	+	+
Диагностика	Получение на электронную почту файла со списком системных сообщений об ошибках устройства (Рисунок 87). Название файла – `Reports.tar.bz2` **ПРИМЕЧАНИЕ.** По умолчанию отчет, содержащий список системных сообщений, отправляется на почтовый ящик, соответствующий текущей учетной записи администратора, которая может быть изменена. Если Email оператора не заполнен или не является действительным (например, в созданном тенанте), необходимо ввести его вручную. **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	+	-	-
Пароль админа	Установка одноразового пароля администратора для разблокировки устройства, если пользователь не знает или не может вспомнить пароль. Пароль должен содержать от 7 до 12 символов. 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. 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	+	-	-
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 и соответствовать требованиям парольной политики. 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	+	-	-
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. **ПРИМЕЧАНИЕ.** Для устройств на базе ОС семейства Linux функционал приведен в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux». 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]»	+	+	+

Оперативная команда	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
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]»	+	+	-
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]»	+	-	-
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	+	-	-
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	+	+	-

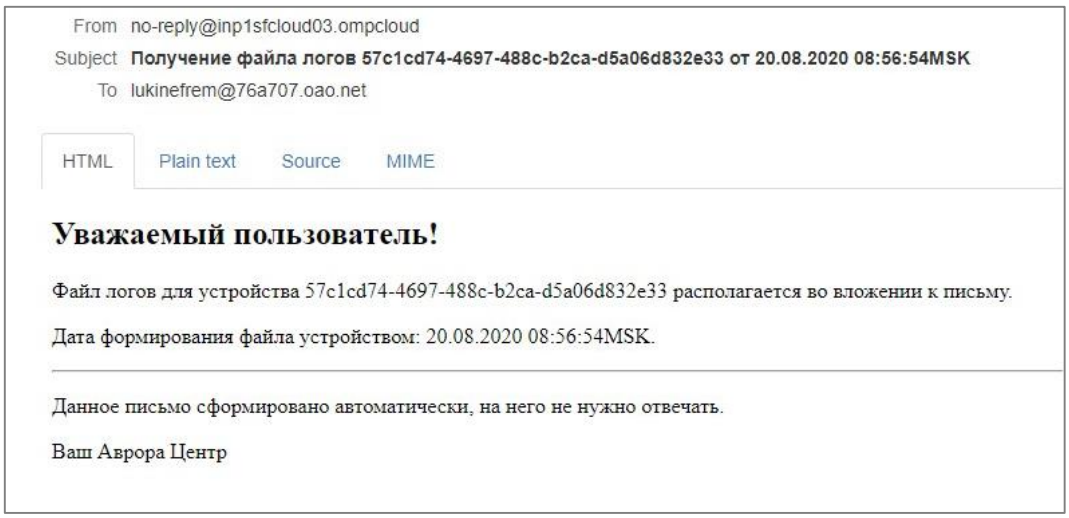

Рисунок 87

2.2.10. 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. 2.2.10.1);
– каточку группы устройств (пп. 2.2.10.2).

2.2.10.1.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 88 [1]);
– в списке быстрых действий нажать значок 🗑 «Исключить устройство из группы» (Рисунок 88 [2]);

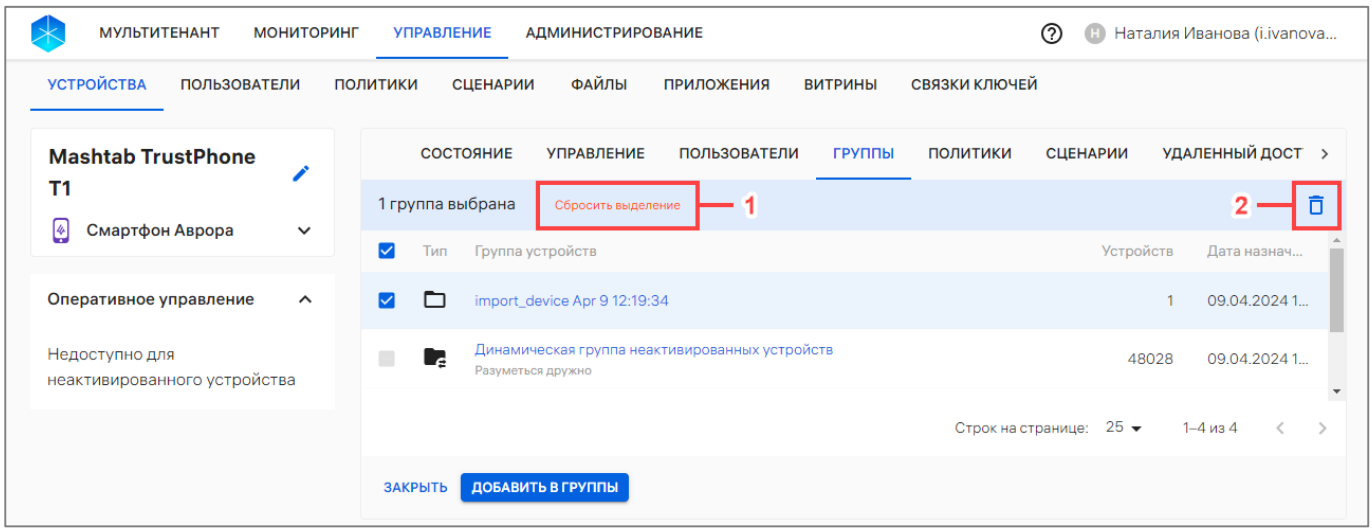

Рисунок 88

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 89).

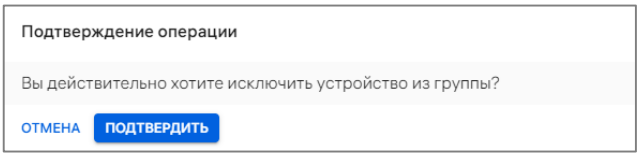

Рисунок 89

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.

2.2.10.2.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 90 [1]);

– в списке быстрых действий нажать значок «Отвязать устройства от группы» (Рисунок 90 [2]);

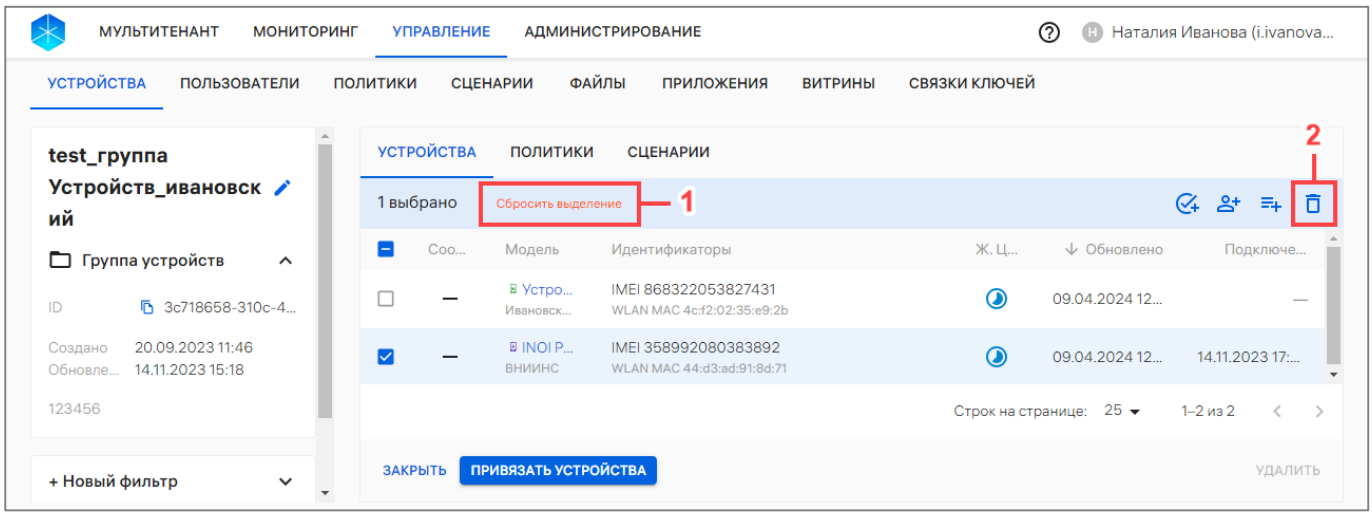

Рисунок 90

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 91).

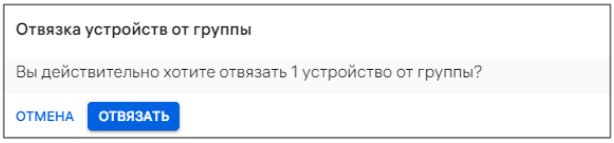

Рисунок 91

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.

2.2.11. 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. 2.2.12.

Перед архивированием активированного устройства необходимо очистить его с помощью оперативных команд (п. 2.2.9).

Архивирование устройства может быть выполнено:

– в подразделе «Устройства» с помощью списка быстрых действий (пп. 2.2.11.1);

– с помощью карточки устройства (пп. 2.2.11.2).

2.2.11.1.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 92 [1]);

– в списке быстрых действий выбрать значок «Архивировать» (Рисунок 92 [2]);

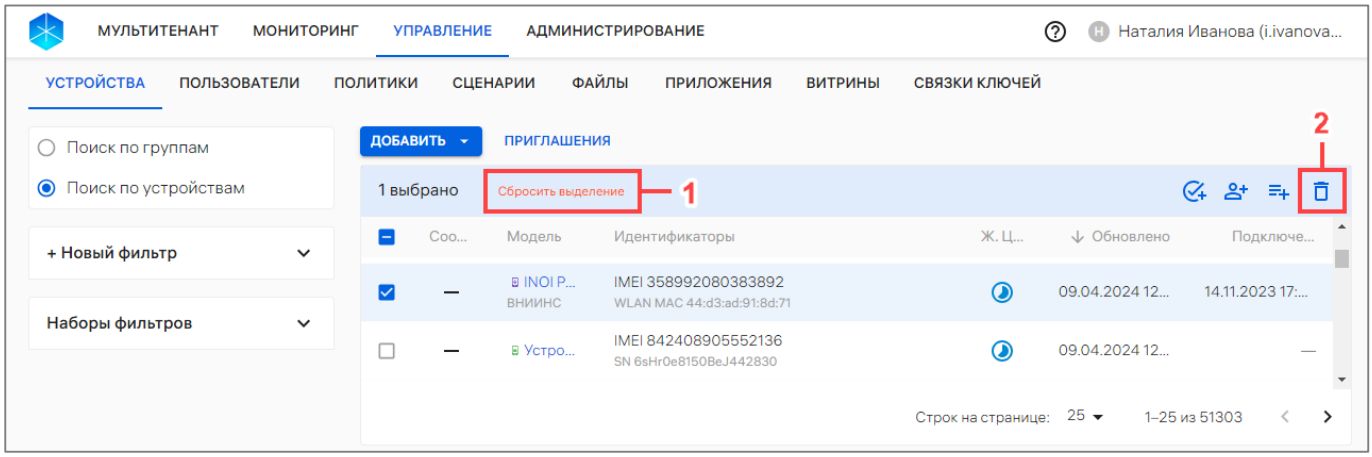

Рисунок 92

– если выбранные устройства были очищены, то отобразится окно подтверждения операции, где необходимо нажать кнопку «Архивировать» (Рисунок 93).

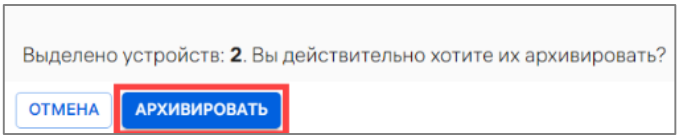

Рисунок 93

Если одно или несколько устройств не очищены, отображается сообщение (Рисунок 94), в котором необходимо выбрать соответствующую кнопку:

– для архивирования только очищенных устройств нажать кнопку «Архивировать только очищенные» (Рисунок 94);

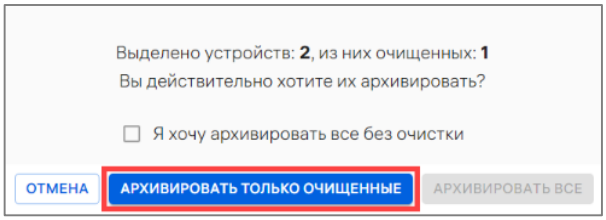

Рисунок 94

– для архивирования без очистки необходимо:

- подтвердить архивирование без очистки, установив галочки в чекбоксе (Рисунок 95 [1]);
- нажать кнопку «Архивировать все» (Рисунок 95 [2]).

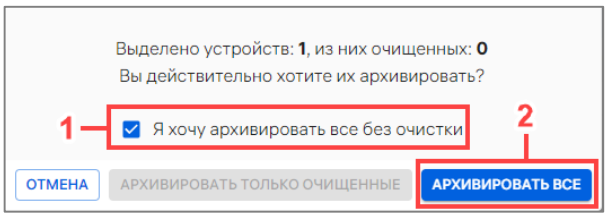

Рисунок 95

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).

2.2.11.2.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 96);

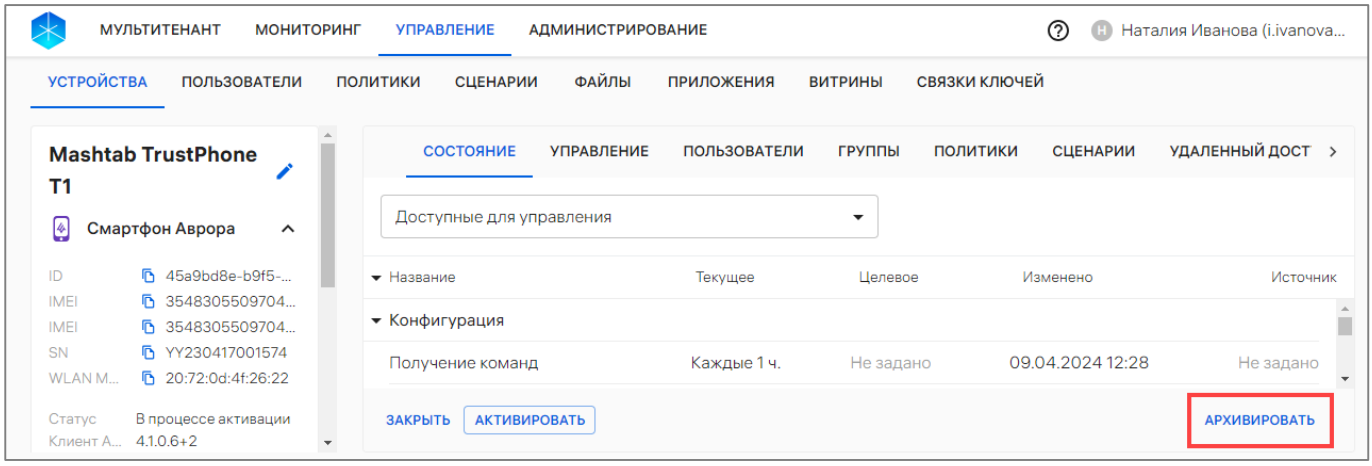

Рисунок 96

– если устройство не очищено, отобразится соответствующее сообщение. Для подтверждения архивирования необходимо нажать кнопку «Архивировать» (Рисунок 97).

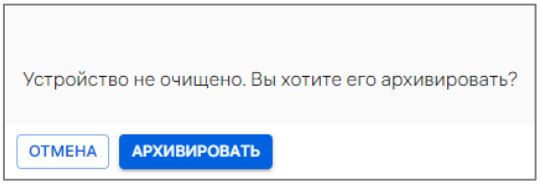

Рисунок 97

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. 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 98 [1]);

– выбрать значок «Активация устройств» (Рисунок 98 [2]);

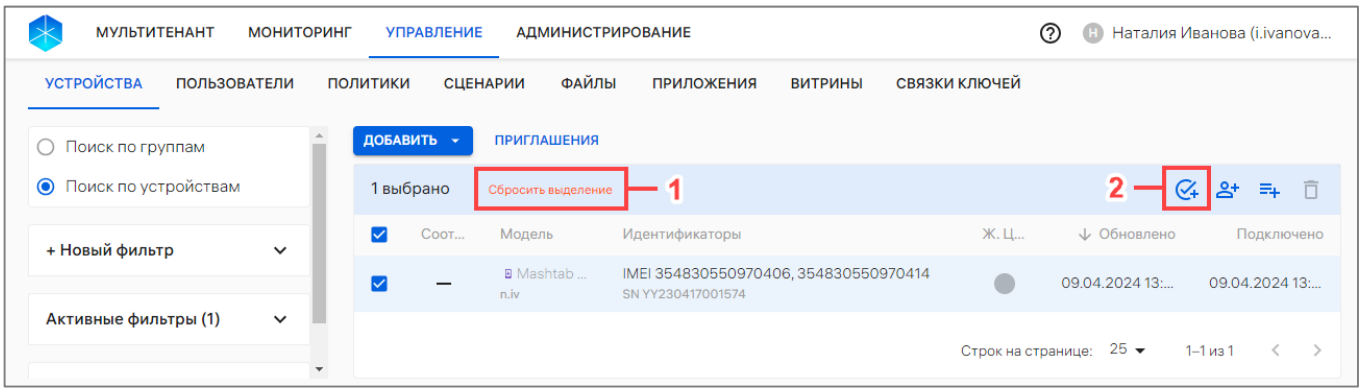

Рисунок 98

– в отобразившемся окне активации устройств установить галочку в чекбоксе «Перенесено в архив» (Рисунок 99 [1]) и нажать кнопку «Дальше»(Рисунок 99 [2]).

Рисунок 99

При наличии у устройств связей со статистическими группами и/или пользователями на шаге «Восстановление связей» необходимо подтвердить восстановление связей, установив галочку в чекбоксе (Рисунок 100 [1]), и нажать кнопку «Дальше» (Рисунок 100 [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.

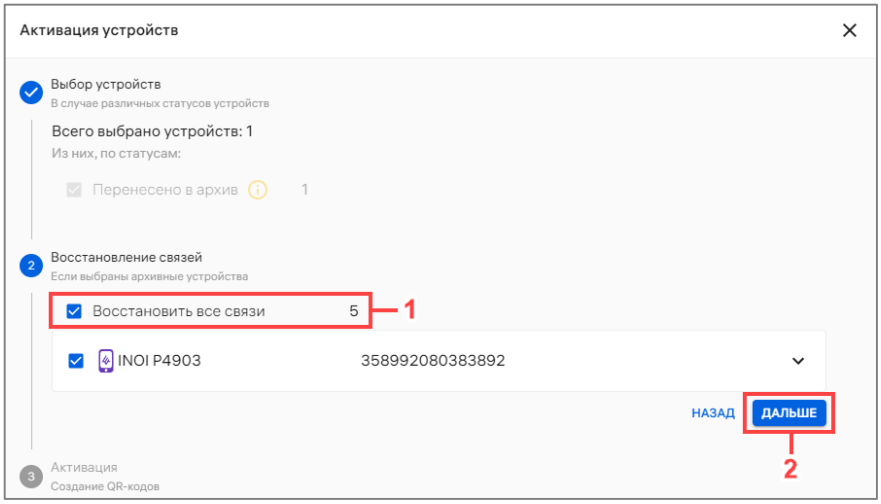

Рисунок 100

Далее активировать устройства возможно одним из способов:

– нажать кнопку «Отправить на Email» (Рисунок 101 [1]), в открывшемся окне ввести адрес электронной почты и далее нажать кнопку «Отправить»;

– нажать кнопку «Активация вручную» (Рисунок 101 [2]) и далее нажать кнопку «Продолжить».

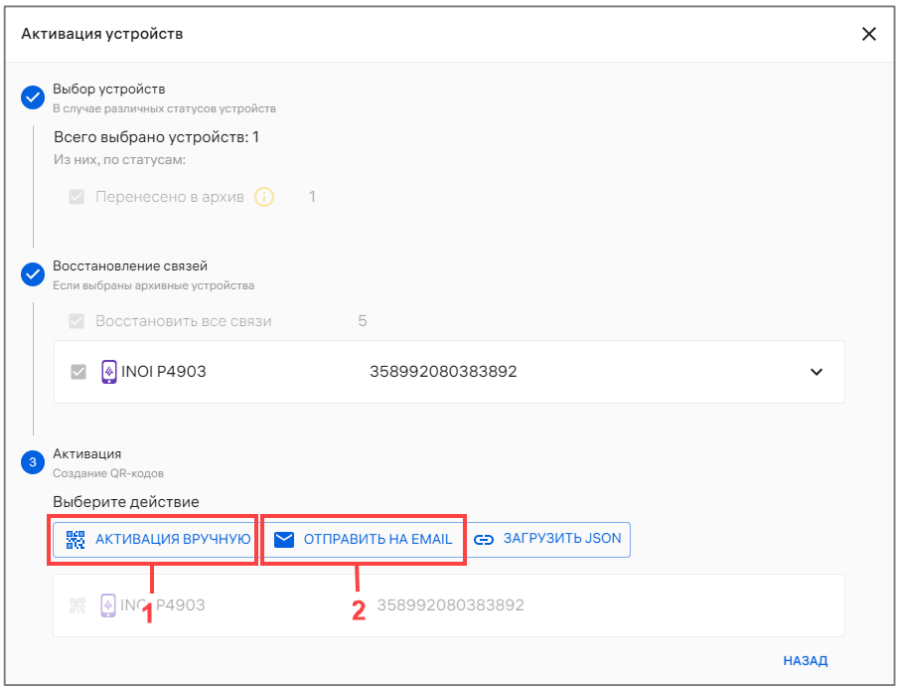

Рисунок 101

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 документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.13. Удаление группы устройств

ПРИМЕЧАНИЕ. Перед удалением группы устройств необходимо предварительно исключить все устройства из группы в соответствии с п. 2.2.10.

ВНИМАНИЕ! Из ПУ возможно удалить только статическую группу устройств (группу с типом «Группа устройств»).

После исключения всех устройств из группы данная группа устройств 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 устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.5);

– в открывшейся карточке перейти во вкладку «Устройства» и удалить все устройства из группы (пп. 2.2.10.2);

– в карточке группы устройств нажать кнопку «Удалить» (Рисунок 102);

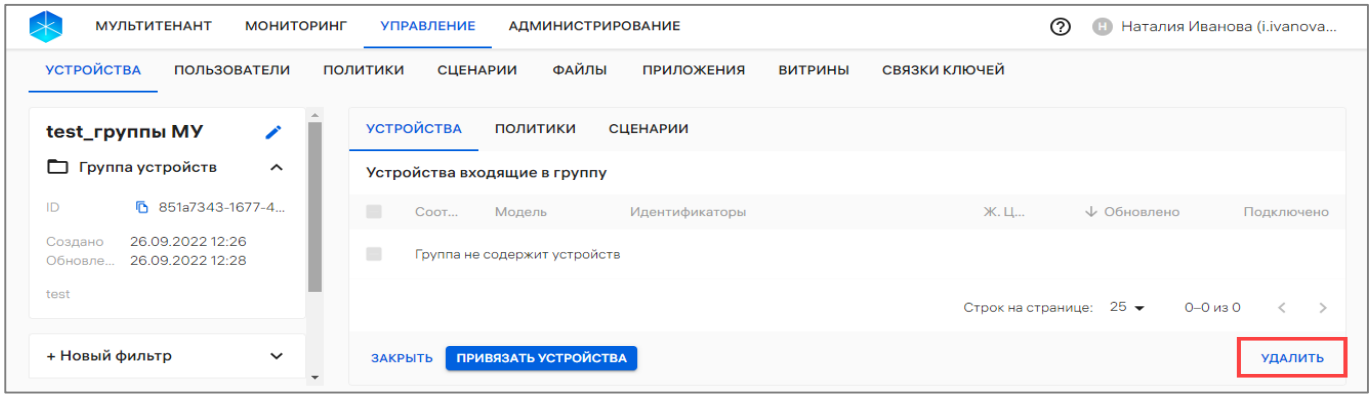

Рисунок 102

– в отобразившемся окне (Рисунок 103) подтвердить либо отменить действия.

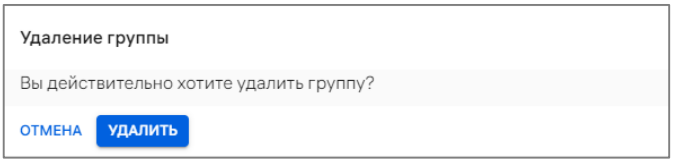

Рисунок 103

В результате успешного удаления отобразится соответствующее сообщение.

2.2.14. 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 30) в соответствии с п. 2.2.9, в результате чего отобразится окно подтверждения операции, где необходимо нажать кнопку «Очистить» (Рисунок 104).

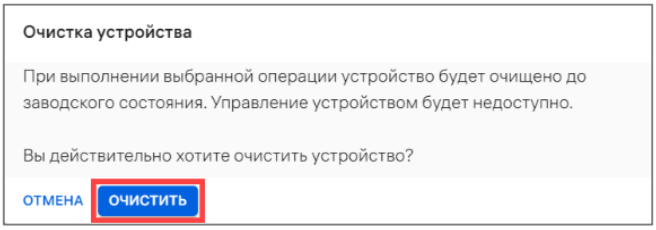

Рисунок 104

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

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. 2.2.8).

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

2.2.15. 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 105);

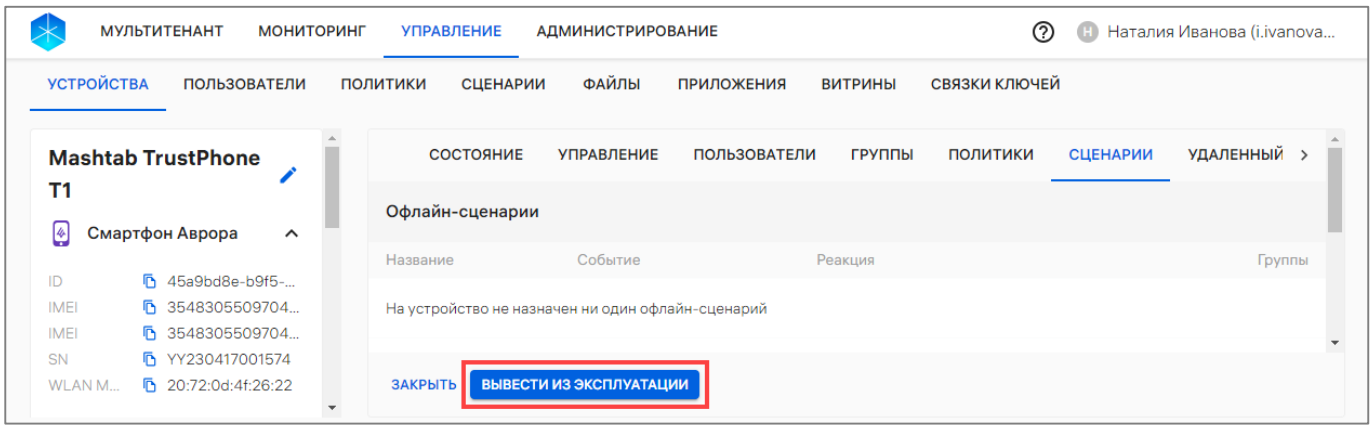

Рисунок 105

– в отобразившемся окне подтверждения операции (Рисунок 106) подтвердить либо отменить действия.

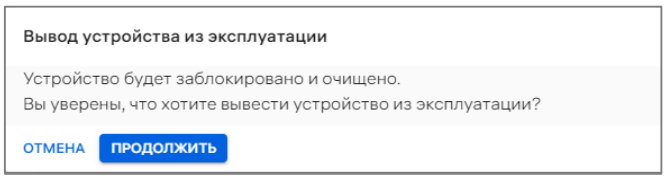

Рисунок 106

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

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

– очистка устройства (сброс к заводским настройкам);

– архивирование устройства (удаление из списка устройств).

ПРИМЕЧАНИЕ. Сценарий запустится при следующем подключении устройства к серверу ПУ.

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 107 [2]).

ПРИМЕЧАНИЕ. Для отображения группы пользователей необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 107 [1]).

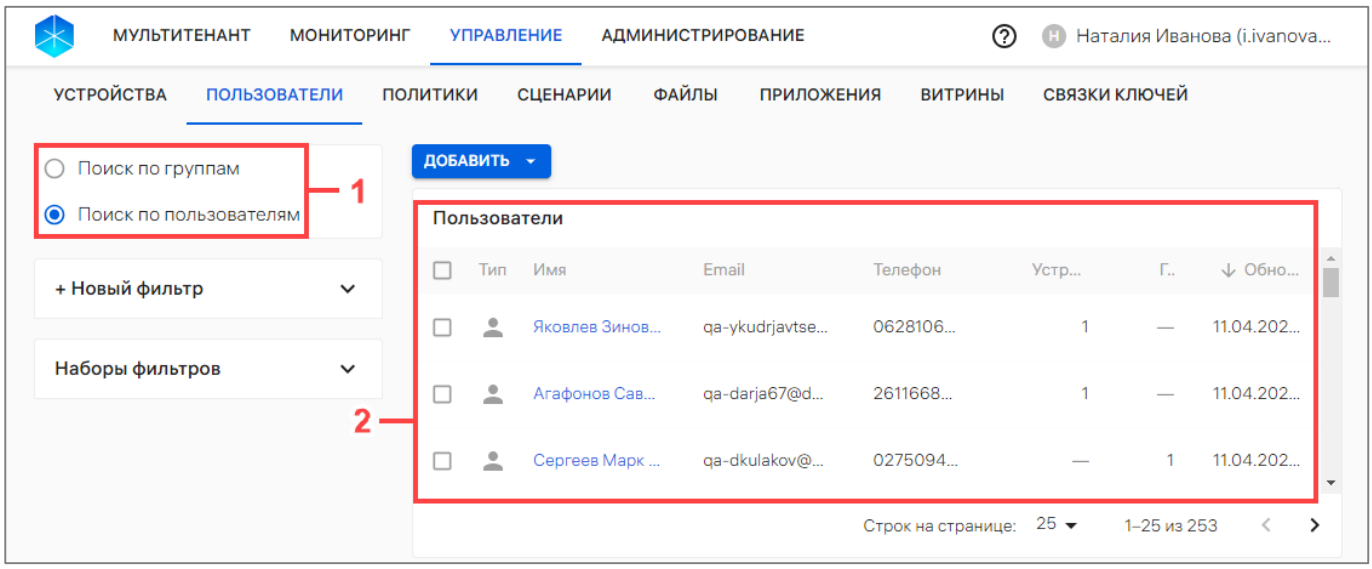

Рисунок 107

В рабочей области информация о пользователях и группах пользователей отображается в столбцах, приведенных в таблице (Таблица 31), 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 31

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
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)
Пользователей	Количество пользователей, привязанных к группе

Параметр	Описание
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).

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 108);

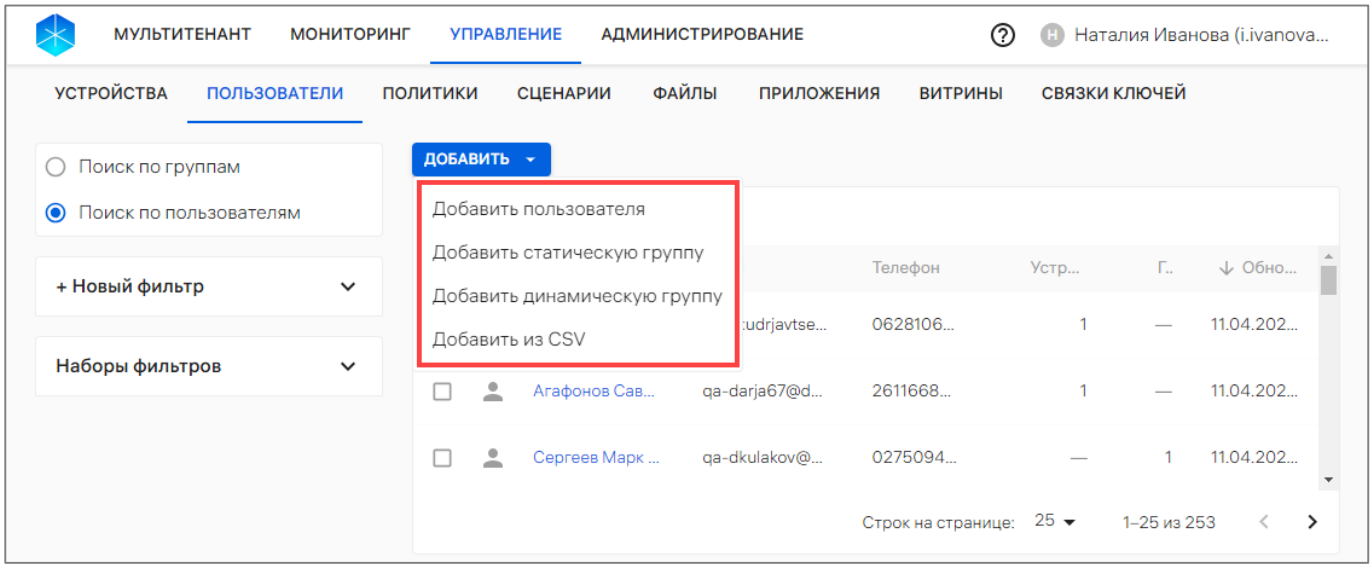

Рисунок 108

– в открывшемся окне (Рисунок 109) ввести данные о пользователе (Таблица 32);

Таблица 32

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

Поле ввода	Значение	Примечание
Почта рабочая	Рабочий email пользователя	Поле обязательно для заполнения и является идентификатором пользователя Аврора Центр
Должность	Должность пользователя 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 109).

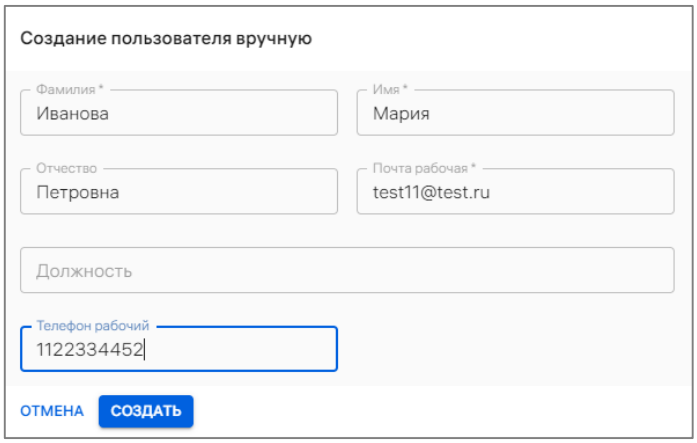

Рисунок 109

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 в ручную доступно:
– добавление статической группы пользователей (пп. 2.3.2.1);
– добавление динамической группы пользователей (пп. 2.3.2.2).

2.3.2.1. Добавлене 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 108);
– в открывшемся окне (Рисунок 110) заполнить поля (Таблица 33).

Таблица 33

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 110).

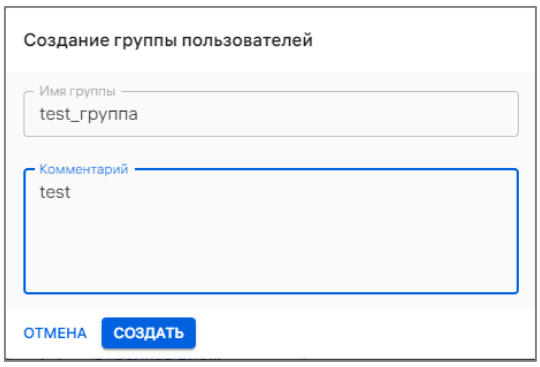

Рисунок 110

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 — это 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:

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

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить динамическую группу» (см. Рисунок 108);

– в открывшемся окне (Рисунок 111) заполнить поля, приведенные в таблице (см. Таблица 33);

– в блоке «Принцип добавления в группу» в раскрывающемся списке задать значение дополнительного атрибута, по которому пользователи будут добавлены в динамическую группу;

– 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.

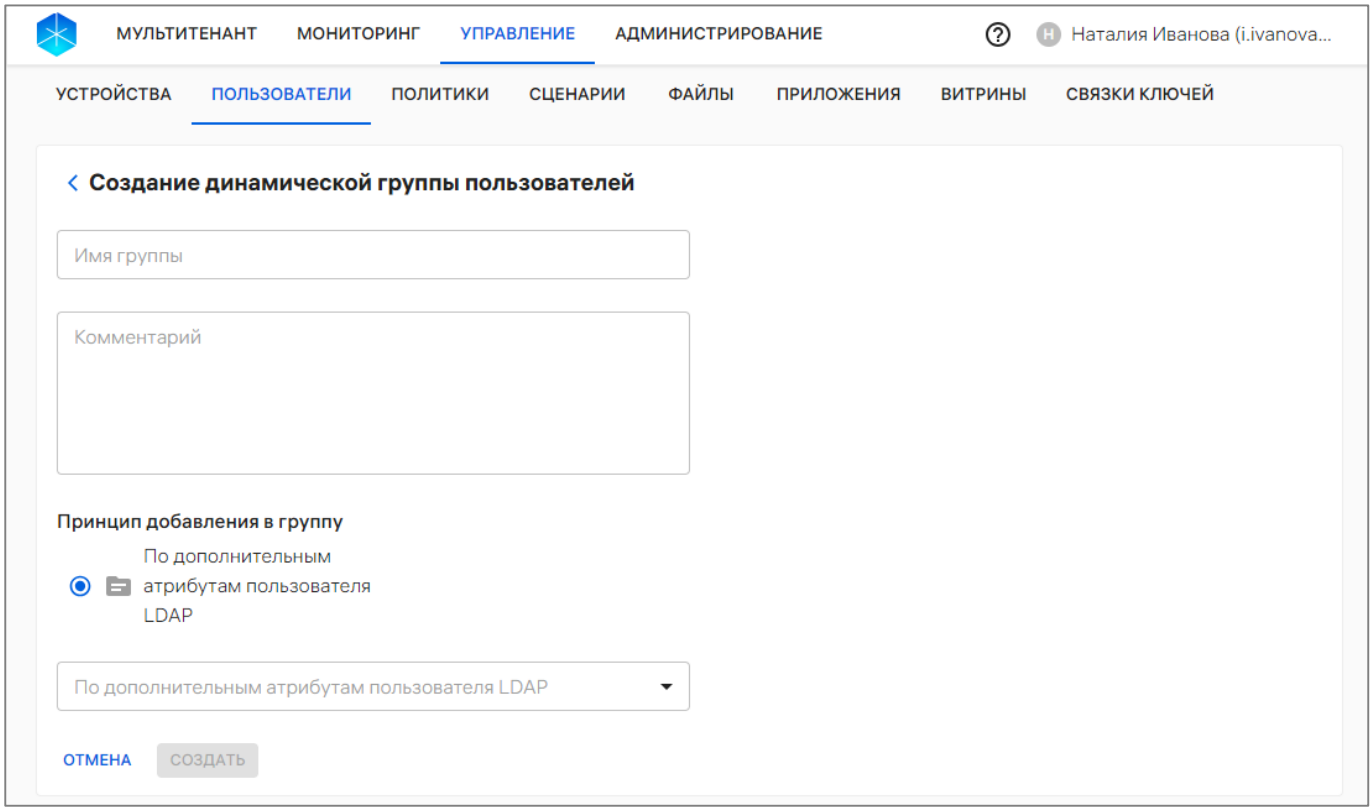

Рисунок 111

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 108);

– в открывшемся окне нажать «Шаблон .CSV ⬇» (Рисунок 112), в результате чего шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 34).

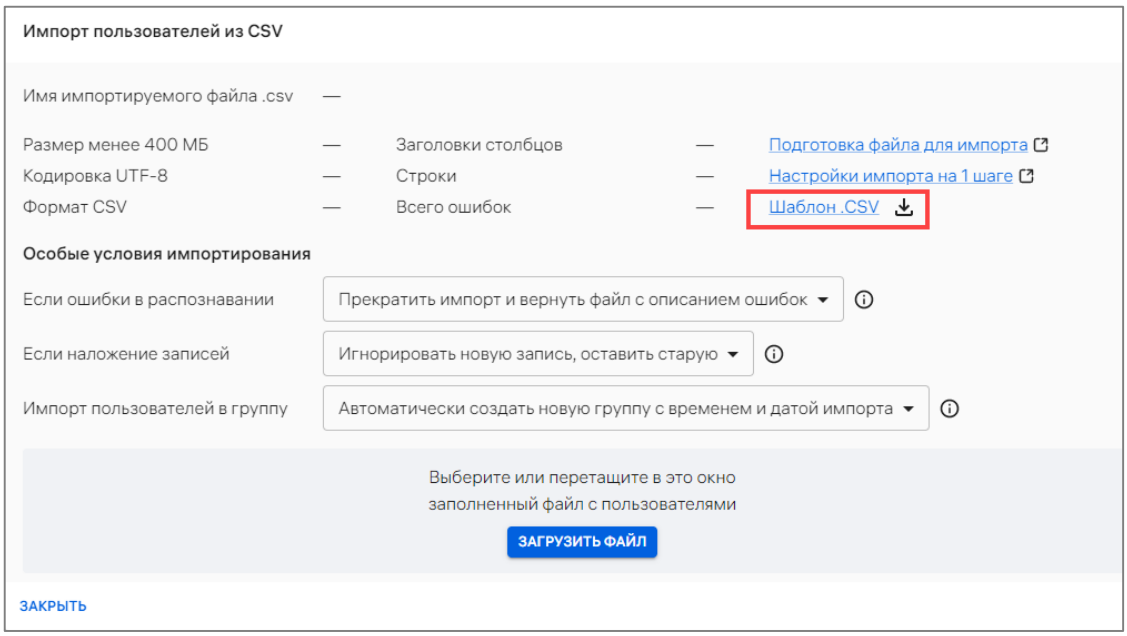

Рисунок 112

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 113).

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 113

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 насколько частей и загружать их поочередно;

– формат файла — `.csv`;

– кодировка файла — UTF-8;

– 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 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 (0xFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «a».

Описание требований к значениям параметров приведено в таблице (Таблица 34).

Таблица 34

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; – привязке пользователя к группе
FIRST_NAME	Имя пользователя. Содержит следующие буквы и символы: а-я, А-Я, a-z, A- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	

Параметр	Описание	Примечание
LAST_NAME	Фамилия пользователя. Содержит следующие буквы и символы: а-я, А-Я, a-z, A- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	
PATRONYMIC	Отчество пользователя. Содержит следующие буквы и символы: а-я, А-Я, a-z, A- 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, a-z, A- 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	Правило разрешения конфликтующих записей. Доступные значения: – `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	Параметр не обязателен для заполнения. Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта

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 108);

– в открывшемся окне задать особые условия импортирования, приведенные в таблице (Таблица 35).

Таблица 35

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 114 [1]): – **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: • файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ (Рисунок 114 [1],[2]). В результате отобразится текст подсказки следующего содержания: при завершении импорта система предоставит 2 файла: список системных сообщений ошибок распознавания и Журнал успешно импортированных устройств
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 114 [2]): – **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; – **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.	

Наименование полей	Описание	Примечание
	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	
Импорт пользователей в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 114 [3]): – **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	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ (Рисунок 114 [3]). В результате отобразится текст подсказки следующего содержания: в процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую

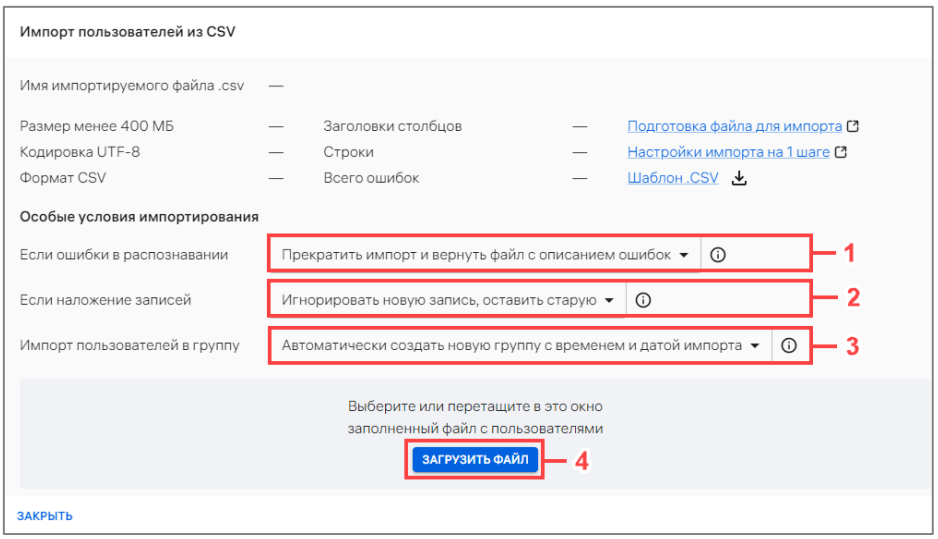

Рисунок 114

– далее необходимо загрузить CSV-файл одним из способов:

- переместить CSV-файл в область загрузки;
- нажать кнопку «Загрузить файл» (см. Рисунок 114 [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 115).

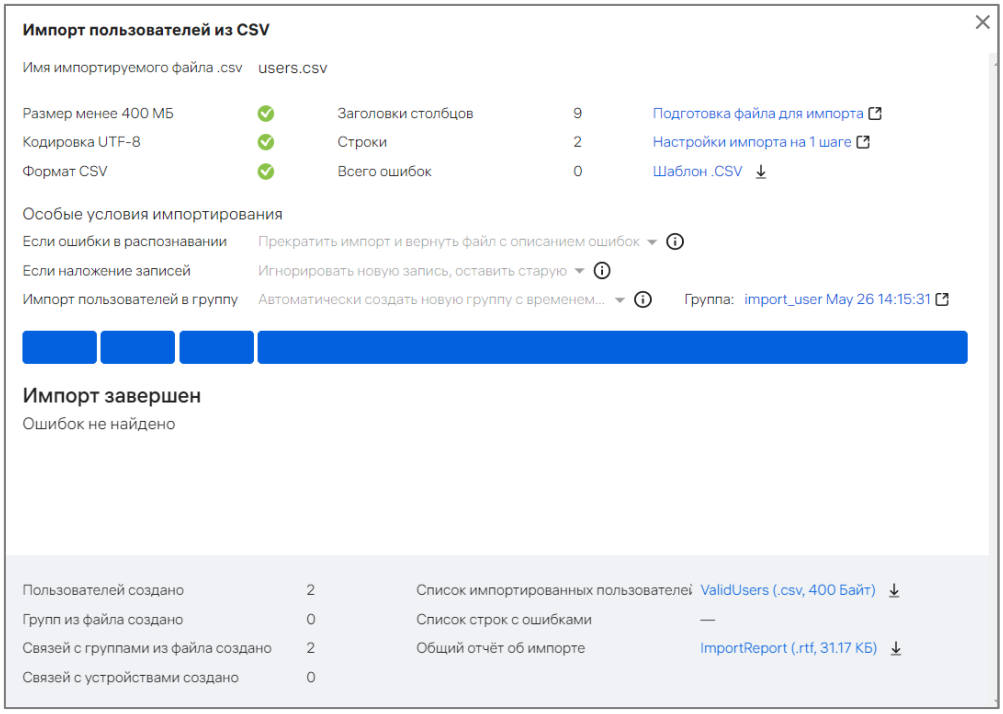

Рисунок 115

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 116 [6]).

Рисунок 116

В окне с результатами импорта пользователей отображается следующая информация:

– название импортируемого файла (см. Рисунок 116 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 116 [2]);

– количество столбцов, всех импортируемых строк и ошибок в файле (при их наличии) (см. Рисунок 116 [3]);

– ссылки (см. Рисунок 116 [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 116 [5]), см. Таблица 35);

– шкала прогресса импорта (см. Рисунок 116 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (Рисунок 116 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (Рисунок 116 [8]);

– количество созданных пользователей, групп пользователей, связей пользователей с группами и устройствами (Рисунок 116 [9]);

– ссылки на скачивание отчетов (Рисунок 116 [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 подразделе 3.1.

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).

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

Привязка пользователей к группам с помощью списка быстрых действий возможно 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»/группу пользователей, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 117 [1], Рисунок 118 [1]);

– в списке быстрых действий выбрать значок (Рисунок 117 [2]) или (Рисунок 118 [2]) «Привязать пользователей к группам»;

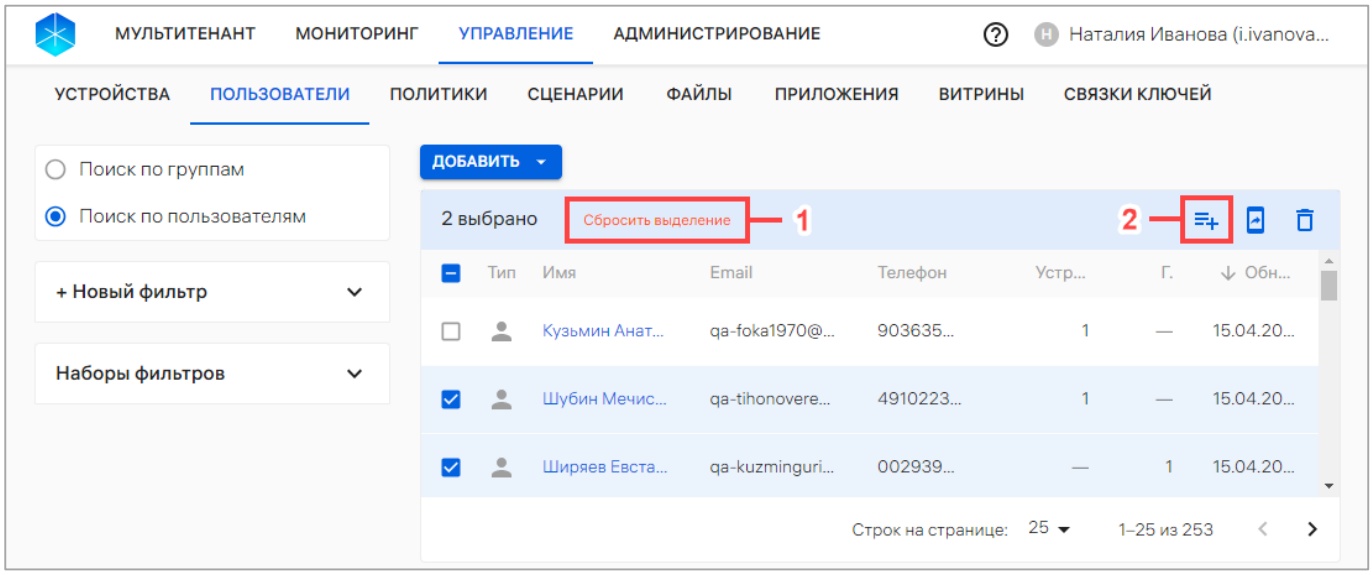

Рисунок 117

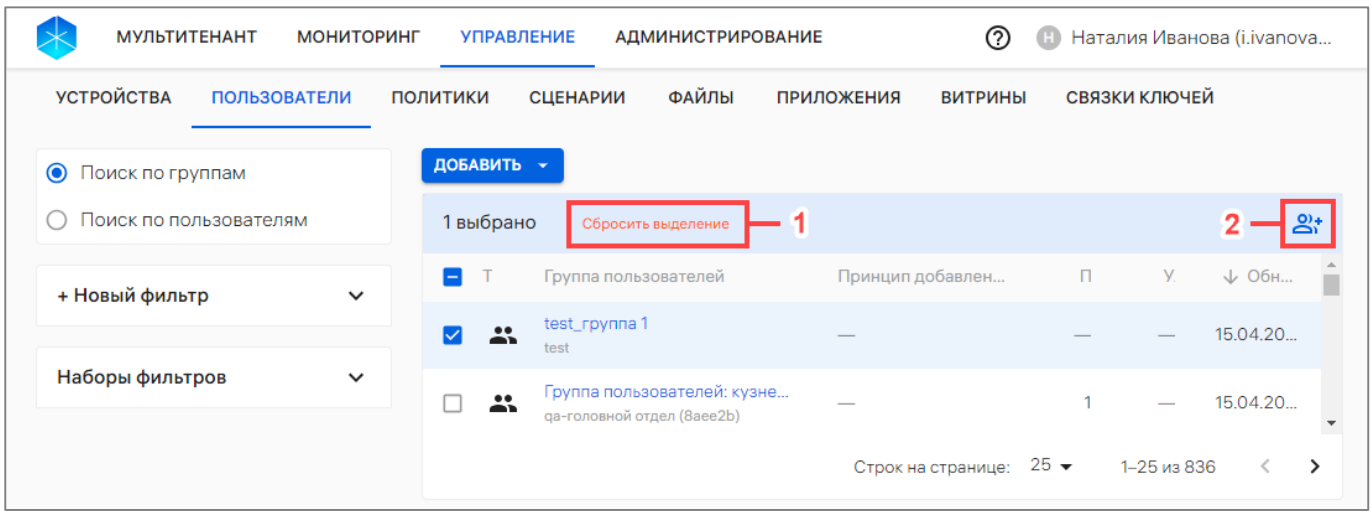

Рисунок 118

– в отобразившемся окне выбрать необходимую группу пользователей (Рисунок 119[1]) или пользователя (Рисунок 120 [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 119 [3], Рисунок 120 [3]).

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

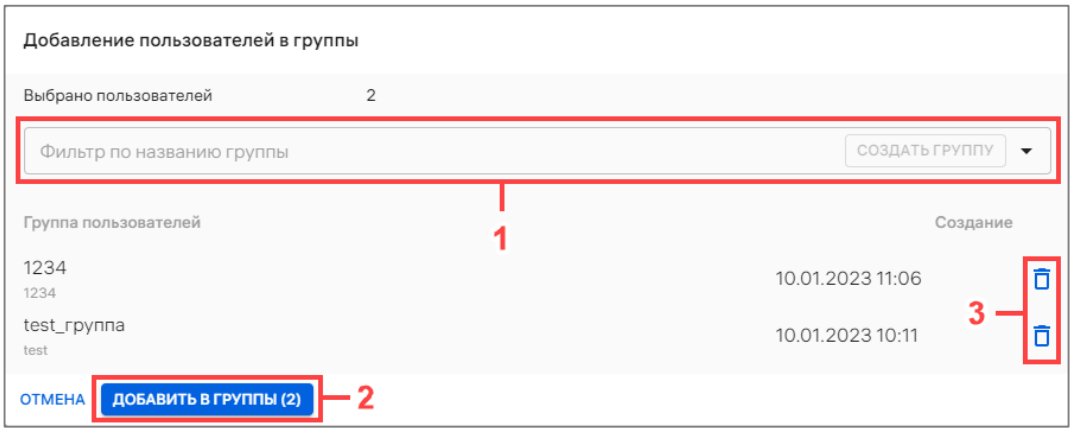

Рисунок 119

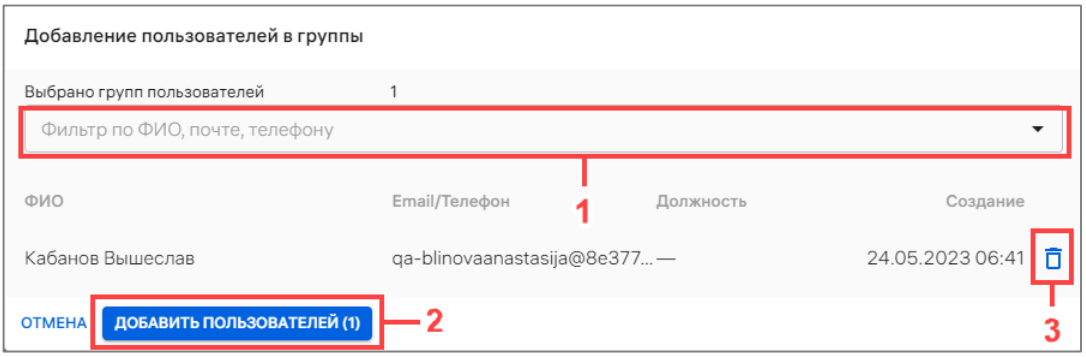

Рисунок 120

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 121 [1]) и нажав кнопку «Создать группу» (Рисунок 121 [2]). В результате успешного создания группы отобразится соответствующее сообщение;

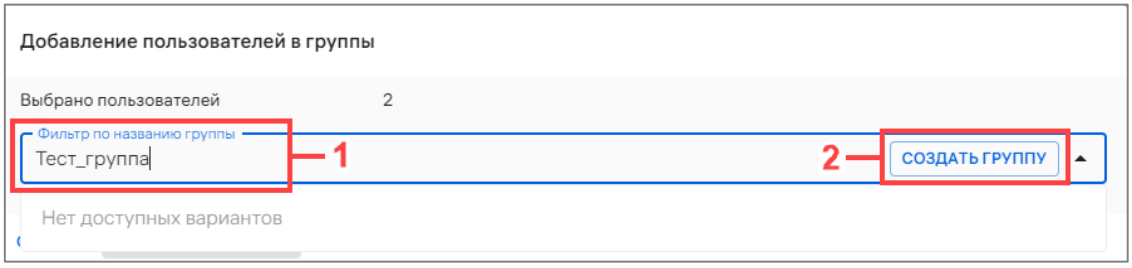

Рисунок 121

– нажать кнопку «Добавить в группы» (см. Рисунок 119 [2]) или «Добавить пользователей» (см. Рисунок 120 [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 122);

– в отобразившемся окне (см. Рисунок 119) выполнить действия, описанные в пп. 2.3.4.1.

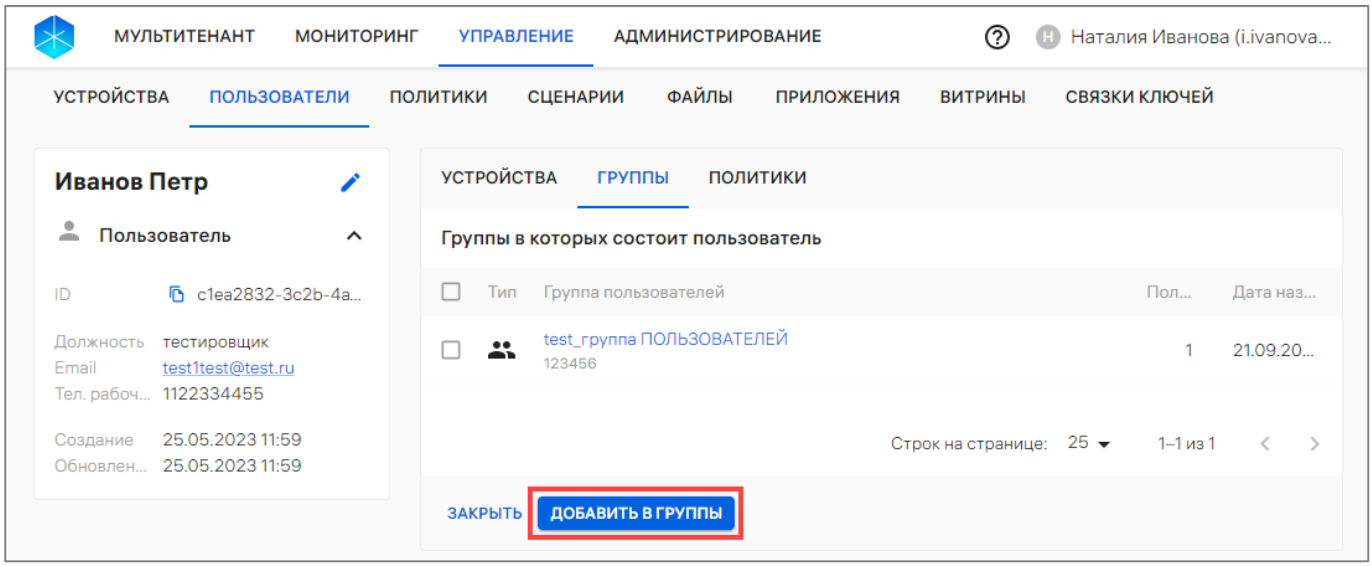

Рисунок 122

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 123 [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 123 [3]).

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

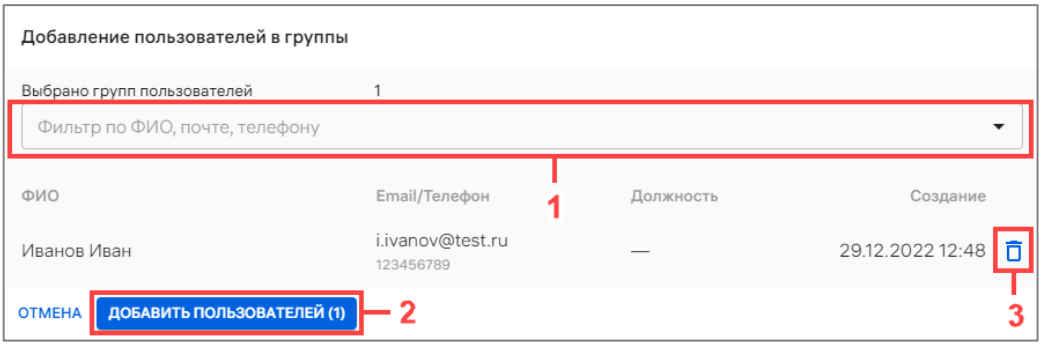

Рисунок 123

– далее нажать кнопку «Добавить пользователей» (Рисунок 123 [2]). В результате успешной привязке 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 124 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям» (Рисунок 124 [2]);

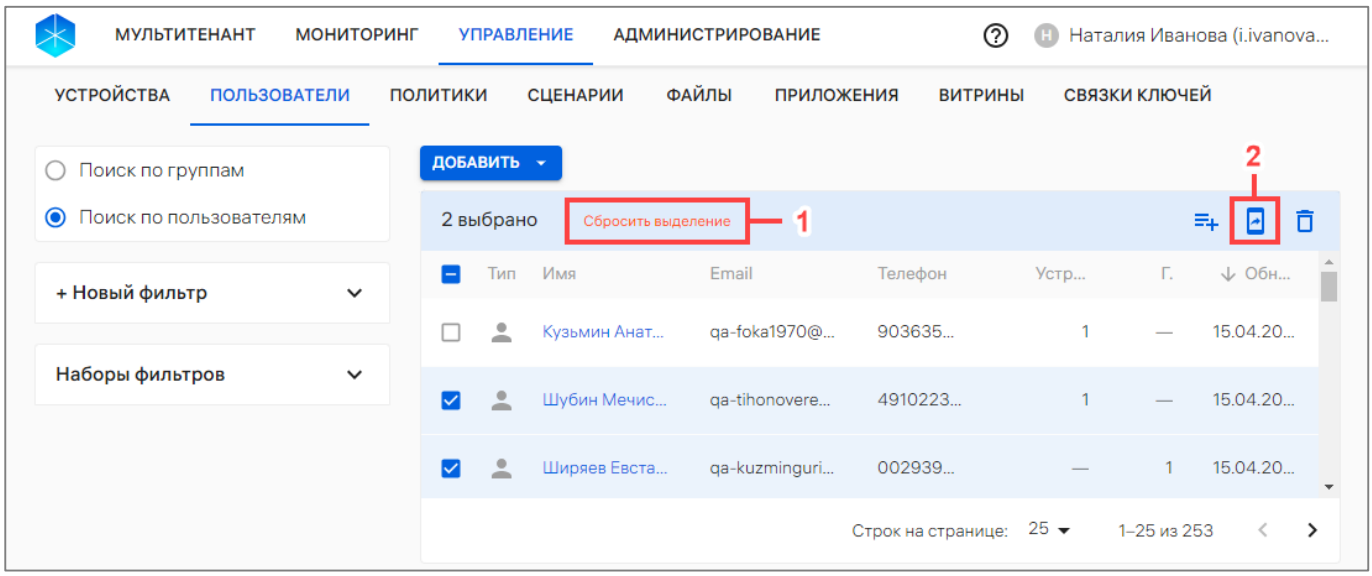

Рисунок 124

– в отобразившемся окне выбрать устройства из раскрывающегося списка или воспользоваться фильтром по идентификатору или комментарию (Рисунок 125 [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 125 [3]);

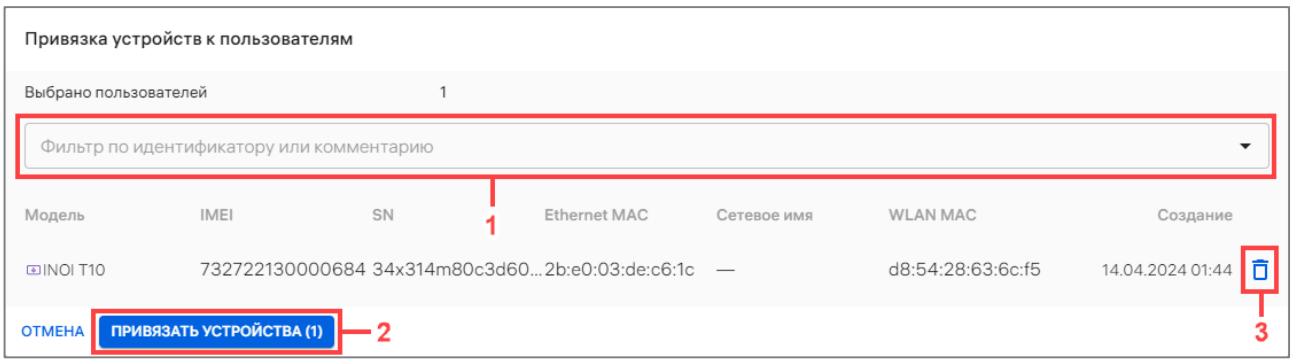

Рисунок 125

– нажать кнопку «Привязать устройства» (Рисунок 125 [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 125) выполнить действия, описанные в пп. 2.3.5.1.

2.3.6. 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 126);

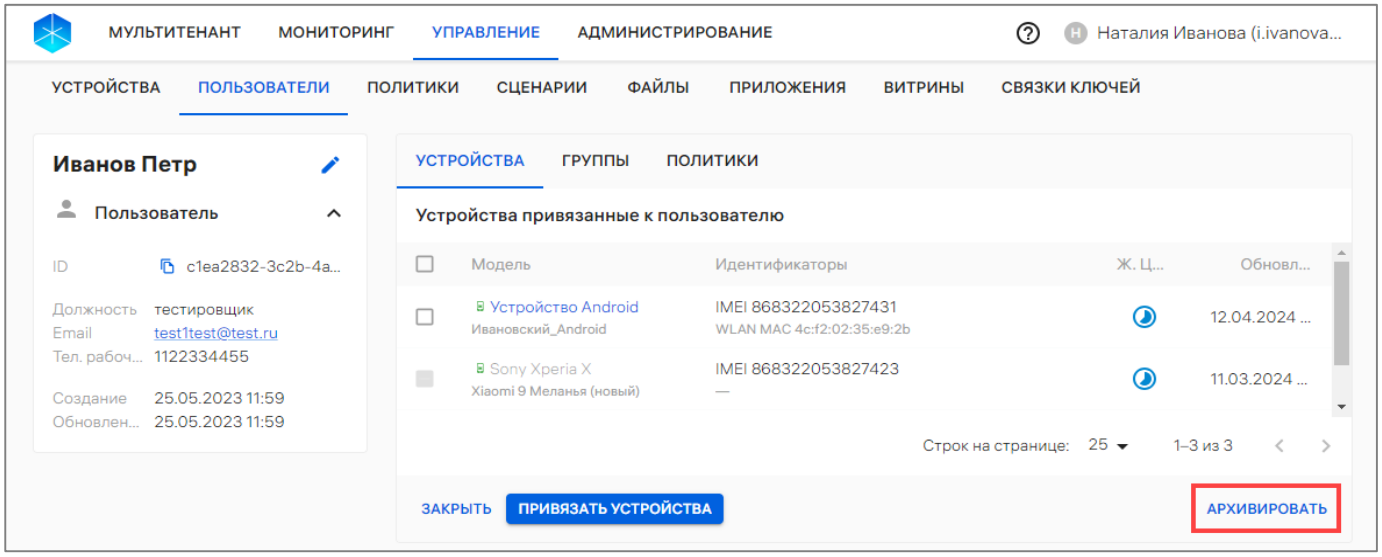

Рисунок 126

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 127);

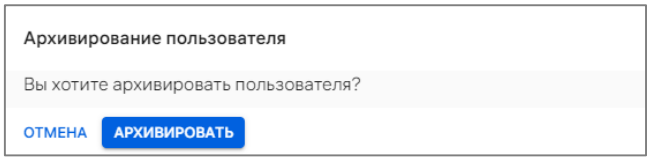

Рисунок 127

2) С помощь 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 128 [1]);

– в списке быстрых действий выбрать значок (Рисунок 128 [2]);

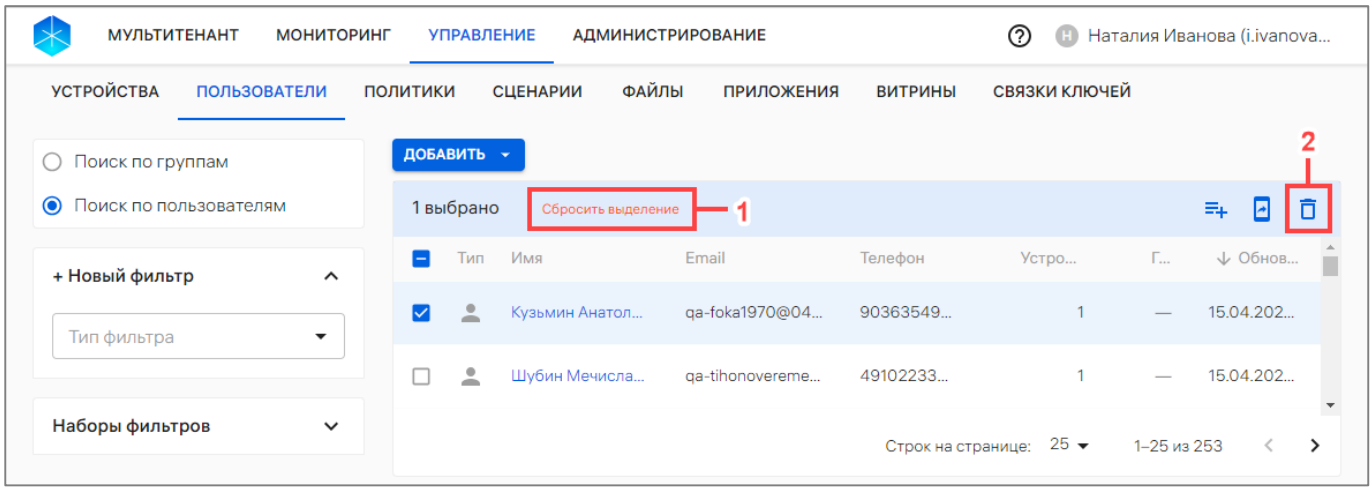

Рисунок 128

– в отобразившемся окне подтвердить либо отменить действия (см. Рисунок 127).

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

2.3.7. Удаление группы пользователей

ВНИМАНИЕ! Удаление группы пользователей невозможно, если группа пользователей имеет тип «Организационное подразделение» (группа пользователей, синхронизированная с LDAP-сервером).

Для удаления группы пользователей необходимо предварительно исключить всех пользователей из группы и 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 удалить всех пользователей из группы и нажать кнопку «Удалить» (Рисунок 129);

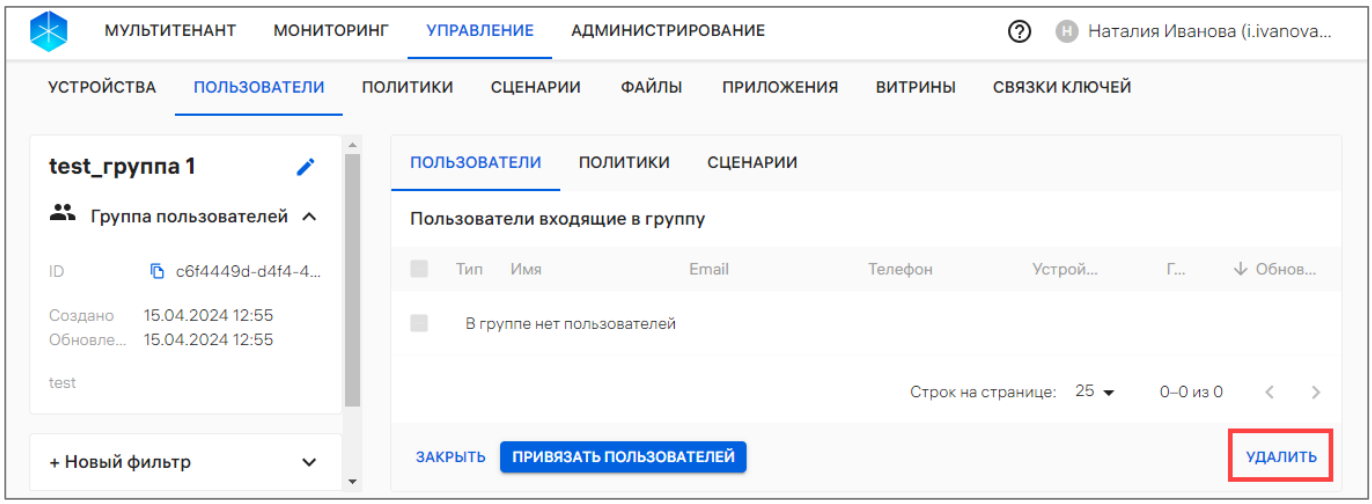

Рисунок 129

– в открывшемся окне (Рисунок 130) подтвердить либо отменить действия.

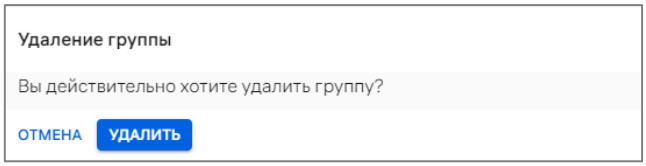

Рисунок 130

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.

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».

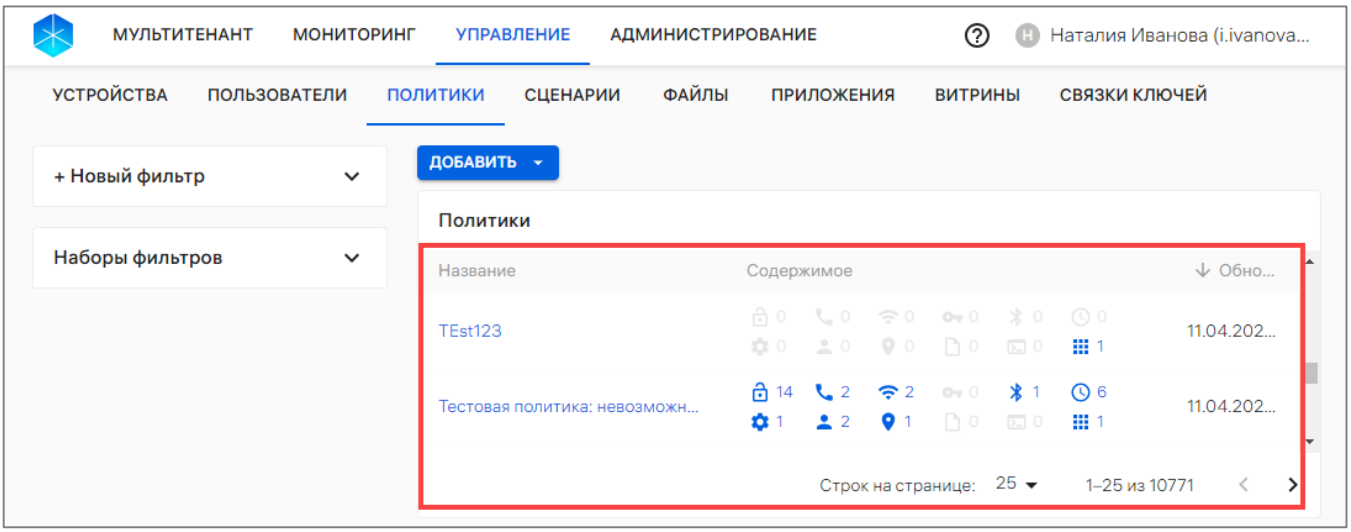

Рисунок 131

В рабочей области подраздела «Политики» (Рисунок 131) информация о политике отображается в столбцах, приведенных в таблице (Таблица 36).

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

Таблица 36

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 Bluetooth®
			Конфигурация
			Система
			Настройки пользователя
			Геопозиционирование
			Установка приложений
	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 вовремя, так и после ее создания.

Список правил политик, доступных для каждой версии ОС, приведен в таблице (Таблица 37).

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 37).

Таблица 37

№ 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	7-11	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	7-11	-	-	-	-	пп. 2.4.1.2
3	Ограничение доступа/Снимки экрана	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.3
4	Ограничение доступа/Управление авиарежимом	4.0.2 и выше	9-11	-	-	-	-	пп. 2.4.1.4
5	Ограничение доступа/Управление точкой доступа WLAN	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.5
6	Ограничение доступа/Управление Bluetooth	4.0.2 и выше	9-11	-	-	-	-	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	9-11	-	-	-	-	пп. 2.4.1.8
9	Ограничение доступа/Передача данных MTP	4.0.2 и выше	9-11	-	-	-	-	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	-	-	-	-	-	пп. 2.4.1.12
13	Ограничение доступа/Использование SD-карт	4.1.0 и выше	-	-	-	-	-	пп. 2.4.1.13
14	Ограничение доступа/Режим киоска	-	7-11	-	-	-	-	пп. 2.4.1.14
15	Голосовые вызовы/Исходящие вызовы	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.15
16	Голосовые вызовы/Входящие вызовы	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.16
17	Конфигурация WLAN/Режим работы WLAN	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.17
18	Конфигурация WLAN/Подключения к сети WLAN	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.18
19	Конфигурация VPN/Подключения VPN	4.0.2 и выше	7-11	-	-	-	-	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 Bluetooth/Режим работы Bluetooth	4.0.2 и выше	9-11	-	-	-	-	пп. 2.4.1.20
21	Конфигурация/Расписание получения команд	4.0.2 и выше	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.21
22	Конфигурация/Расписание отправки состояния	4.0.2 и выше	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.22
23	Конфигурация/Расписание отправки событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.23
24	Конфигурация/Исключения событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.24
25	Конфигурация/Хранение логов на устройстве	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.25
26	Конфигурация/Обновление координат в клиенте Аврора Центр	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.26
27	Система/Установить версию ОС	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.27
28	Настройки пользователя/Требования к паролю	4.0.2 и выше	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.28
29	Настройки пользователя/Создать пользователя	4.0.2 и выше	-	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.29

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
30	Настройки пользователя/Сертификаты пользователя	4.0.2 и выше	7-11	-	-	-	-	пп. 2.4.1.30
31	Геопозиционирование/ Настройки режима работы геопозиционирования	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.33
32	Файлы/Доставка на устройство	-	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.31
33	Скрипты/Выполнение на устройстве	-	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	7.3.4	пп. 2.4.1.32
34	Приложения/Установка приложений на устройство	4.0.2 и выше	7-11	p10	1.7 «Special Edition»	20 LTS, 22 LTS	-	пп. 2.4.1.34

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.

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

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 МТР и исходящие вызовы (кроме экстренных). Поэтому если на устройство назначена политика с разрешением передачи данных по МТР 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 132).

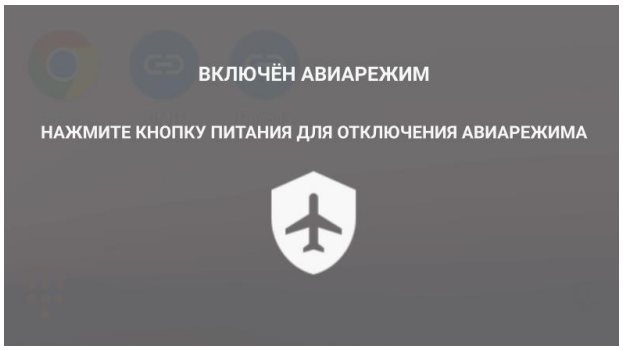

Рисунок 132

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).

ПРИМЕЧАНИЯ:

✓ 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.

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 применении 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.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 помощи переключателя.

ПРИМЕЧАНИЕ. При добавлении правила переключатель по умолчанию включен;

2) В поле «Отключение панели управлений» 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) В поле «Приложения» указать приложения, которые будут доступны пользователю в режиме киоска. Для этого следует ввести название пакета приложения (необходимые данные доступны для просмотра в карточке устройства в столбце «Инфо» (пп. 2.1.1.9).

ПРИМЕЧАНИЯ:

✓ Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного ярлыка веб-страницы;

✓ Возможно добавление нескольких приложений;

5) Добавить ярлыки веб-страниц, позволяющих открыть необходимые сайты, 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/.

ПРИМЕЧАНИЯ:

✓ Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного приложения;

✓ Возможно добавление нескольких ярлыков веб-страниц;

6) Настроить список разрешенных/запрещенных сайтов доступна, если в качестве дефолтного браузера используется Chrome.

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.omp.ru/) и нажать Enter.

ПРИМЕЧНАИЯ:

✓ С помощью кнопки «Добавить ярлыки в список исключений» также возможно добавить в разрешенный список адреса сайтов из ярлыков, которые указаны на шаге 5;

✓ 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.omp.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.omp.ru/, то после редиректа он станет https://omp.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 132);

– 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.

2.4.1.15.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).

2.4.1.16.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.

2.4.1.17.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).

2.4.1.18.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 этого необходимо:

Для подключения к беспроводной сети с технологией безопасности WPA-EAP по протоколу TLS необходимо:

– в раскрывающемся списке «Безопасность» выбрать «WPA-EAP»;

– в раскрывающемся списке «Протокол» выбрать «TLS»;

– в раскрывающемся 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 раскрывающемся списке «Идентификатор» выбрать динамическую перемененную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

- `{{UserEmail}}` – email из карточки пользователя;
- `{{UserPrincipalName}}` –значение параметра «userPrincipalName» из LDAP-данных о пользователе.

2) EAP

Для подключения к беспроводной сети с технологией безопасности WPA-EAP по протоколу PEAP необходимо:

– в раскрывающемся списке «Безопасность» выбрать «WPA-EAP»;

– в раскрывающемся списке «Протокол» выбрать «PEAP»;

– в раскрывающемся списке «Идентификатор» выбрать динамическую перемененную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

- `{{UserEmail}}` – email из карточки пользователя;
- `{{UserPrincipalName}}` – значение параметра «userPrincipalName» из LDAP-данных о пользователе;
- `{{sAMAccountName}}` - значение параметра sAMAccountName из LDAP-данных о пользователе.

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 получено несколько пользователей, то будет выбран тот, который привязан к устройствам последним.

Если необходимо создать на устройствах еще 1 подключение к сети WLAN, то необходимо нажать значок + внизу правила и повторить шаги, приведенные выше.

2.4.1.19.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» введите 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 вместе с созданием подключения VPN, чтобы 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 недоступен для редактирования;

• в раскрывающемся списке «Логин» необходимо выбрать динамическую перемененную, 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 который был получен из интеграции с LDAP. Если из LDAP получено несколько пользователей, то будет выбран тот, 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.

2.4.1.20.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).

2.4.1.21.Конфигурация/Расписание получения команд

Правило задает расписание на получение оперативных команд и политик.
Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.22.Конфигурация/Расписание отправки состояния

Правило задает расписание отправки состояния устройства на ПУ.
Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.23.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.»

2.4.1.24.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 вручную 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 плюса внизу фильтра и также ввести вручную 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.

2.4.1.25.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.

2.4.1.26.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»).

2.4.1.27.Система/Установить версию ОС

Правило предназначено для обновления ОС на устройствах и задает:

– версию ОС, которая будет установлена на устройствах;

– временной интервал, в течение которого на устройствах будет установлена указанная версия ОС.

Если текущая версия ОС Аврора больше или равна версии из политики, обновление ОС Аврора не выполняется.

Для создания правила требуется выбрать из раскрывающегося списка необходимую версию ОС. Список версий ОС заполняется в соответствии с версиями дистрибутивов в файловом хранилище ПООС. Описание ПООС приведено в документе «Руководство администратора».

Выбор времени старта и завершения обновления в формате: «Установка с [часы]: [минуты] до [часы]: [минуты]».

2.4.1.28.Настройки пользователя/Требования к паролю

Правило задает следующие параметры:

– сложность пароля для разблокировки устройства;

– срок действия пароля.

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

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;

– «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.

2.4.1.29.Настройки пользователя/Создать пользователя

Правило разрешает или запрещает создание пользователя при активации устройства.

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

Выбор значения из списка:

– «Создавать» (при добавлении правила значение выбрано по умолчанию);

– «Не создавать».

2.4.1.30.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. 2.2.6);

– выполнить одно из действий:

- привязать устройство к группе устройств (п. 2.2.7);

- 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.

2.4.1.31.Файлы/Доставка на устройство

Правило позволяет выбрать один или несколько файлов, которые необходимо доставить на устройство.

Для создания правила необходимо:

– 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 добавьте его, выполнив действия описанные в п. 2.6.1;

– 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.

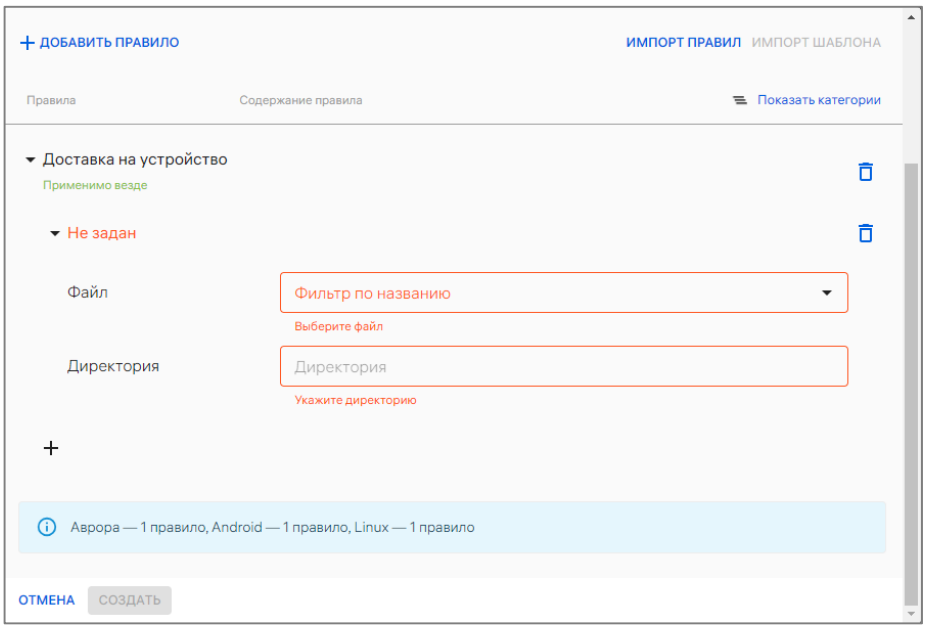

Рисунок 133

2.4.1.32.Скрипты/Выполнение на устройстве

Правило позволяет доставить и выполнить скрипт на устройстве.

Для создания правила необходимо:

– в раскрывающемся списке «Путь к файлу» (Рисунок 134 [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» и заполнить параметры правила по доставке файлов (пп. 2.4.1.31).

– в поле «Таймаут» (Рисунок 134 [2]) необходимо ввести время в формате [мм:сс], если требуется чтобы скрипт на устройстве выполнился через некоторое время после доставки.

Если необходимо добавить в правило еще один выполняемый скрипт, то необходимо нажать на значок + (Рисунок 134 [3]) в левом нижнем углу и повторить действия описанные выше.

Подробное описание о выполнении скриптов на устройстве приведено в п. 2.6.2.

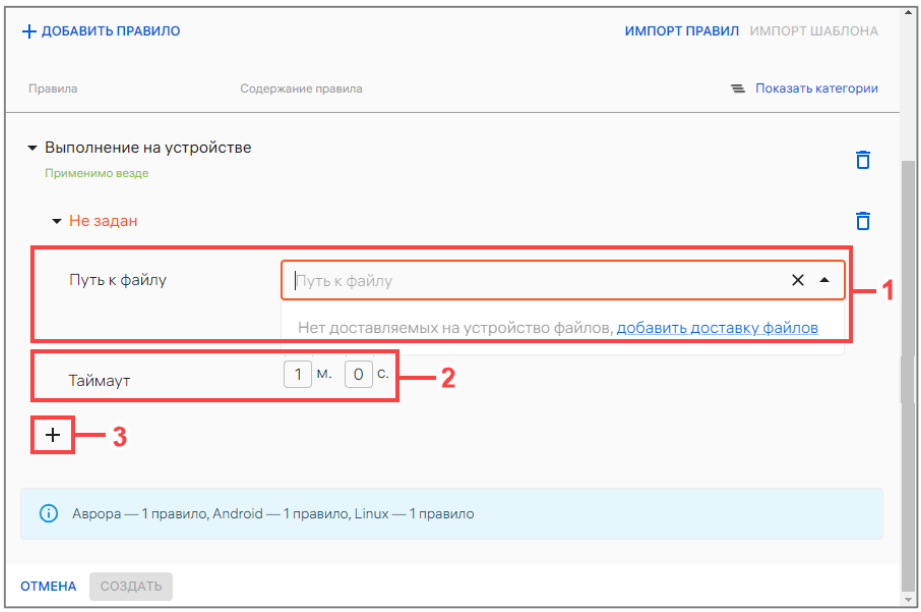

Рисунок 134

2.4.1.33.Геопозиционирование/Настройки режима работы геопозиционирования

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.

2.4.1.34.Приложения/Установка приложений на устройство

Правило предназначено для установки приложения выбранной витрины и версии на устройствах, а также позволяет обновлять и удалять установленные приложения. Приложений в политике может быть задано несколько.

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

ПРИМЕЧАНИЕ. Предусмотрена возможность задать дополнительные правила по добавлению нескольких приложений в политику, выполнив действия, описанные в п. 2.4.5.

Чтобы приложение было доступно для выбора, необходимо выполнение следующих условий:

– приложение должно быть добавлено и опубликовано в ПМ (подробная информация приведена в документе «Руководство пользователя. Часть 2. Подсистема «Маркет»);

– видимость витрины с приложением включена в настройках интеграции с Сервером приложений (п. 4.1.4);

– приложения для ОС Аврора, ОС Android, ОС Альт Linux и ОС Astra Linux должны находиться в отдельных витринах (описание процедуры создания витрины с приложением приведено в документе «Руководство пользователя. Часть 2. Подсистема «Маркет»).

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.

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.

Для создания правила необходимо:

1) 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 135);

– в раскрывающемся списке «Время установки» выбрано значение «Моментально».

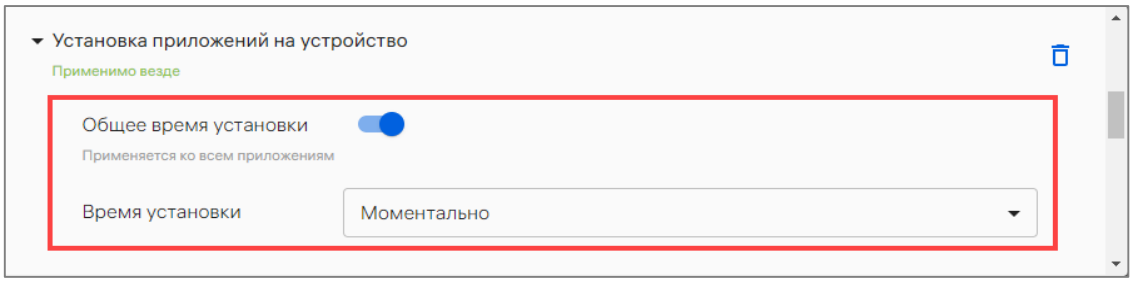

Рисунок 135

2) 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 136);

– в раскрывающемся списке «Время установки» выбрано значение «Интервал»;

– в поле «Интервал установки» указать начало и конец временного интервала, в течение которого можно установить приложения.

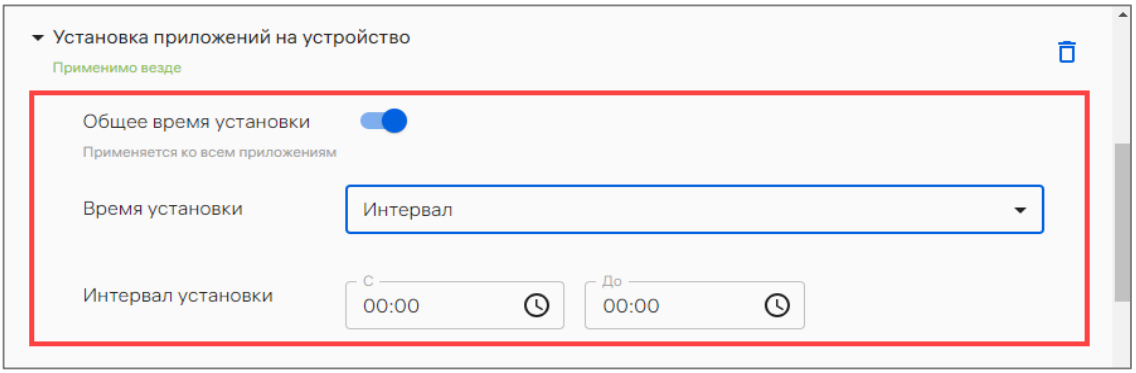

Рисунок 136

3) В полях с раскрывающимися списками выбрать (Рисунок 137):

– витрину, в которой размещено приложение;

– приложение, которое необходимо установить на устройства;

– номер версии приложения;

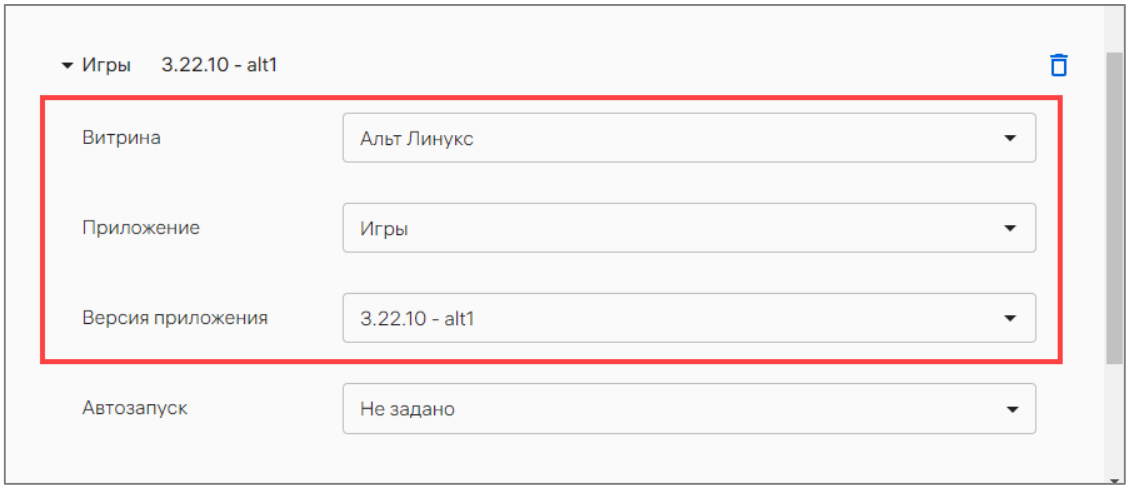

Рисунок 137

4) Для устройств, функционирующих на базе ОС Аврора доступно задать автозапуск приложения. Для этого в раскрывающемся списке «Автозапуск» 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;

5) 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 138), если необходимо, чтобы приложение установилось сразу после получения политики устройством;

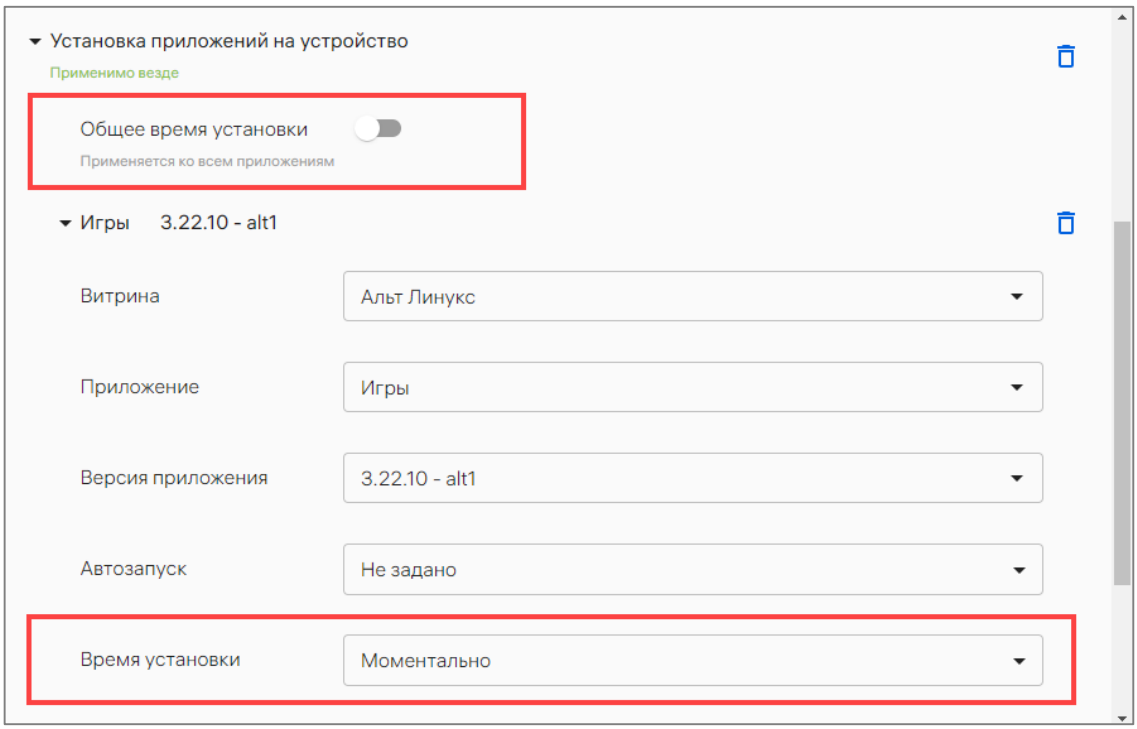

Рисунок 138

- пункт «Интервал» (Рисунок 139), если необходимо, чтобы приложение установилось на устройстве в заданный интервал времени. И затем в поле «Интервал установки» указать начало и конец временного интервала.

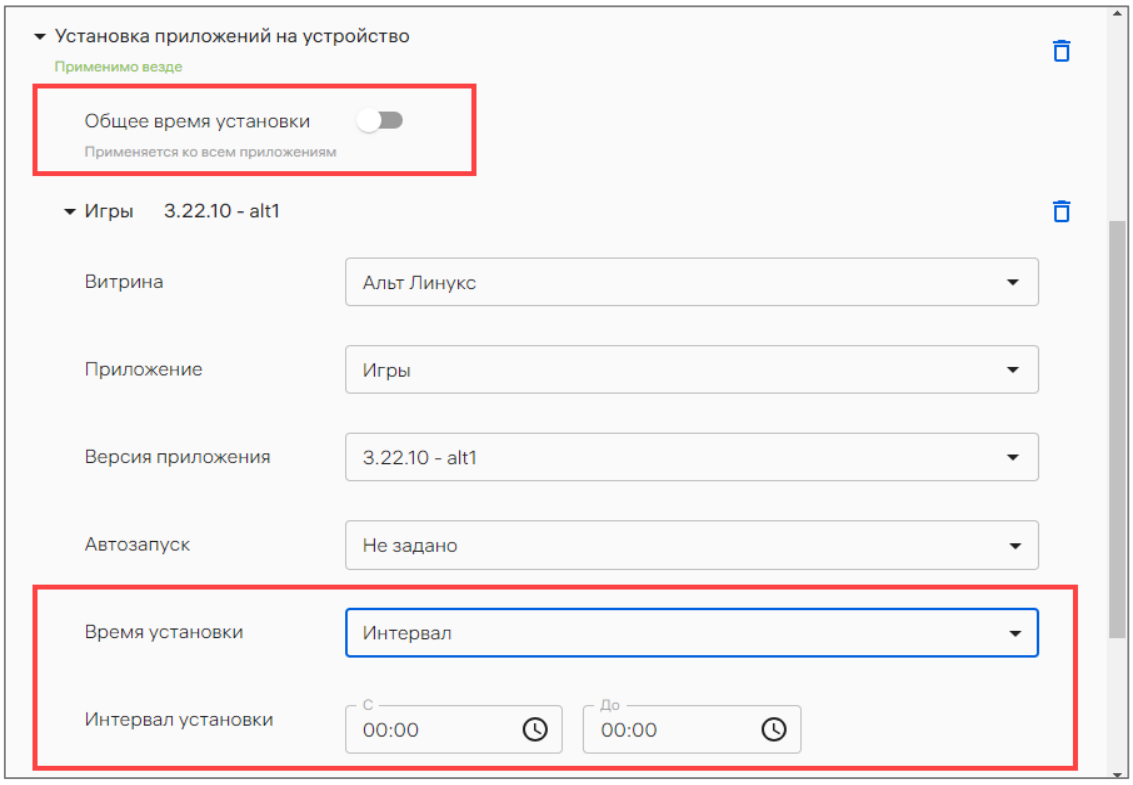

Рисунок 139

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 140).

После выдачи разрешения это окно не будет отображаться при последующих установках приложений с помощью политики.

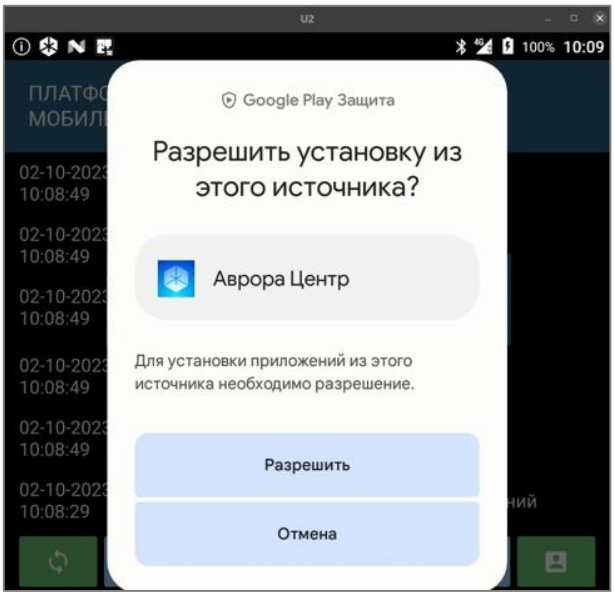

Рисунок 140

Начиная с версии ОС Аврора 5.1.0:

– 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.

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 141);

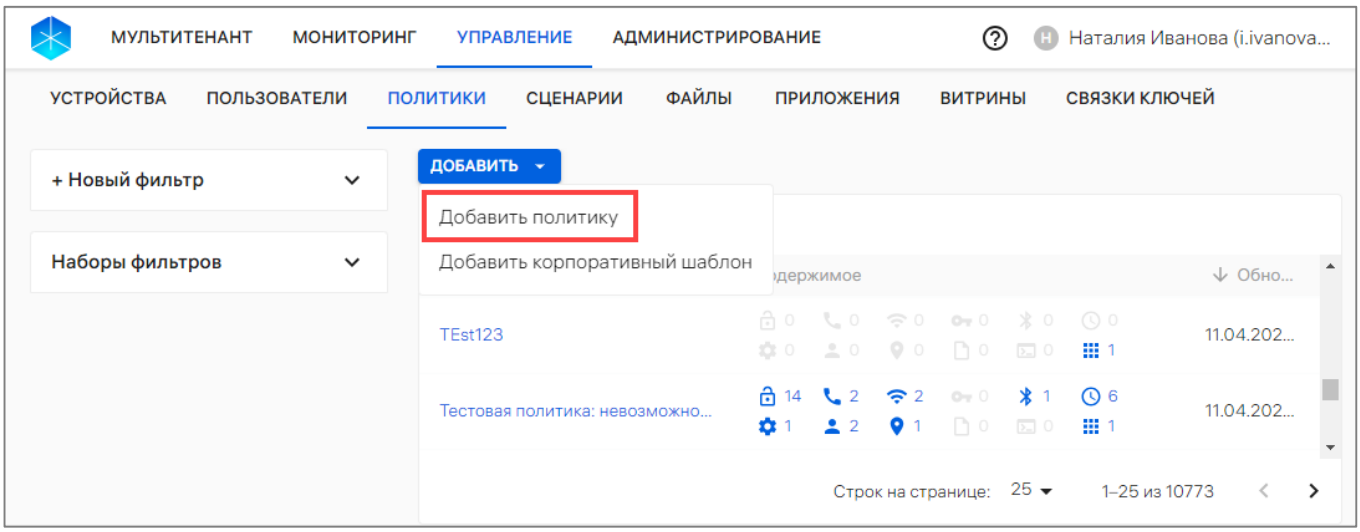

Рисунок 141

– в открывшемся окне:

- ввести название политики - название политики должно быть уникальным. Поле обязательно для заполнения (Рисунок 142 [1]);
- ввести комментарий - при необходимости ввести дополнительную информацию к политике (Рисунок 142 [2]);
- нажать кнопку «Добавить правило» (Рисунок 142 [3]) и выбрать правило политики из раскрывающегося списка;
- задать параметры правила (Рисунок 142 [4]). Описание правил для политик приведено в таблице (см. Таблица 37).

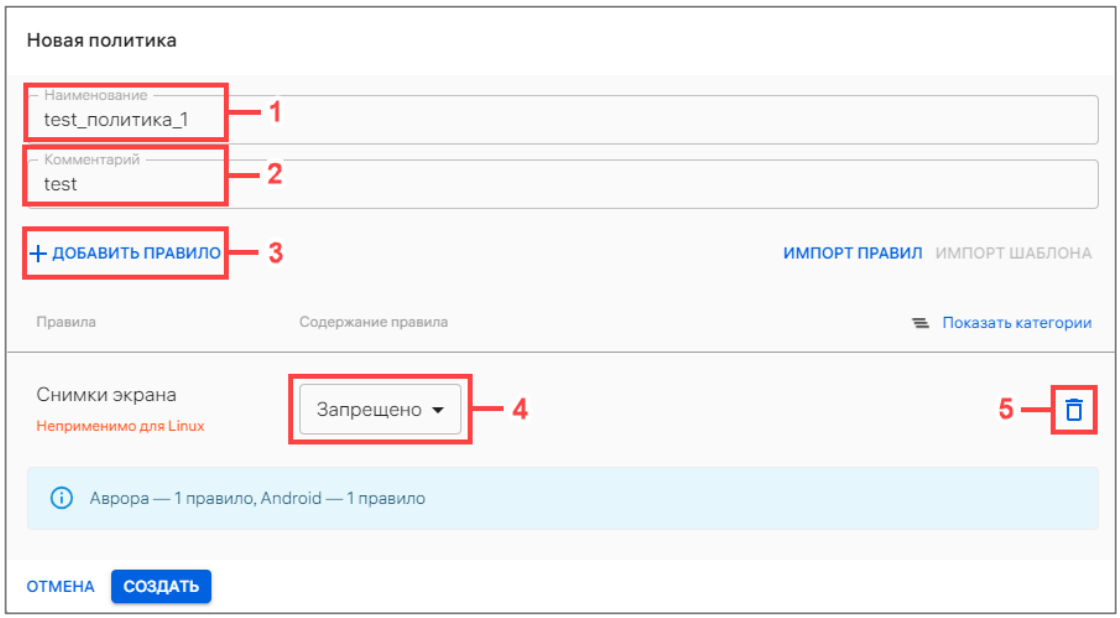

Рисунок 142

В случае необходимости создать политику из нескольких правил, следует повторить действия, описанные выше.

В случае необходимости удалить правило следует нажать значок «Удалить» (Рисунок 142 [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. 2.4.5).

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 143), в результате чего правила из корпоративного шаблона будут импортированы в новую политику.

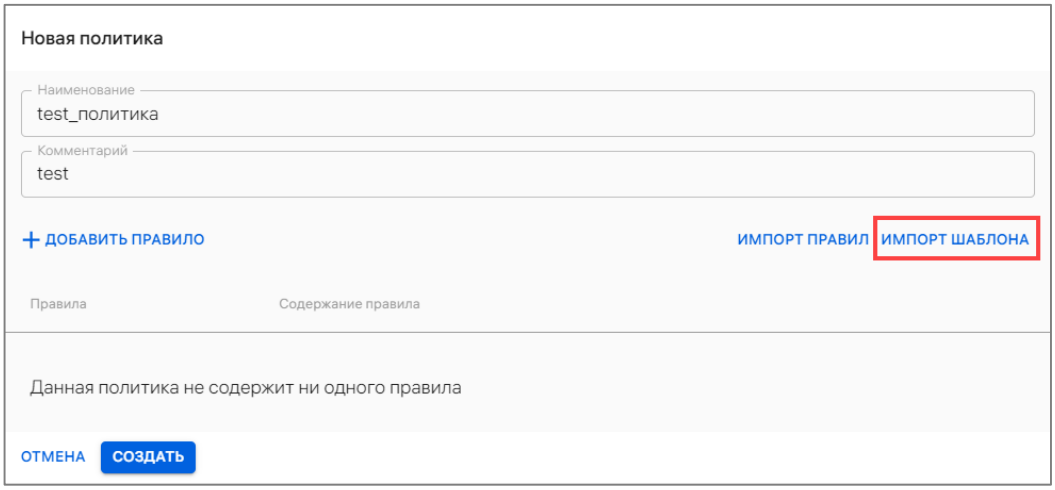

Рисунок 143

При необходимости, в соответствии с п. 2.4.1, импортированные правила возможно:

– изменить (см. Рисунок 142 [4]). Описание правил для политик приведено в таблице (см. Таблица 37);

– добавить правило в политику (см. Рисунок 142 [3]);

– удалить правило (см. Рисунок 142 [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» (Рисунок 144).

ВНИМАНИЕ! Предусмотрена возможность создания только 1 корпоративного шаблона. Пункт меню «Добавить корпоративный шаблон» отсутствует, если корпоративный шаблон политик уже создан. Вместо него отображается пункт меню «Редактировать корпоративный шаблон» (Рисунок 146);

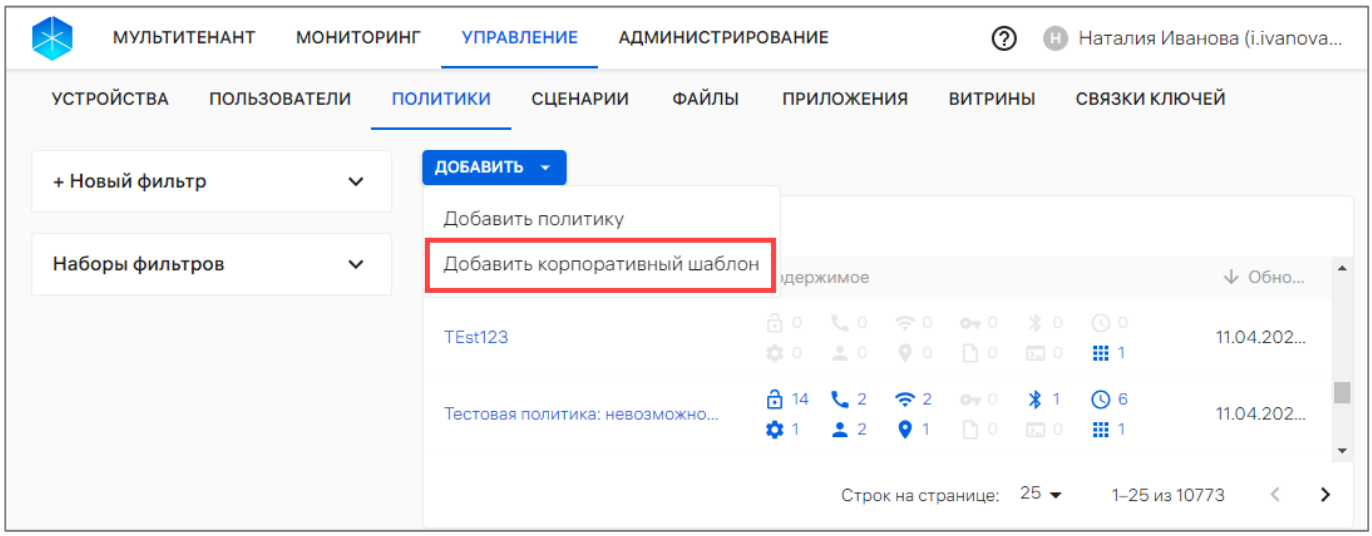

Рисунок 144

– в открывшемся окне возможно выполнить следующие действия:

- при необходимости изменить комментарий к корпоративному шаблону (наименование корпоративного шаблона проставляется автоматически) (Рисунок 145 [1]);
- добавить правила в корпоративный шаблон, нажав на кнопку «Добавить правило» (Рисунок 145 [2]). Добавление правила выполняется в соответствии с п. 2.4.1.

ПРИМЕЧАНИЕ. По умолчанию корпоративный шаблон не содержит ни одного правила;

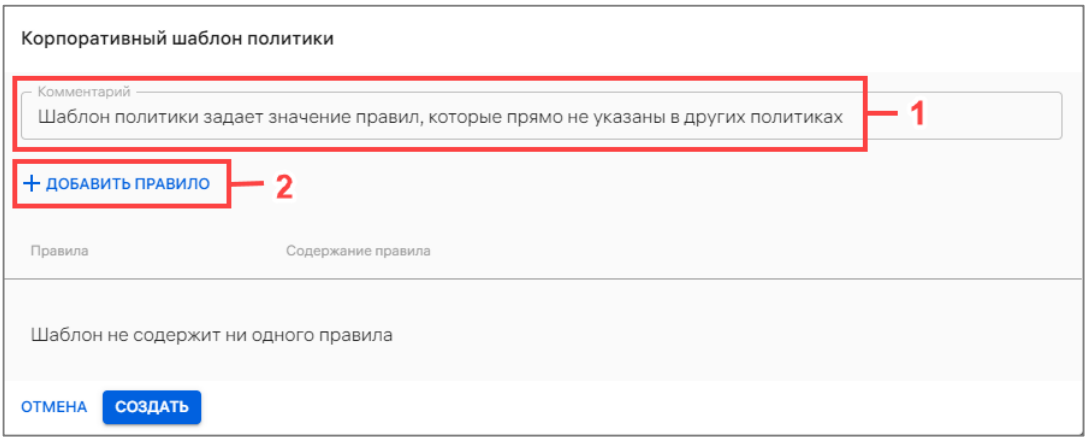

Рисунок 145

– 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 146);

– в открывшемся окне (см. Рисунок 145) внести изменения, выполнив действия, приведенные в пп. 2.4.3.1.

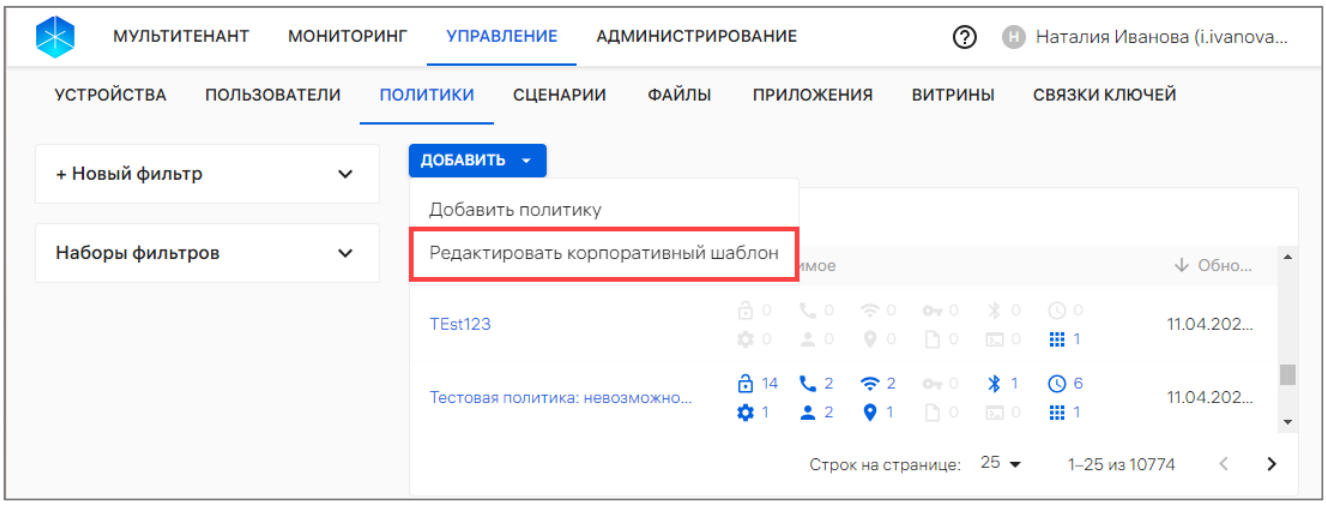

Рисунок 146

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. 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, п. 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 147);

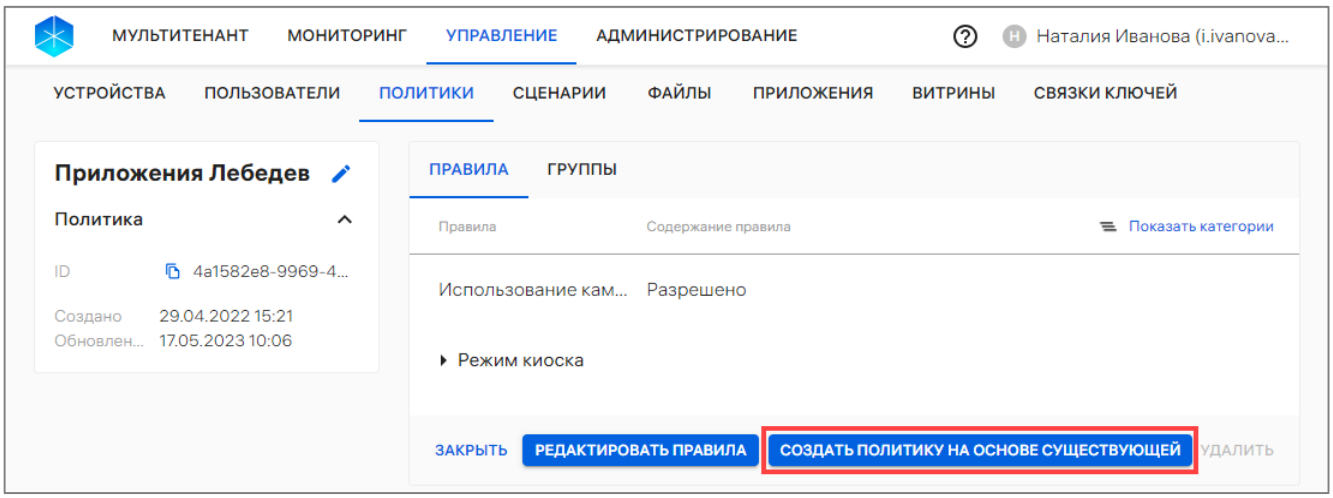

Рисунок 147

• в списке политик нажать кнопку «Добавить» или выбрать из раскрывающегося списка «Добавить политику» (см. Рисунок 141), а затем нажать кнопку «Импорт правил» (Рисунок 148 [1]). Из раскрывающегося списка выбрать правило политики, которое необходимо скопировать (при необходимости воспользоваться фильтром по названию политики) (Рисунок 148 [2]). В результате правила из выбранной политики будут импортированы в новую политику;

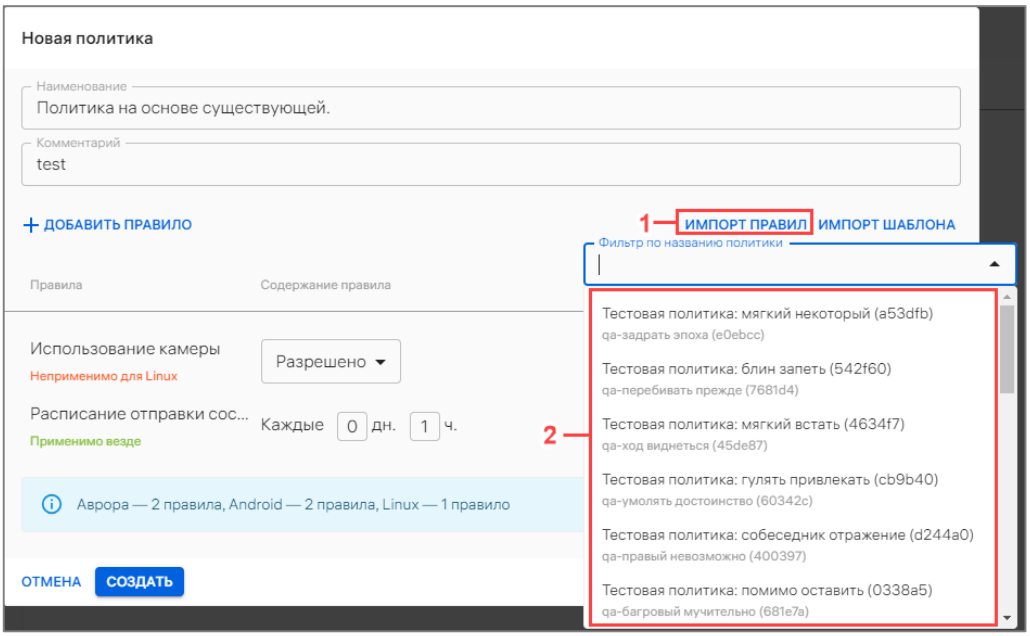

Рисунок 148

– 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 37).

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.

2.4.5. Редактирование правила политики

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 149);

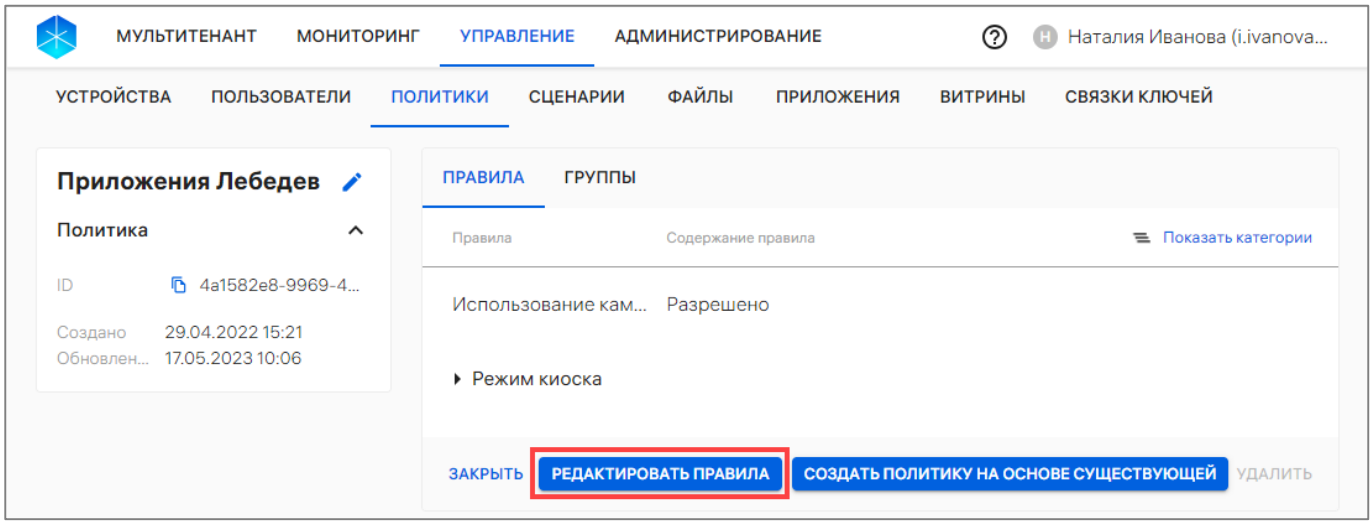

Рисунок 149

– в открывшемся окне внести изменения в правилах политики (Рисунок 150 [2]) в соответствии с таблицей (см. Таблица 37);

– для добавления дополнительных правил нажать кнопку «Добавить правило» (Рисунок 150 [1]) и выбрать правило политики из раскрывающегося списка и задать его параметры (при необходимости);

– для удаления правил из политики нажать значок «Удалить» (Рисунок 150 [3]) справа от правила (при необходимости);

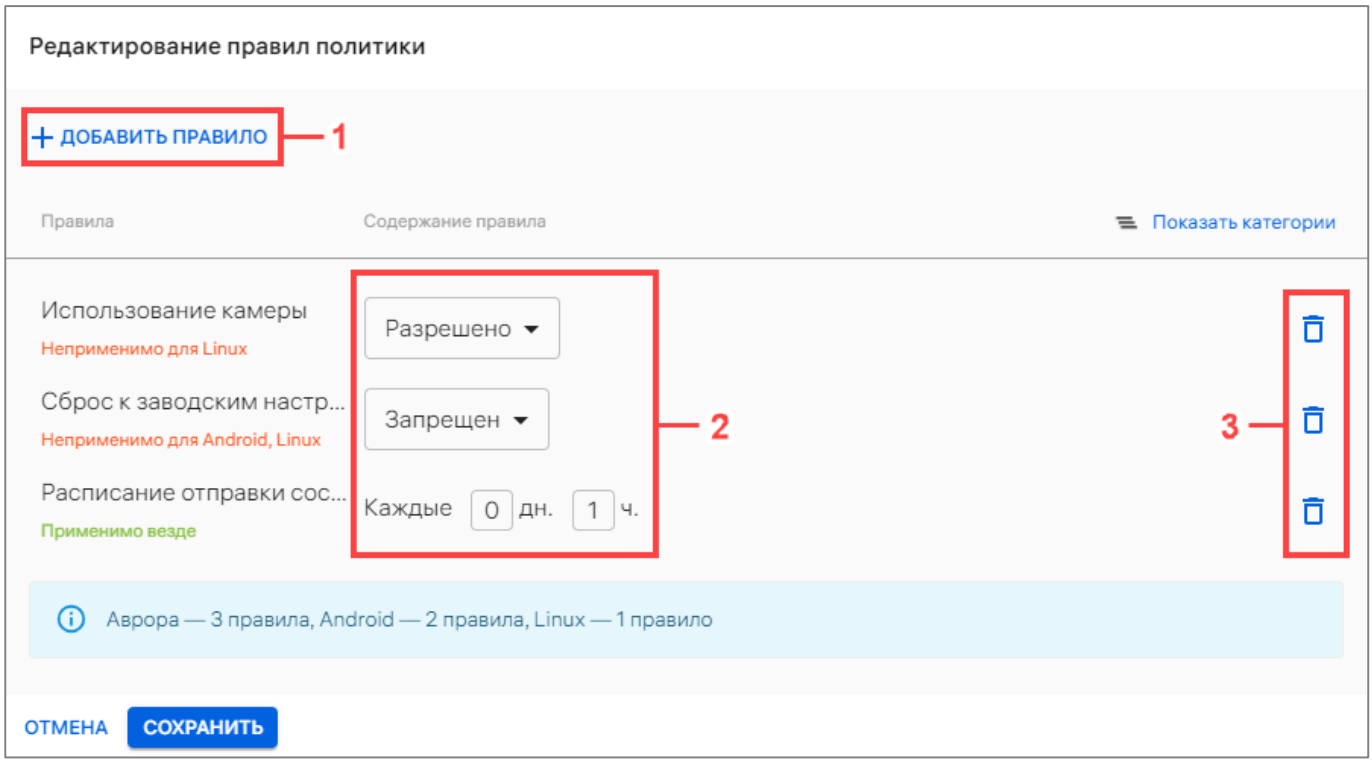

Рисунок 150

– 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 151 [1]).

Для автоматического применения политики следует нажать кнопку «Подтвердить» (Рисунок 151 [2]), не дожидаясь результата проверки, в результате чего политика с обновленными правилами будет назначена на все устройства.

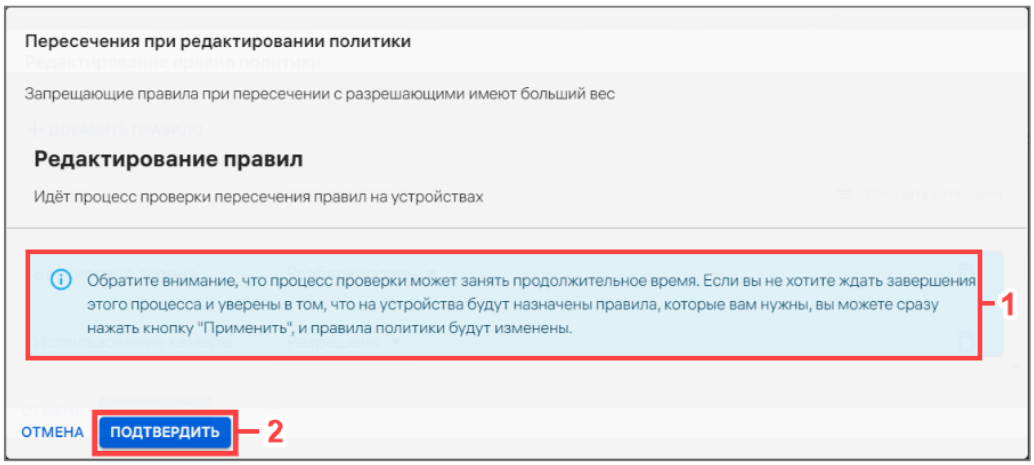

Рисунок 151

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 152), 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.

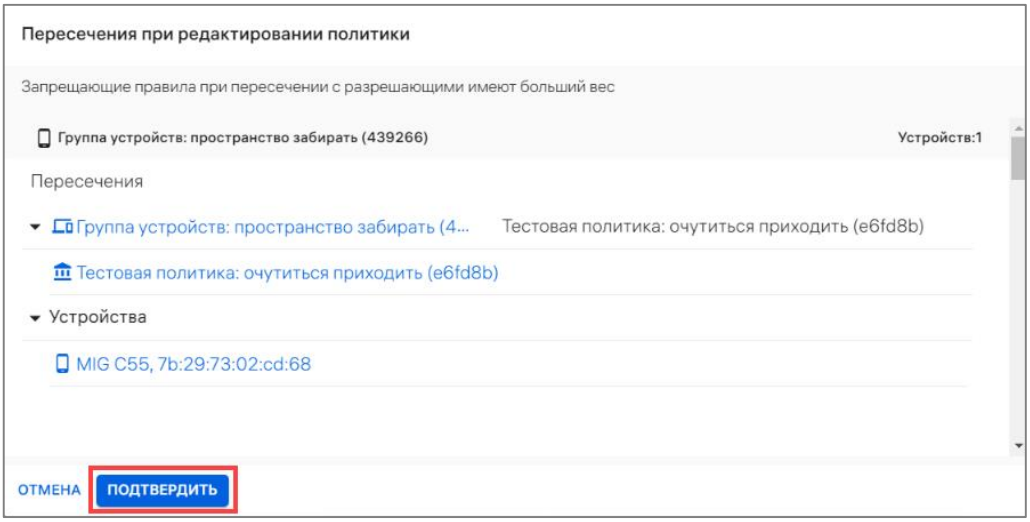

Рисунок 152

ПРИМЕЧАНИЕ. Перед применением скомбинированной политики следует учитывать следующее:

– приоритет имеют запрещающие правила;
– для правил с датами приоритет у более поздней даты 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.

2.4.6. Назначение политики на группы устройств или группы пользователей

Назначить политику на группу устройств и/или группу пользователей возможно через:

– карточку политики (пп. 2.4.6.1);
– карточку группы устройства (пп. 2.4.6.2);
– карточку группы пользователей (пп. 2.4.6.3).

2.4.6.1. 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 153 [1]);
– в раскрывающемся списке выбрать тип группы (Рисунок 153 [2]):
- «Группу устройств»;
- «Группу пользователей»;

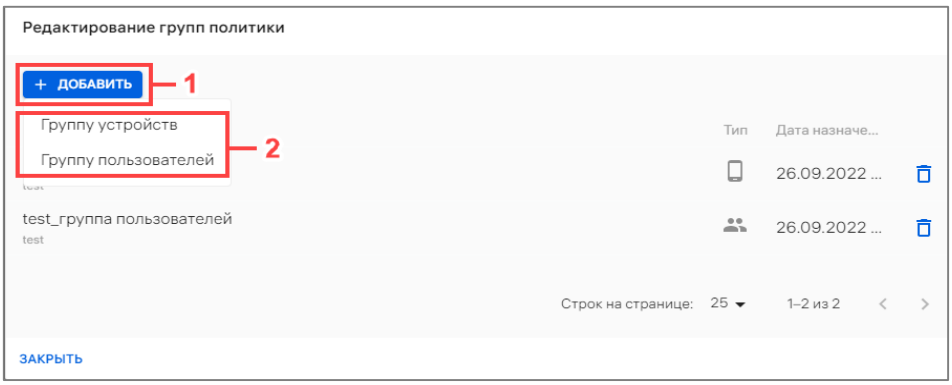

Рисунок 153

– 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. 2.4.5.

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.

2.4.6.2. 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 154 [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 154 [3]);

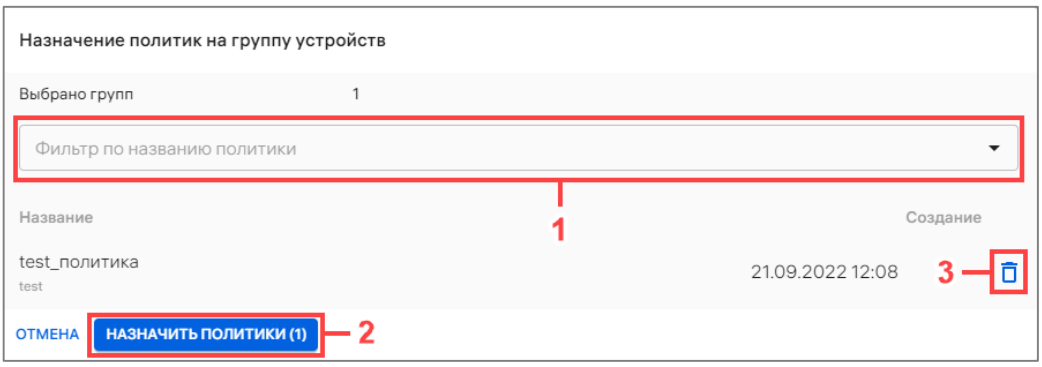

Рисунок 154

– нажать кнопку «Назначить политики» (Рисунок 154 [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. 2.4.5.

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.

2.4.6.3. 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 154) выполнить действия, приведенные в пп. 2.4.6.2.

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.

2.4.7. Отвязка политики от группы устройств или группы пользователей

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 155).

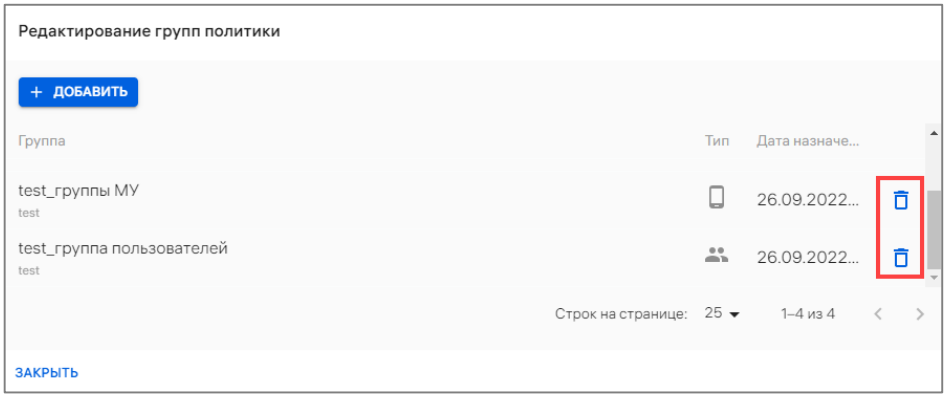

Рисунок 155

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. 2.4.5.

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 156 [1]);

– в списке быстрых действий выбрать значок «Отвязать политики от группы» (Рисунок 156 [2]).

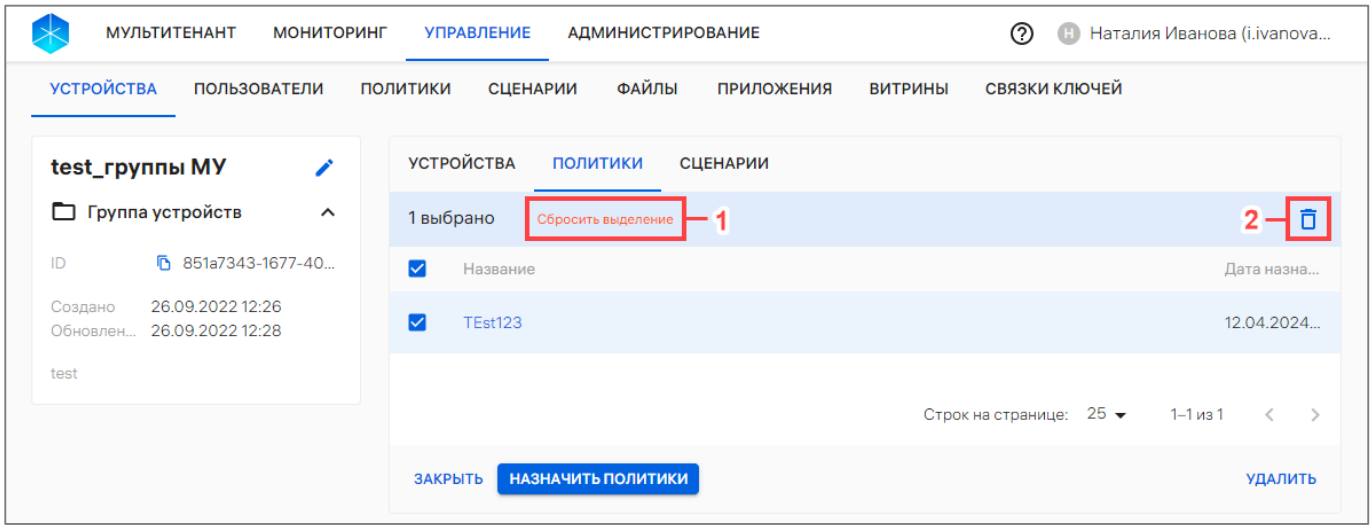

Рисунок 156

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. 2.4.5.

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 157 [1]);

– в списке быстрых действий выбрать значок «Отвязать политики от группы» (Рисунок 157 [2]).

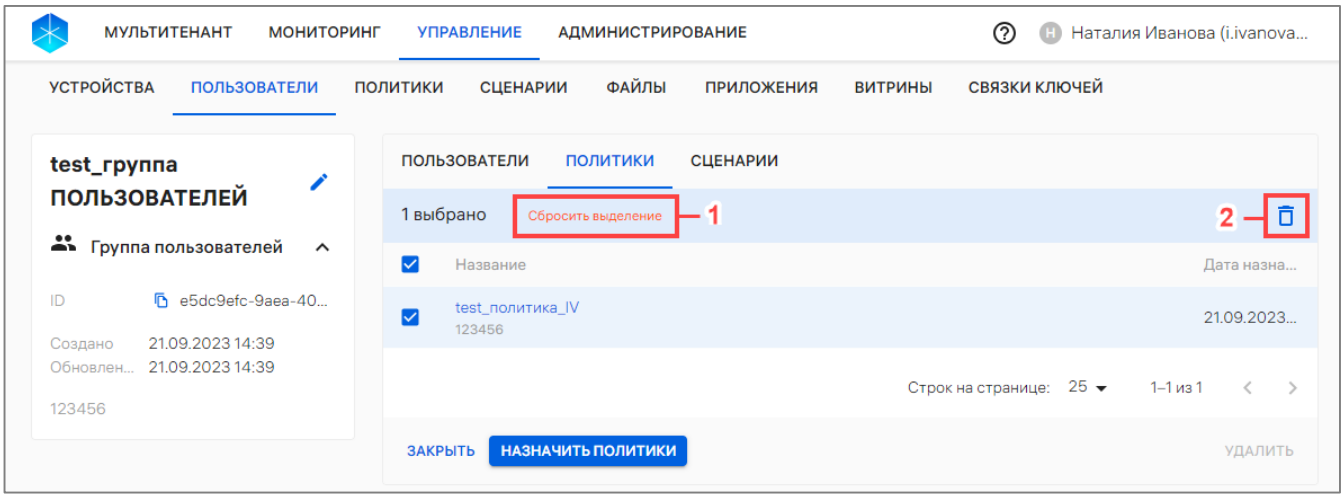

Рисунок 157

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. 2.4.5.

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 158);

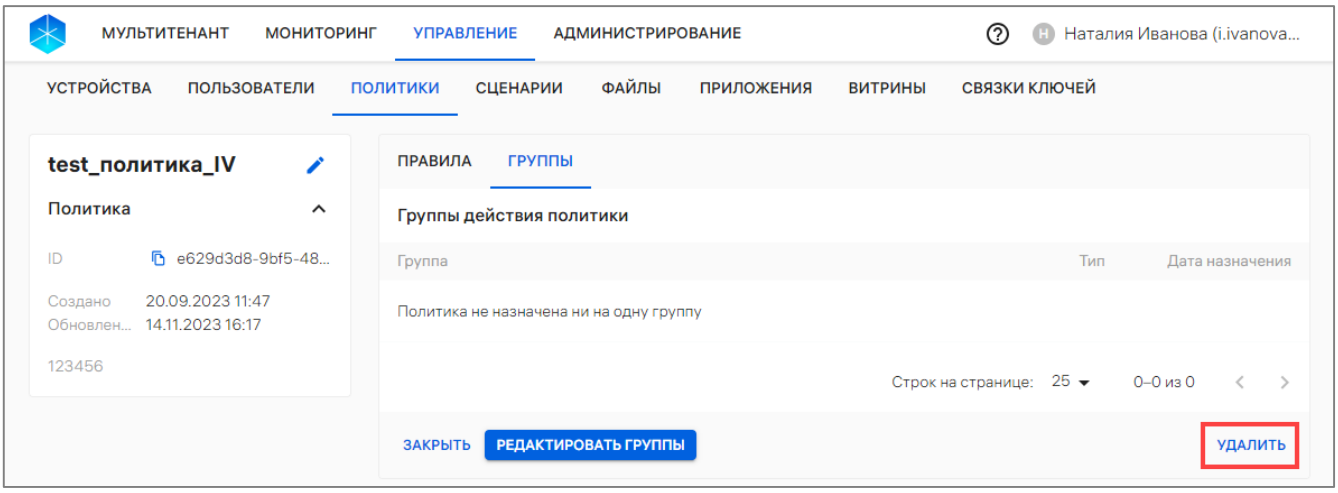

Рисунок 158

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 159).

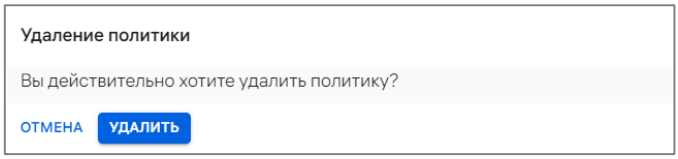

Рисунок 159

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.

ПРИМЕЧАНИЕ. 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 38).

Таблица 38

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 7-11	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	ОС Аврора 4.0.2 и выше
Нахождение вне территорий, определяемых координатами	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	ОС Аврора 4.0.2 и выше
Нахождение на территориях, определяемых координатами	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	ОС Аврора 4.0.2 и выше	ОС Аврора 4.0.2 и выше	– ОС Аврора 4.0.2 и выше; – ОС Android 7-11	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 160 [1]).

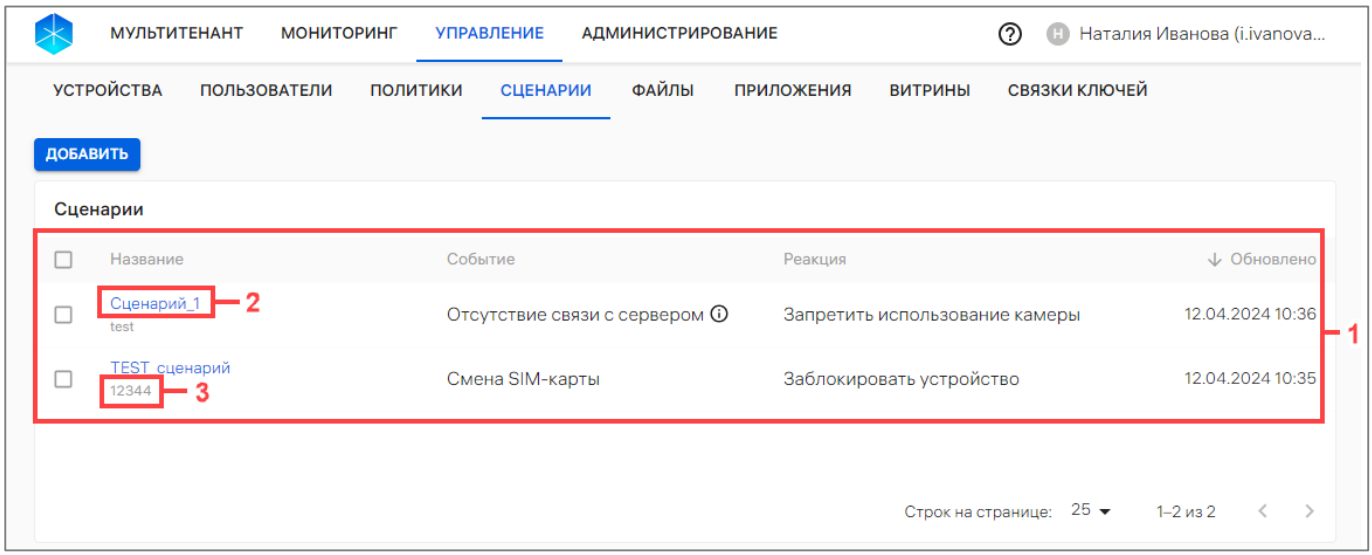

Рисунок 160

В рабочей области подраздела «Сценарии» информация отображается в столбцах, приведенных в таблице (Таблица 39), а при их отсутствии отображается сообщение «Нет данных».

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

Таблица 39

Название столбца	Описание
Название	– название офлайн-сценария (представляет собой активную ссылку (Рисунок 160 [2]), при нажатии на которую осуществляется переход в карточку офлайн-сценария); – комментарий (Рисунок 160 [3]) – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 40). В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ
Реакция	Действие, которое должно произойти с группой в результате назначения данного офлайн-сценария (доступные значения описаны в таблице (Таблица 40)
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 161) заполнить поля, приведенные в таблице (Таблица 40);

– подтвердить либо отменить действия.

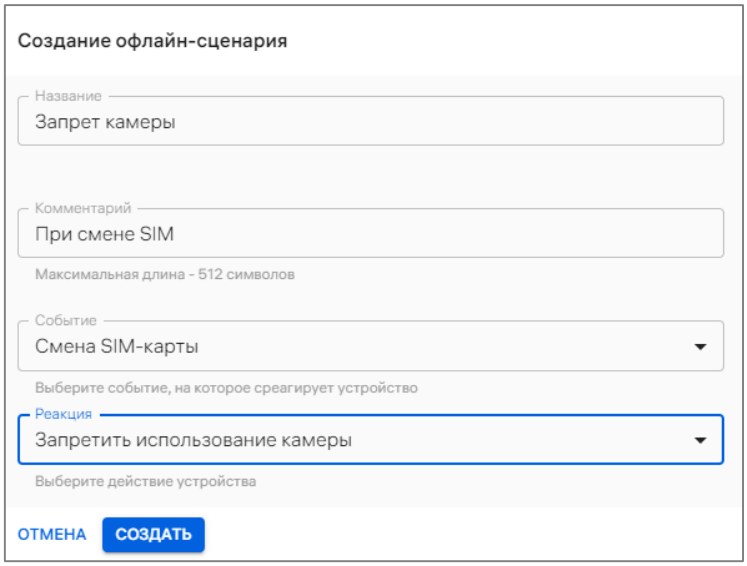

Рисунок 161

При успешном создании офлайн-сценария отобразится соответствующее сообщение.

Таблица 40

Параметр	Значения
Название	Название офлайн-сценария. Поле обязательно для заполнения
Комментарий	Дополнительная информация к офлайн-сценарию. Поле необязательно для заполнения
Событие	Выбор значения из раскрывающегося списка. Событие, на которое среагирует устройство: – **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». **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; – **Нахождение в зоне WLAN** - если устройство обнаружит определенную сеть WLAN в доступных для подключения, то сработает реакция, выбранная из раскрывающегося списка «Реакция». **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; – **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. **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.

	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 отправьте команду оперативного управления с разблокировкой камеры. 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. ВНИМАНИЕ! NFC-метка сканируется на устройствах: – 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. ПРИМЕЧАНИЯ: ✓ Если необходимой территории нет в списке, то требуется добавить ее (п. 4.1.6); ✓ 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;

Параметр	Значения
	✓ 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. 2.4.1.26)
Реакция	Выбор значения из раскрывающегося списка: – **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 162);

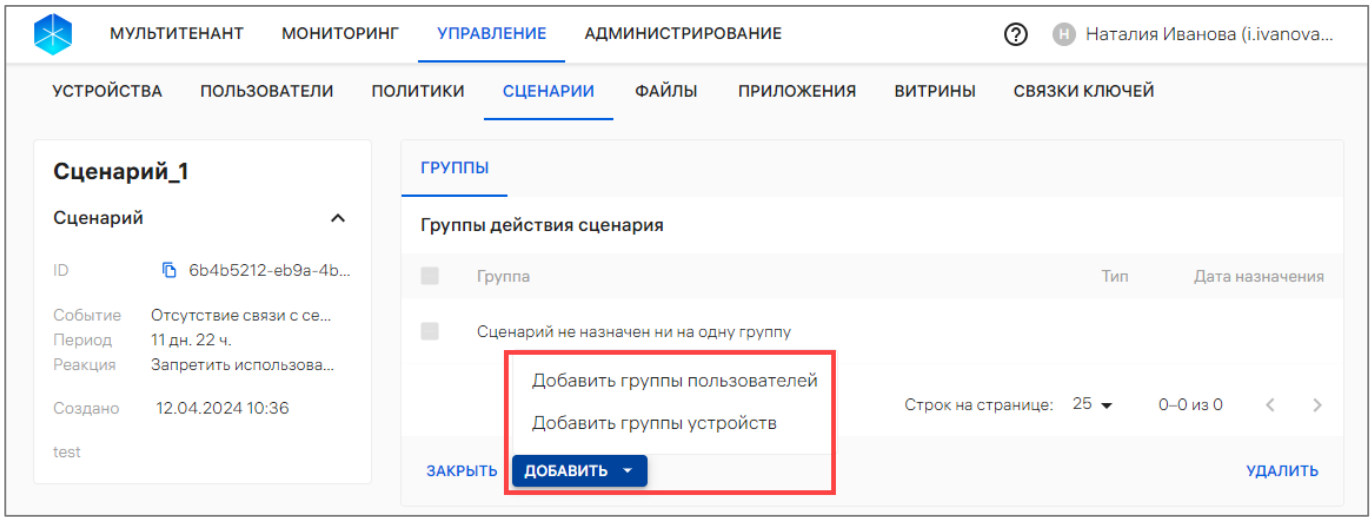

Рисунок 162

– в открывшемся окне выбрать группу из списка, при необходимости воспользовавшись фильтром по названию группы (Рисунок 163 [1]);

– добавленная группа отобразится в списке. При необходимости удалить добавленную группу из списка возможно, нажав значок 🗑 (Рисунок 163 [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 163 [3]).

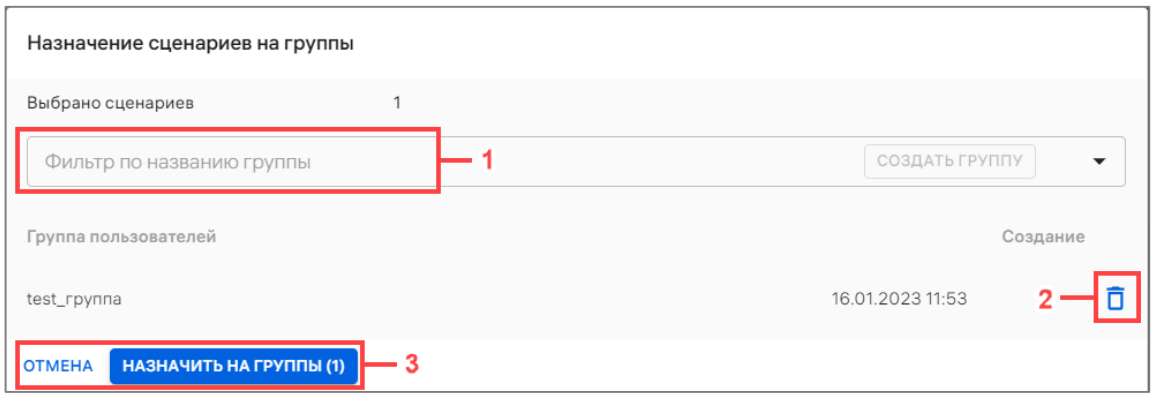

Рисунок 163

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 164 [1]);

– в списке быстрых действий выбрать:

- значок (Рисунок 164 [2]) для назначения офлайн-сценария на группу пользователей;
- значок (Рисунок 164 [3]) для назначения офлайн-сценария на группу устройств;

– в открывшемся окне выполнить действия, приведенные в пп. 2.5.2.1.

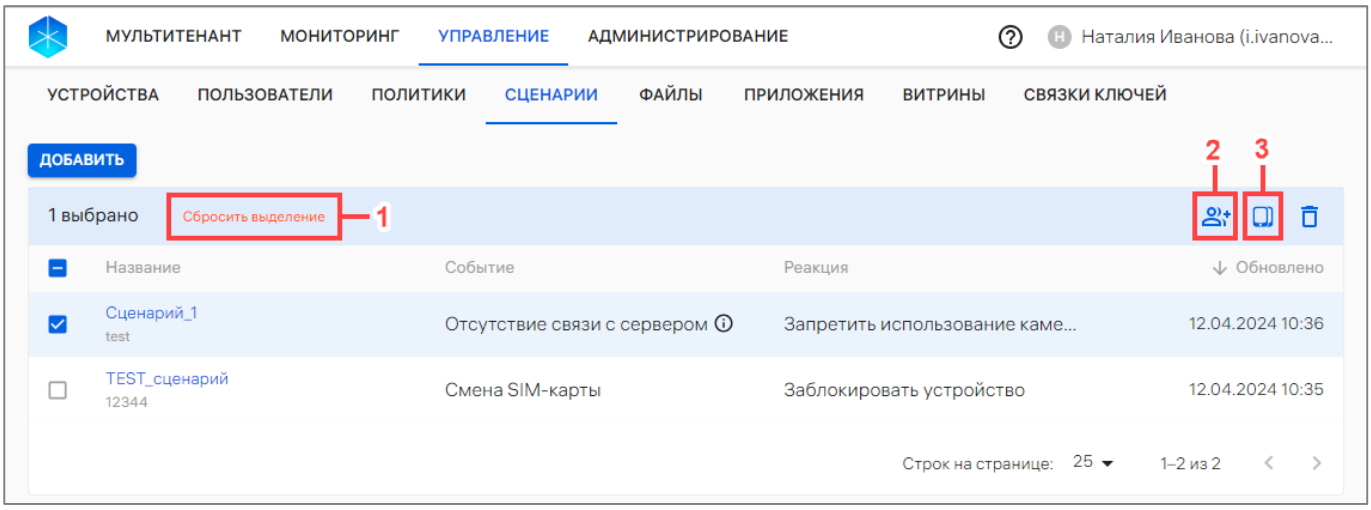

Рисунок 164

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 165);

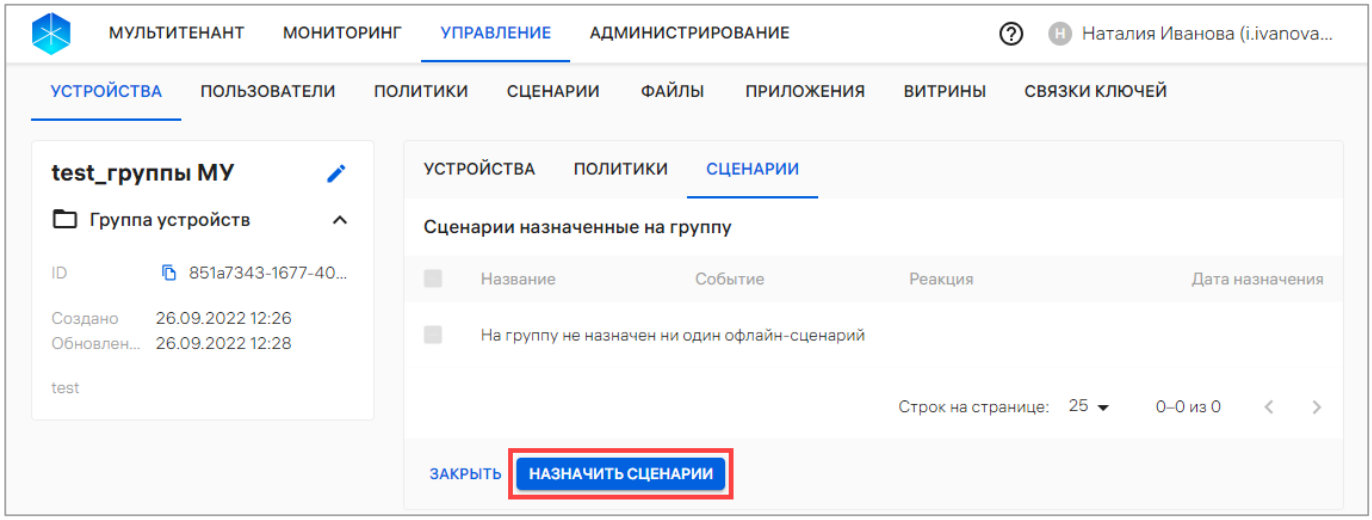

Рисунок 165

– в отобразившемся окне выбрать офлайн-сценарий из раскрывающегося списка или воспользоваться фильтром (Рисунок 166 [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 166 [3]);

Рисунок 166

– нажать кнопку «Назначить сценарии» (Рисунок 166 [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 167 [1]);

– в списке быстрых действий выбрать значок «Отвязать сценарий от группы» (Рисунок 167 [2]);

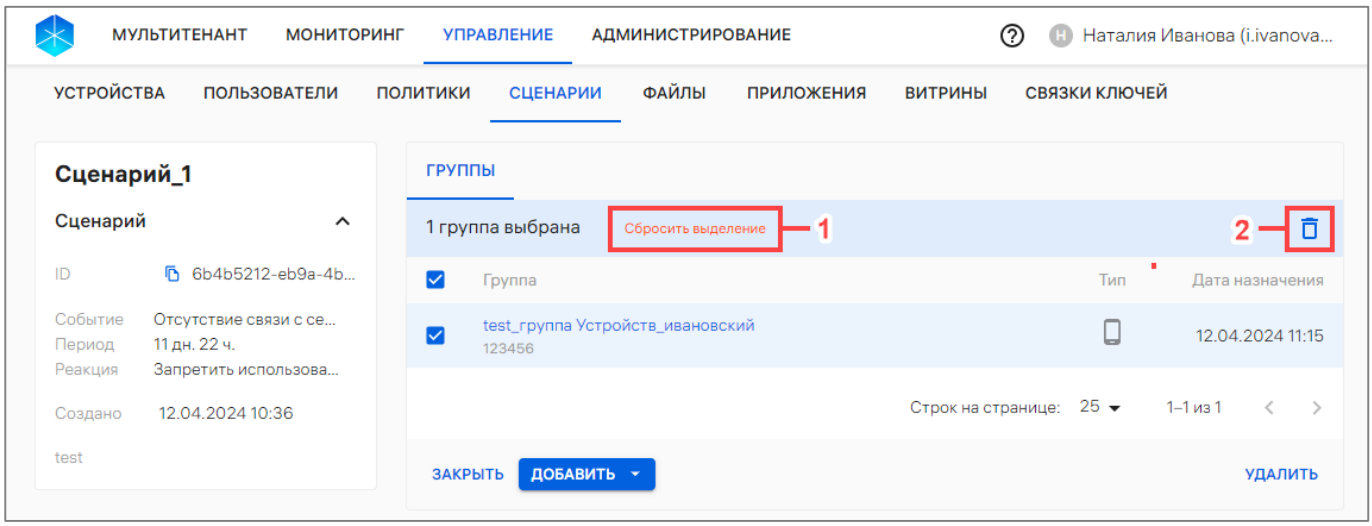

Рисунок 167

– в отобразившемся окне подтвердить либо отменить действие (Рисунок 168).

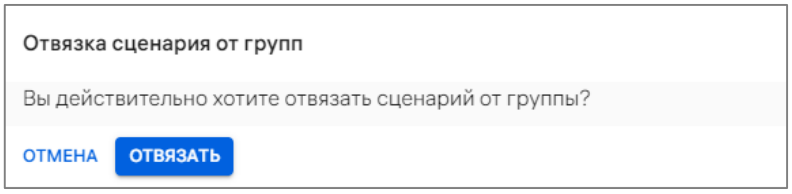

Рисунок 168

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 169 [1]);

– в списке быстрых действий выбрать значок «Отвязать сценарии от группы» (Рисунок 169 [2]);

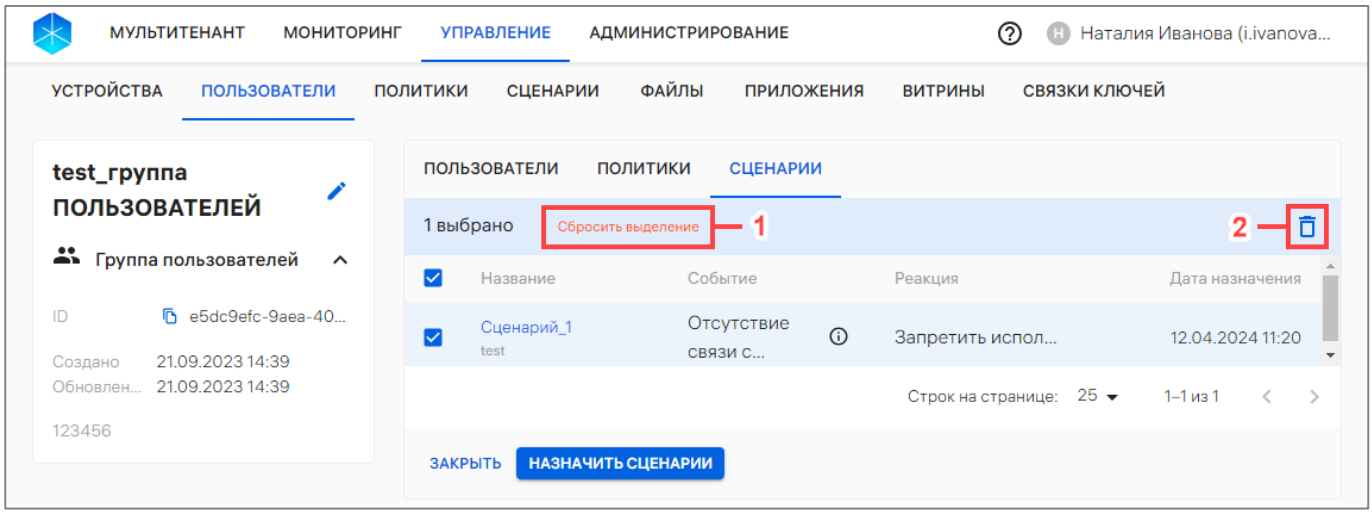

Рисунок 169

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 170).

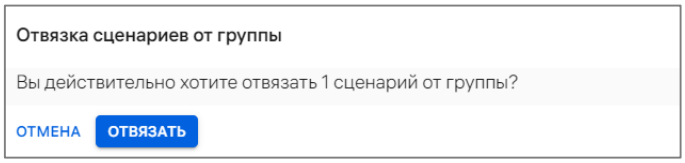

Рисунок 170

В результате успешной отвязки офлайн-сценарий будет удален со всех устройств группы.

ВНИМАНИЕ! Если действие данного офлайн-сценария уже применен 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 помощь списка быстрых действий. Для это 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 171 [1]);

– в списке быстрых действий выбрать значок (Рисунок 171 [2]);

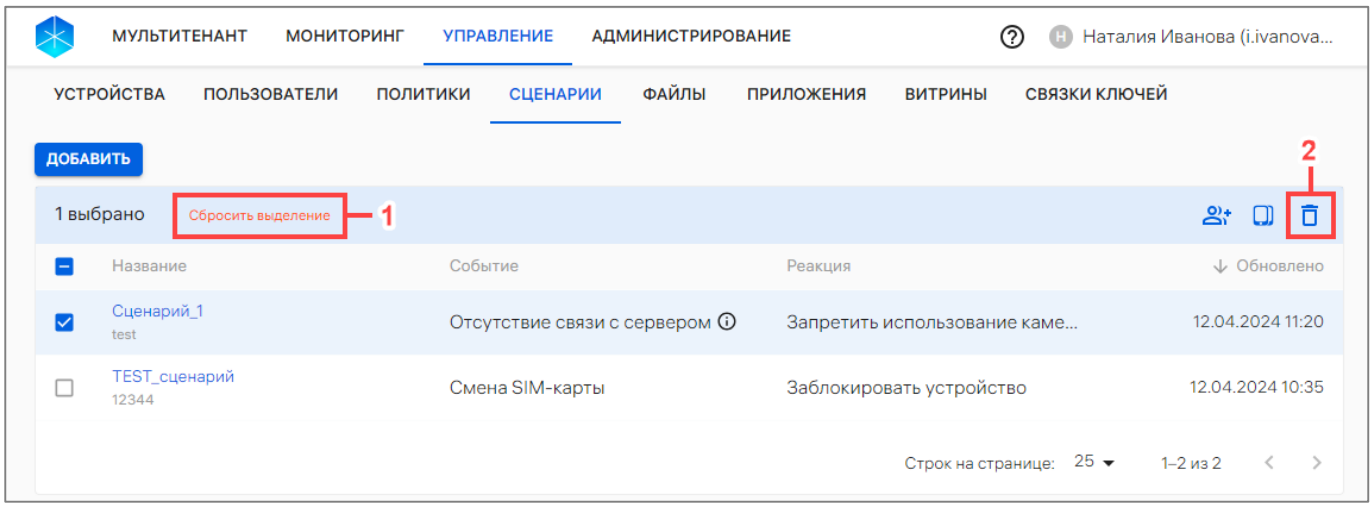

Рисунок 171

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 172);

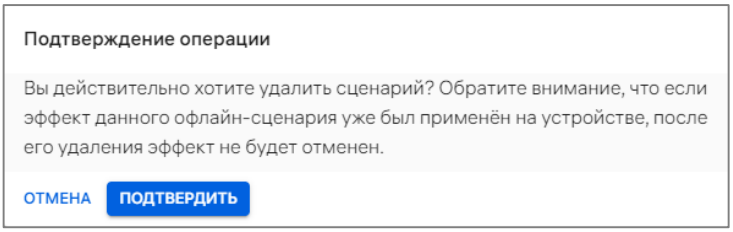

Рисунок 172

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 173);

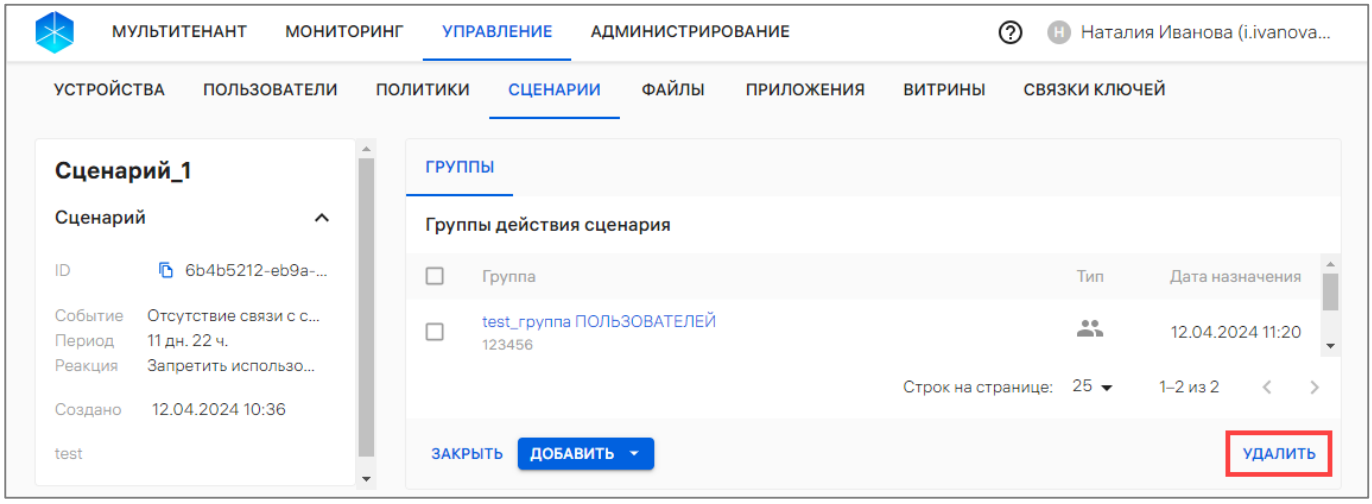

Рисунок 173

– в отобразившемся окне подтвердить либо отменить действия (см. Рисунок 172).

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»

2.6.1. Добавление файла (скрипта)

Для добавления файла (скрипта) на устройство необходимо добавить его в ПУ, выполнив следующие действия:

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

– нажать кнопку «Добавить»;

– в открывшемся окне (Рисунок 174) 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;

– подтвердить либо отменить действия.

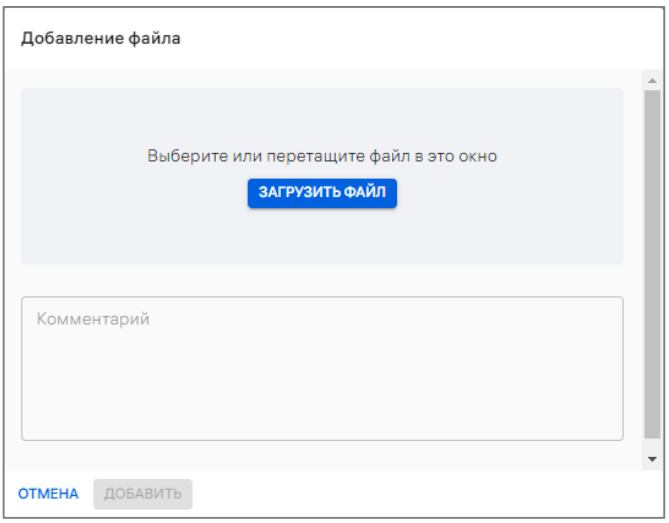

Рисунок 174

При успешном добавлении файл (скрипт) будет добавлен в ПУ и отобразится в списке файлов.

2.6.2. 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. 2.4.1.31) и «Скрипты/Выполнение на устройстве» (пп. 2.4.1.32) или отредактировать существующую политику, добавив в нее новое правило по доставке файлов или выполнения 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).

2.6.3. Удаление файла (скрипта)

Для удаления файла (скрипта) необходимо выполнить следующие действия:

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

– выбрать файл, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение» (Рисунок 175 [1]).

ПРИМЕЧАНИЕ. Доступно удаление только одного файла;

– в списке быстрых действий выбрать значок «Удалить файл» (Рисунок 175 [2]);

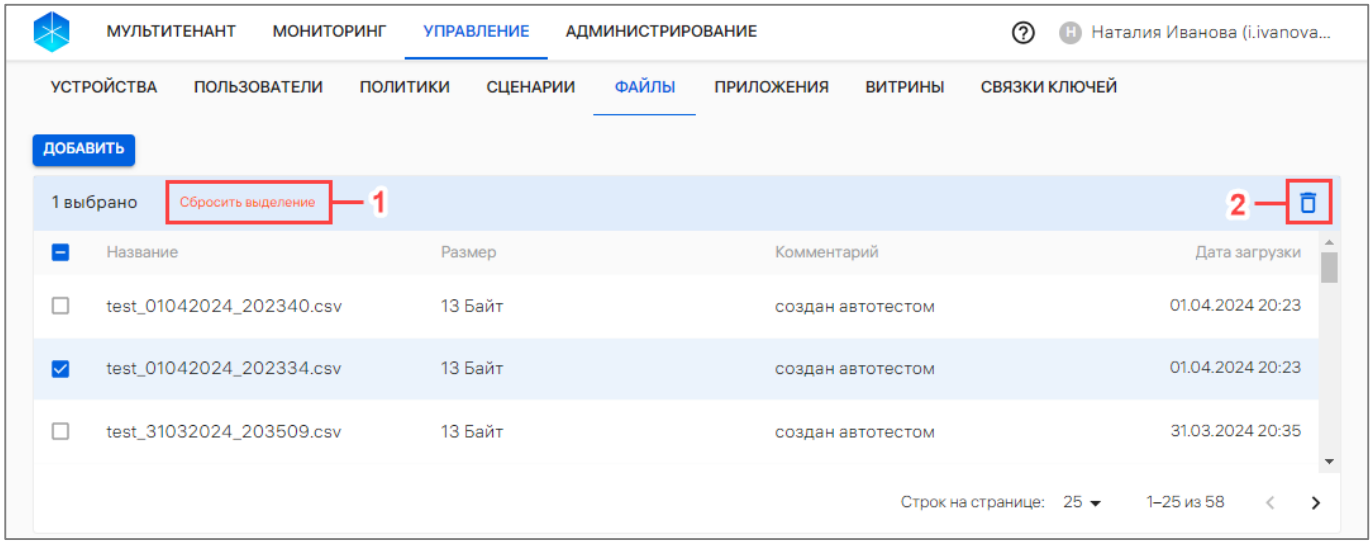

Рисунок 175

– в отобразившемся окне (Рисунок 176) подтвердить либо отменить действия.

ПРИМЕЧАНИЕ. Если файл применен в политике «Файлы/Доставка на устройство», отобразится предупреждающее сообщение о том, что удалить файла невозможно. Для удаления файла необходимо исключить файл из правила политики и выполнить шаги, указанные выше.

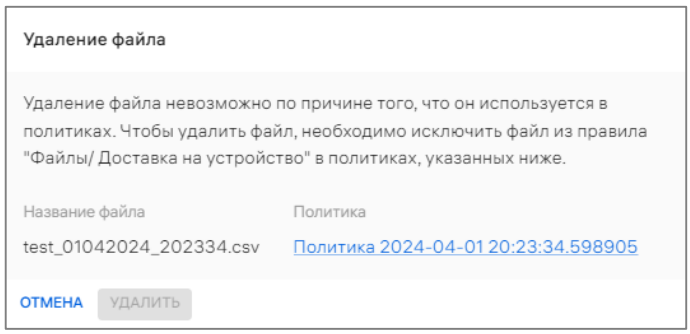

Рисунок 176

В результате файл будет успешно удален.

3. РАБОТА В РАЗДЕЛЕ «МОНИТОРИНГ» КОНСОЛИ АДМИНИСТРАТОРА ПУ

3.1. Подраздел «Индикаторы»

Подраздел «Индикаторы» Консоли администратора ПУ предназначен для мониторинга показателей устройств и контроля их отклонений.

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Мониторинг», подраздел «Индикаторы». В результате отобразится информация об устройствах в виде диаграмм и пояснений к ним, а также фоновый процесс импорта устройств, пользователей и их групп в следующих окнах (Рисунок 177):

– «Подключение устройств»;
– «Соответствие политике»;
– «Активация устройств»;
– «Процессы».

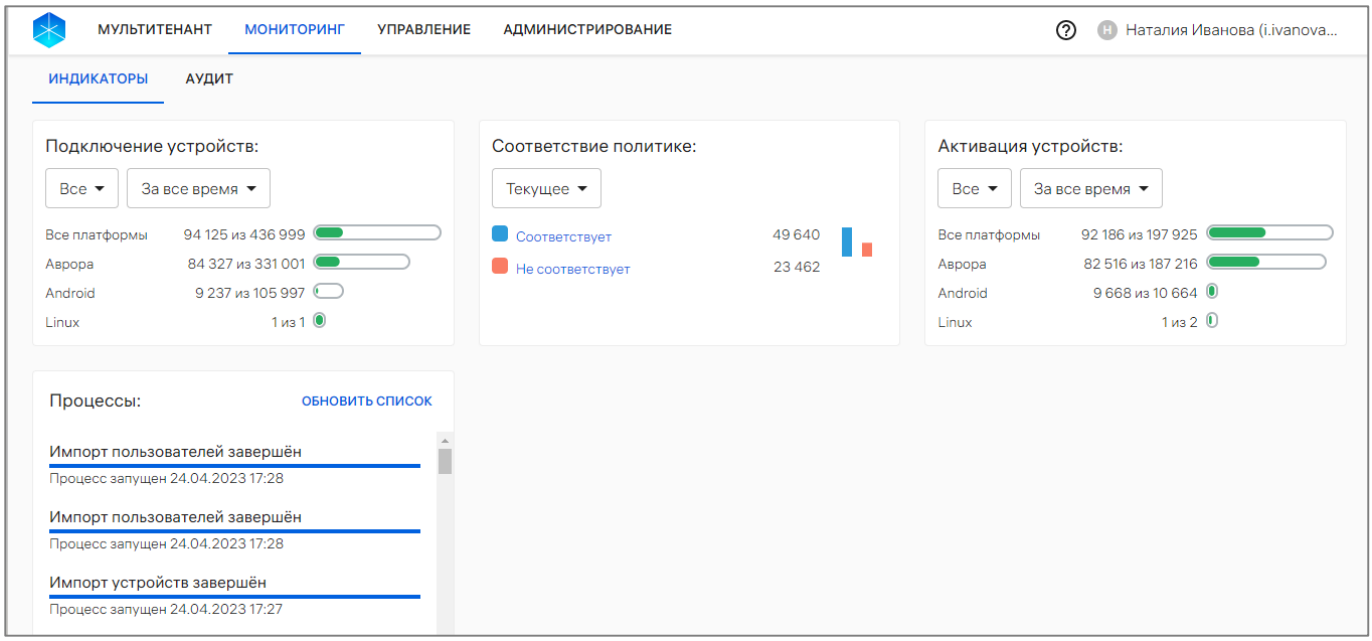

Рисунок 177

В подразделе «Индикаторы» предусмотрена возможность выбрать период отображения данных из раскрывающегося списка (Рисунок 178):

– «За все время» (недоступно для части «Соответствие политике»);
– «Текущее» (недоступно для части «Подключение устройств» и «Активация устройств»);
– «За сутки»;
– «За неделю»;
– «За месяц».

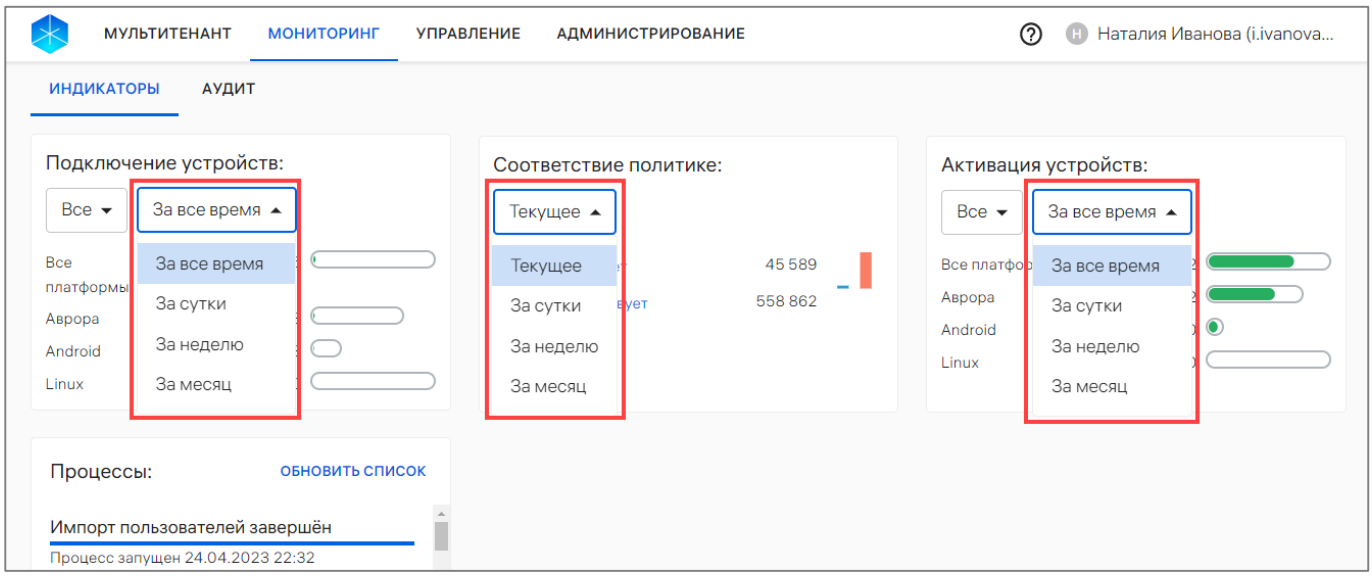

Рисунок 178

Также имеется возможность просмотра подключенных и активированных устройств для определенной платформы в количественном виде и в виде диаграмм. Для этого следует выбрать необходимую платформу устройств либо все платформы из раскрывающегося списка в следующих окнах (Рисунок 179):

– «Подключение устройств»:
  - Все платформы (количество всех подключившихся устройств);
  - Аврора (количество подключившихся устройств, функционирующих под управлением ОС Аврора);
  - Android (количество подключившихся устройств, функционирующих под управлением ОС Android);
  - Linux (количество подключившихся устройств, функционирующих под управлением ОС Linux);

– «Активация устройств»:
  - Все платформы (количество всех активированных устройств);
  - Аврора (количество активированных устройств, функционирующих под управлением ОС Аврора);
  - Android (количество активированных устройств, функционирующих под управлением ОС Android);
  - Linux (количество подключившихся устройств, функционирующих под управлением ОС Linux).

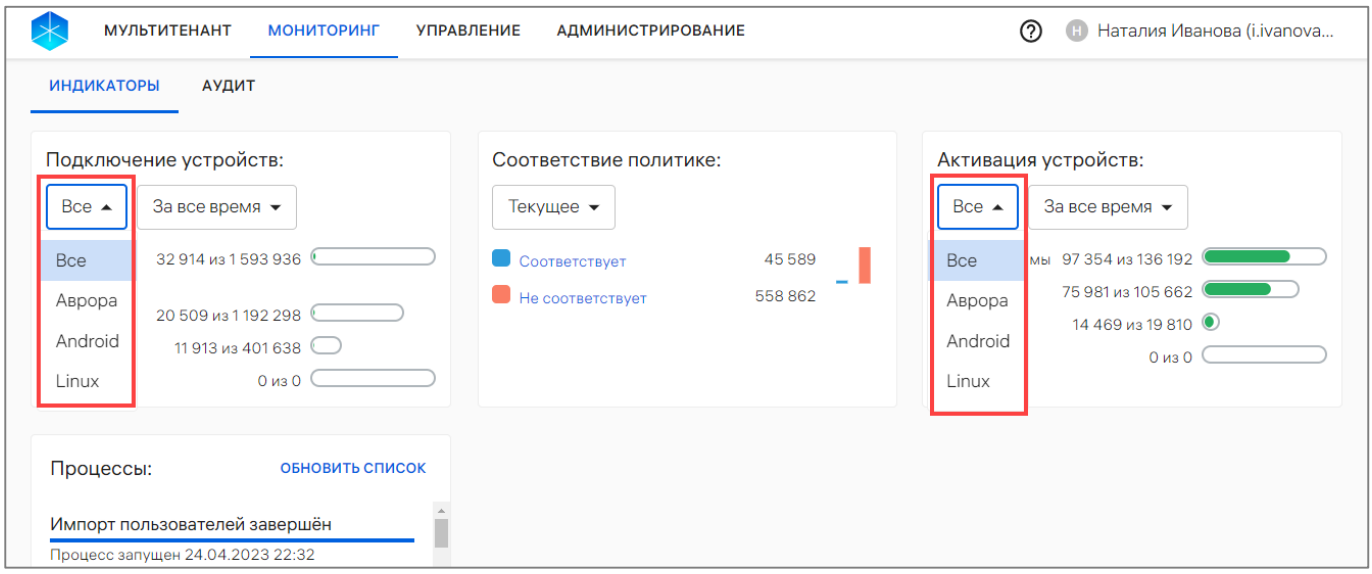

Рисунок 179

В результате отобразится диаграмма, а также количество подключенных или активированных и находящихся в процессе активации устройств для выбранной платформы (Рисунок 180).

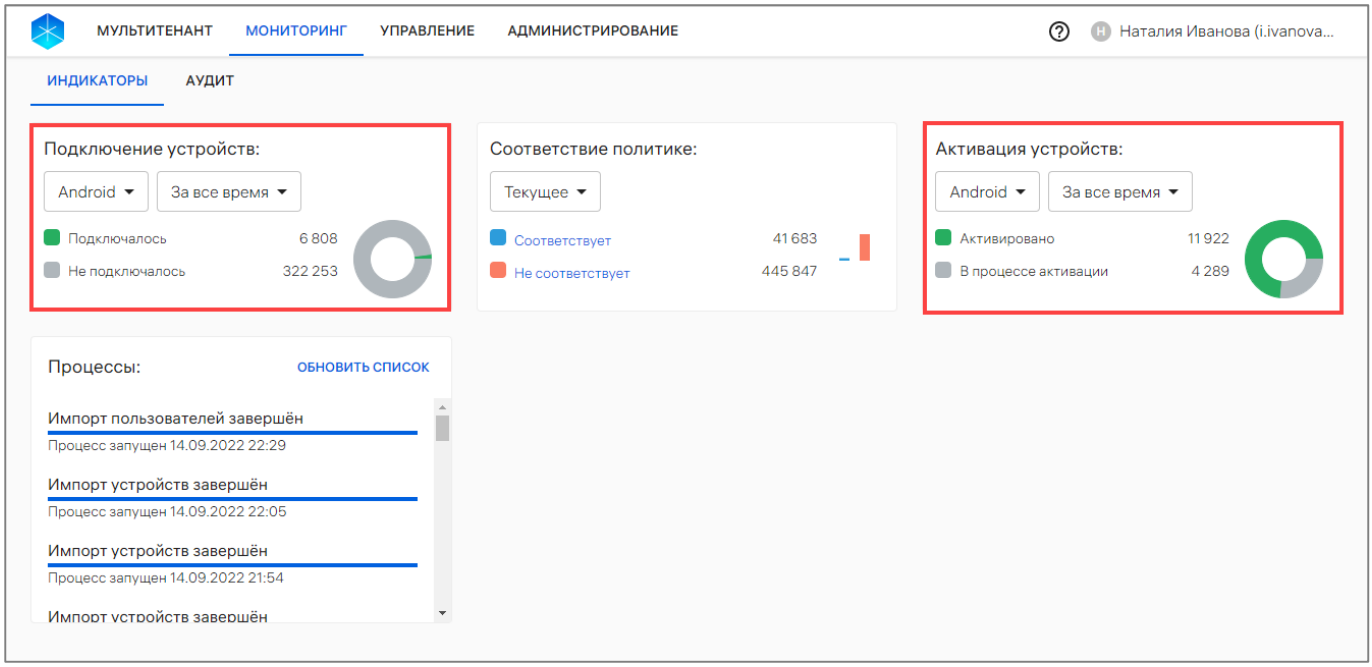

Рисунок 180

В окне «Соответствие политике» отображается информация по следующим показателям:

– «Соответствует» - количество устройств, соответствующих политикам;
– «Не соответствует» - количество устройств, не соответствующих политикам.

Указанные показатели выделены цветом и представляют собой активные ссылки. При переходе по ссылке (Рисунок 160 [1]):

– «Соответствует» будет отображен список устройств, отфильтрованный по статусу политик «Соответствует»;

– «Не соответствует» 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.

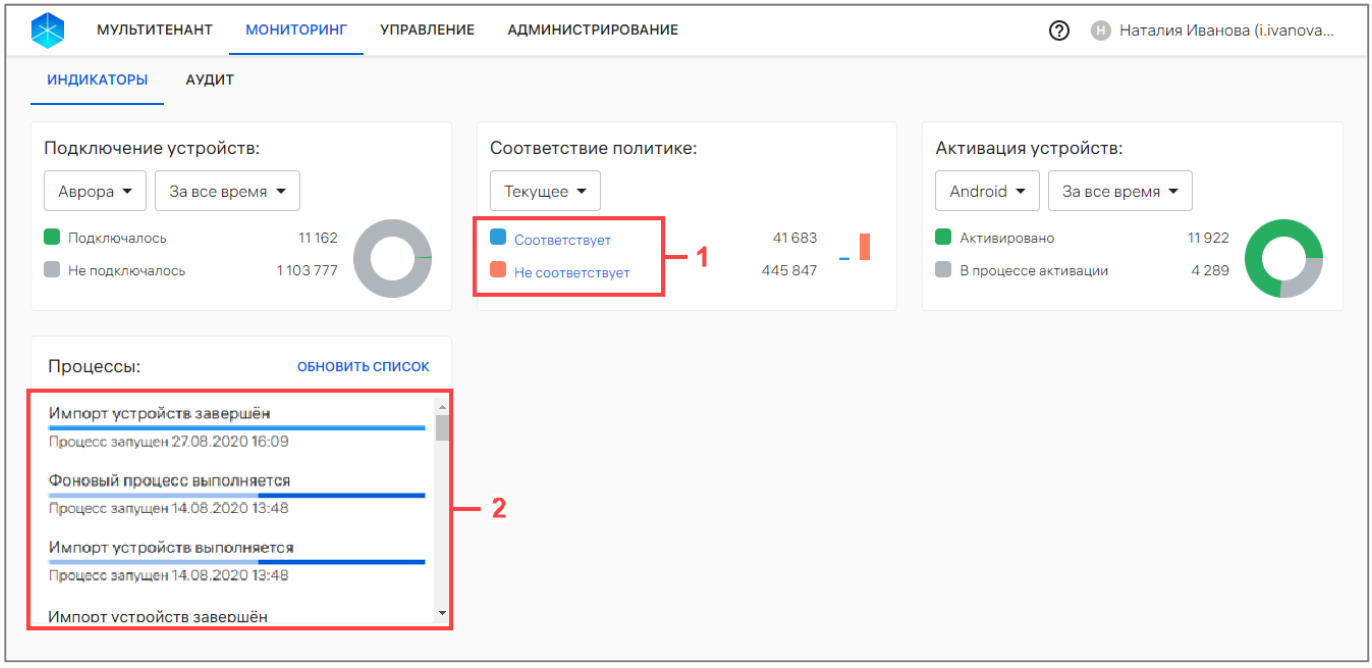

Рисунок 181

В окне «Процессы» отображаются завершенные и текущие процессы импорта устройств, пользователей и их групп из CSV-файла (Рисунок 181 [2]). 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 – отобразится окно с информацией о состоянии импорта, если он еще выполняется, или с результатом импорта, если он завершен (даже с ошибкой) (см. Рисунок 55, Рисунок 56).

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 182 [1]);

– добавления и просмотра категорий пользовательских сертификатов (п. 4.1.2, Рисунок 182 [2]);

– управления отображением архивных устройств (п. 4.1.3, Рисунок 182 [3]);

– просмотра информации о (п. 4.1.4, Рисунок 182 [4]):

- Сервере приложений (также представлена возможность включения/отключения витрин с приложением);
- Обновлении ОС;
- Сервере LDAP (также представлена возможность добавление интеграции с сервером LDAP и настройки синхронизации данных с ППО);
- Сервисе уведомлений Аврора (СУА) (также представлена возможность изменения настроек ПСУ);
- Центрах сертификации;

– доступа к ссылке на приложение «Аврора Центр» для ОС Android (п. 4.1.5, Рисунок 182 [5]);

– просмотра и добавления территории на карте (п. 4.1.6, Рисунок 182 [6]).

Для перехода в подраздел необходимо в верхней панели перейти в раздел «Администрирование» и выбрать подраздел «Настройки».

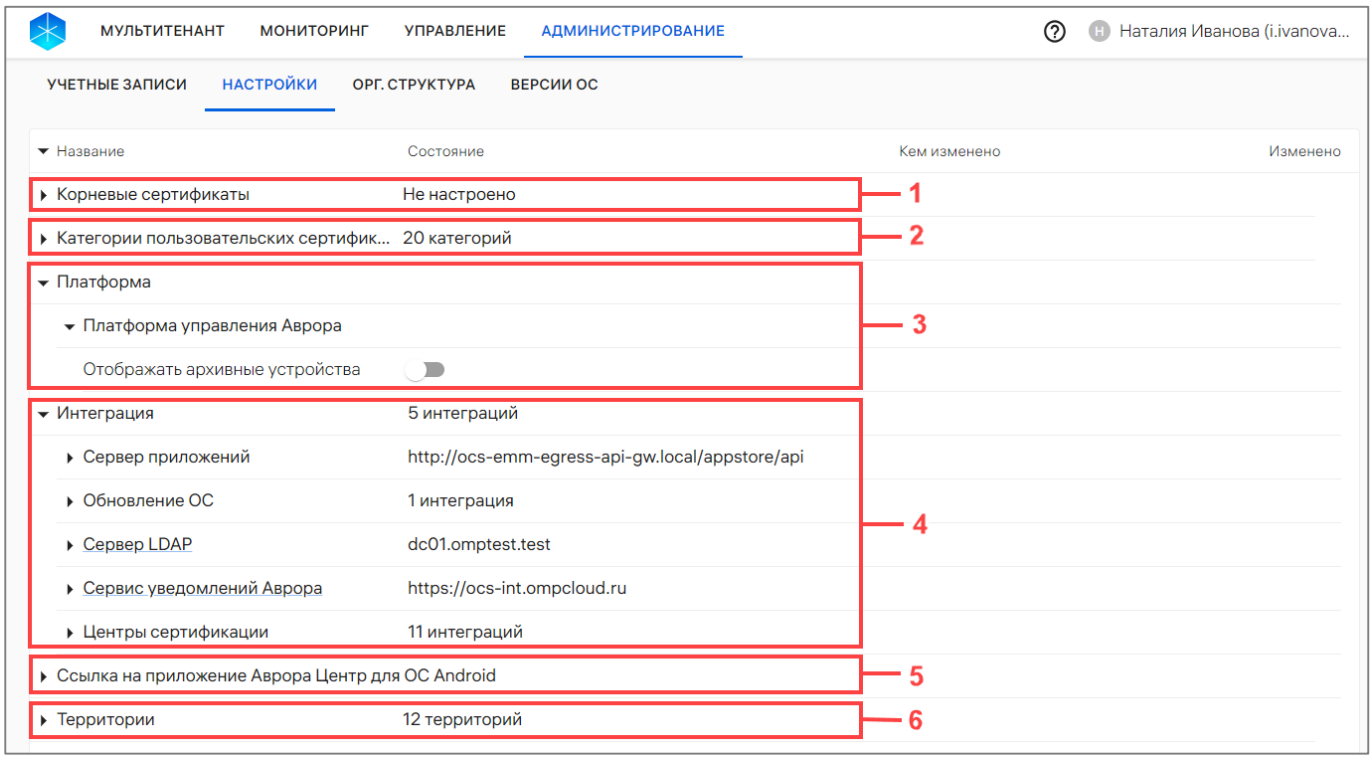

Рисунок 182

4.1.1. Доверенные сертификаты

В раскрывающейся строке «Корневые сертификаты» при нажатии на значок (см. Рисунок 182 [1]) отображается список доверенных сертификатов, добавленных в ПУ (Рисунок 183 [2]).

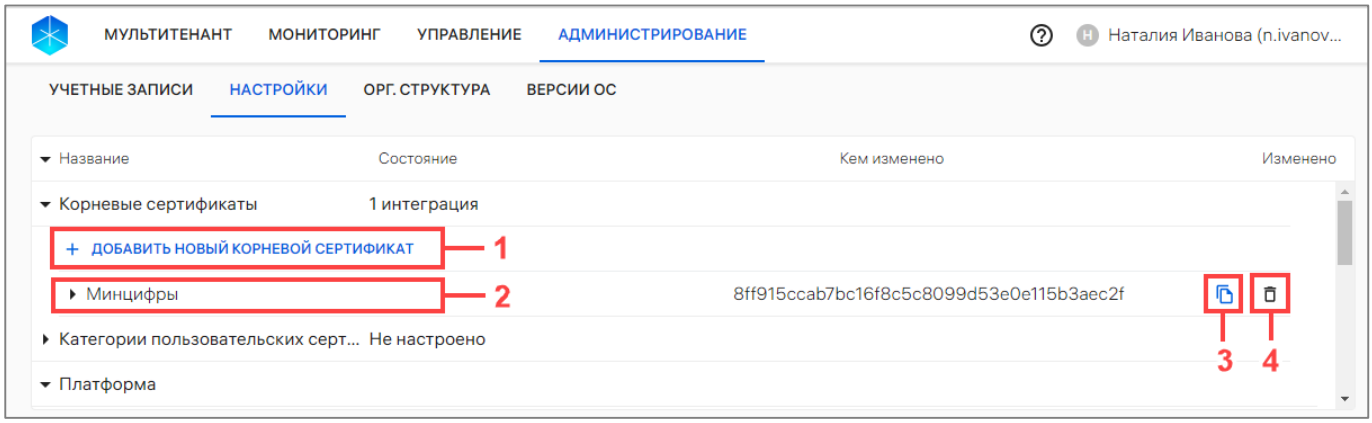

Рисунок 183

Для просмотра информации о доверенном сертификате необходимо в раскрывающейся строке названия сертификата нажать значок , в результате чего отобразится следующая информация (Рисунок 184):

– название удостоверяющего центра;
– дата выпуска сертификата;
– срок действия сертификата;
– используется ли сертификат при активации и самостоятельной регистрации устройства.

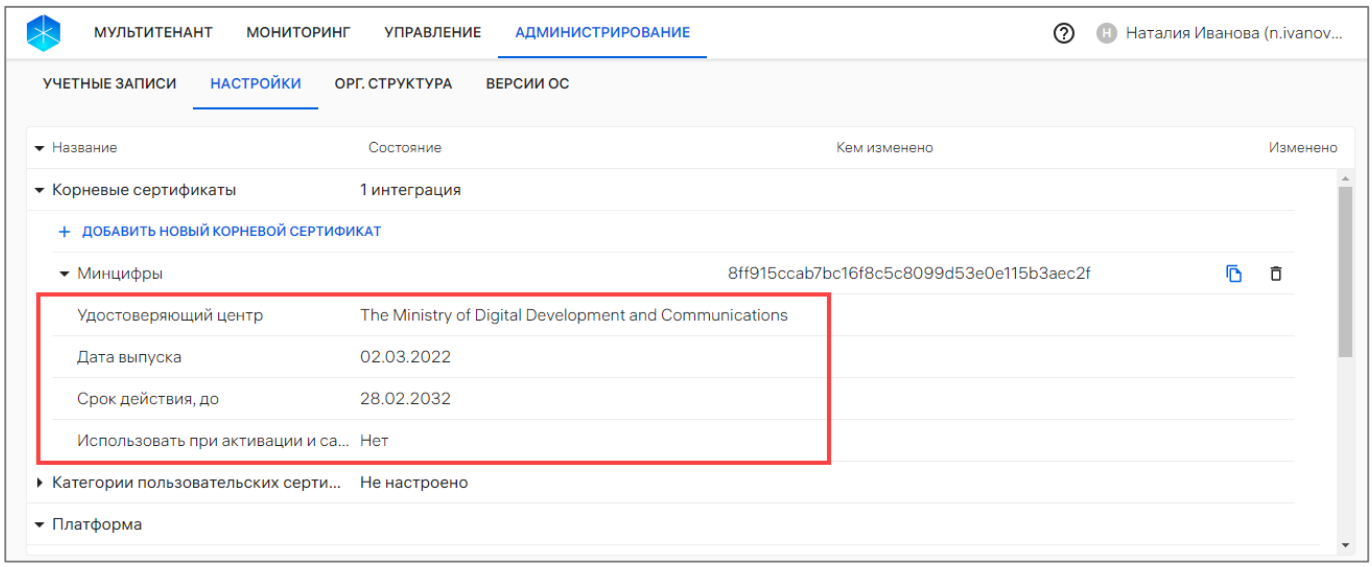

Рисунок 184

Для добавления корневых сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить новый корневой сертификат» (см. Рисунок 183 [1]);

– в открывшемся окне в поле «Имя корневого сертификата» ввести название сертификата (Рисунок 185 [1]). Максимальная длина - 32 символа;

– перевести переключатель «Использовать при активации и саморегистрации» в положение «Включено» (Рисунок 185 [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 185 [3]) для последующего выбора файла для загрузки. Допустимые форматы: `.crt`, `.cer`, `.pem`;

– подтвердить либо отменить действия (Рисунок 185 [4]).

При успешном добавлении сертификат отобразится в списке доверенных сертификатов.

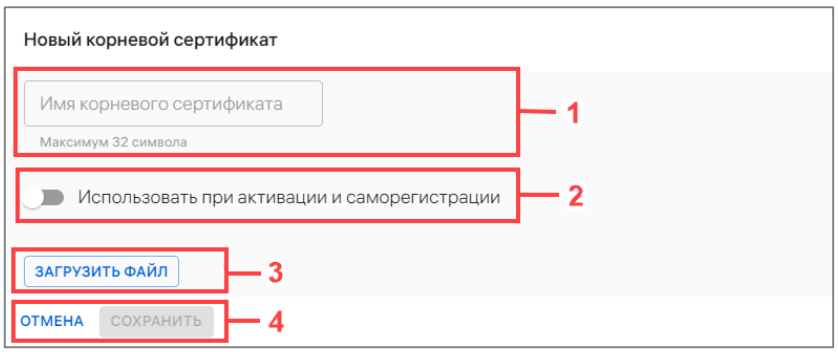

Рисунок 185

При необходимости цифровой отпечаток (Fingerprint) сертификата возможно скопировать в буфер обмена нажатием значка «Копировать в буфер обмена» (см. Рисунок 183 [3]) в строке с сертификатом.

Для удаления корневых сертификатов необходимо нажать значок «Удалить сертификат» в строке сертификатов (см. Рисунок 183 [4]) и в открывшемся окне подтвердить либо отменить действия.

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. 2.4.1.30);

– «Конфигурация WLAN/Подключения к сети WLAN» (пп. 2.4.1.18).

Список созданных категорий возможно посмотреть в раскрывающейся строке «Категории пользовательских сертификатов» при нажатии значка (см. Рисунок 182 [2]).

Для добавления категории пользовательских сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить категорию» (Рисунок 186);

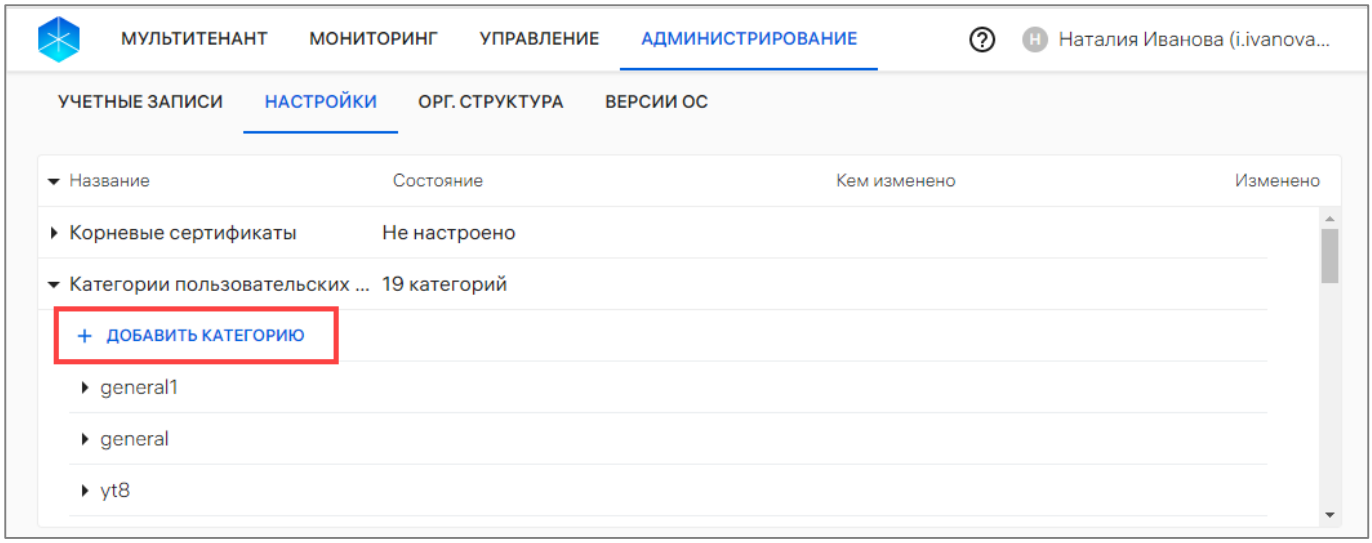

Рисунок 186

– в открывшемся окне (Рисунок 187) заполнить поля, приведенные в таблице (Таблица 41);

– сохранить изменения либо отменить действия.

При успешном сохранении категория пользовательских сертификатов будет добавлена.

ВНИМАНИЕ! Удаление и редактирование категории сертификата недоступно. При необходимости требуется создать новую категорию пользовательских сертификатов.

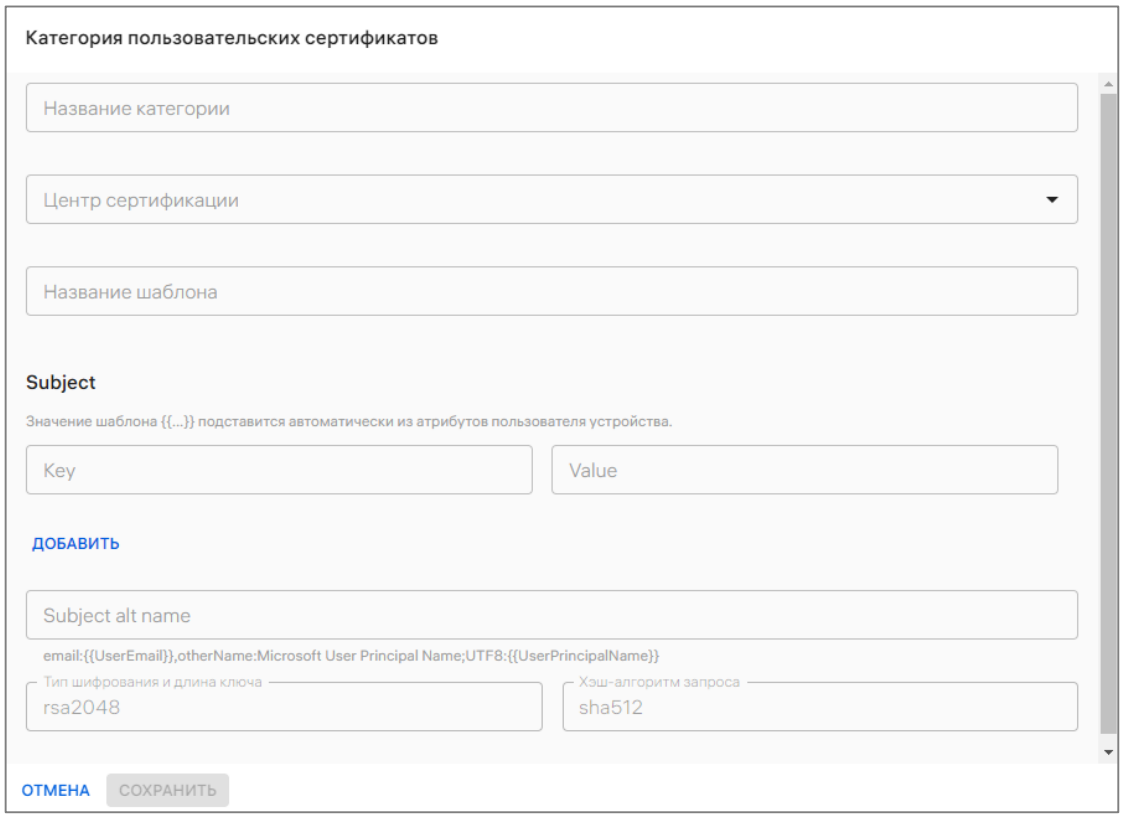

Рисунок 187

Таблица 41

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. 4.1.4). Поле обязательно для заполнения
Название шаблона	Ввод значения с клавиатуры. Может содержать 255 символов. Поле обязательно для заполнения

Параметр		Описание
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 обратится 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»
Subject alt name		При необходимости доступен ввод дополнительных имен субъекта для сертификата. Каждое имя субъекта должно состоять из набора параметров – названия параметра (`key`) и его значения (`value`). Может содержать 1000 символов. Доступен ввод 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);

Параметр	Описание
	– `{{sAMAccountName}}` – логин (значение параметра `sAMAccountName` из LDAP–данных о пользователе); – `{{distinguishedName}}` – значение параметра `distinguishedName` из LDAP–данных о пользователе. **ВНИМАНИЕ!** Ввод других динамических переменных недоступен. Пример заполнения Subject alt name: `email:{{UserEmail}},otherName:Microsoft User Principal Name;UTF8:{{UserPrincipalName}}`

4.1.3. Архивные устройства

В раскрывающейся строке «Платформа» для активации отображения архивных устройств (см. Рисунок 182 [3]) необходимо активировать переключатель . В результате в подразделе «Устройства» раздела «Управление» в списке устройств будут отображаться архивные устройства (Рисунок 188).

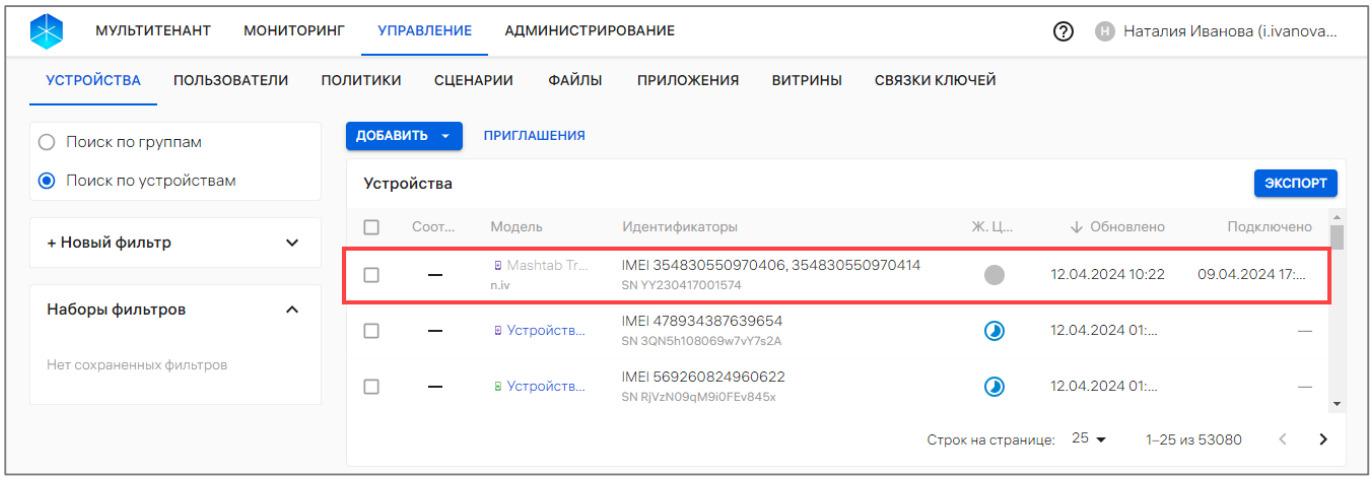

Рисунок 188

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 189 [1]) и список опубликованных витрин на Сервере приложений ПМ (Рисунок 189 [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.

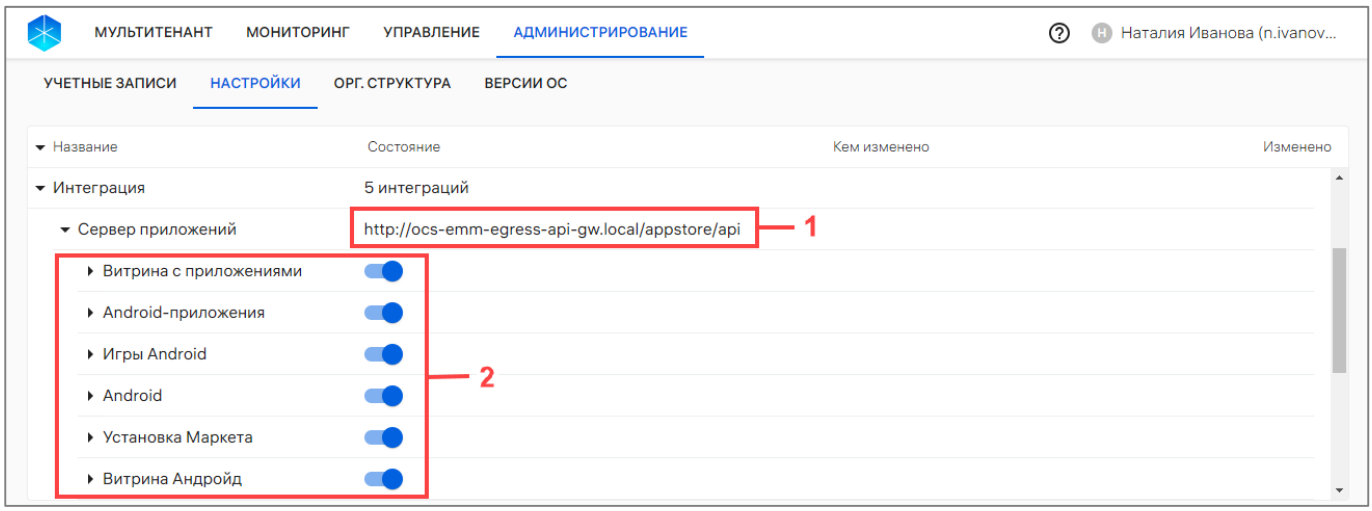

Рисунок 189

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».

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 просмотреть 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 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:

✓ Поддержка интеграции с другими LDAP-серверами не гарантируется;

✓ Предусматривается возможность добавления интеграции с LDAP-сервером для каждого тенанта;

✓ ПУ поддерживает синхронизацию с LDAP-серверами, в которых 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 ADCS.

Для добавления интеграции ПУ с LDAP-сервером необходимо выполнить следующие действия:

– во вложенном списке «Интеграция» нажать «Сервер LDAP» или «Настроить» (Рисунок 190);

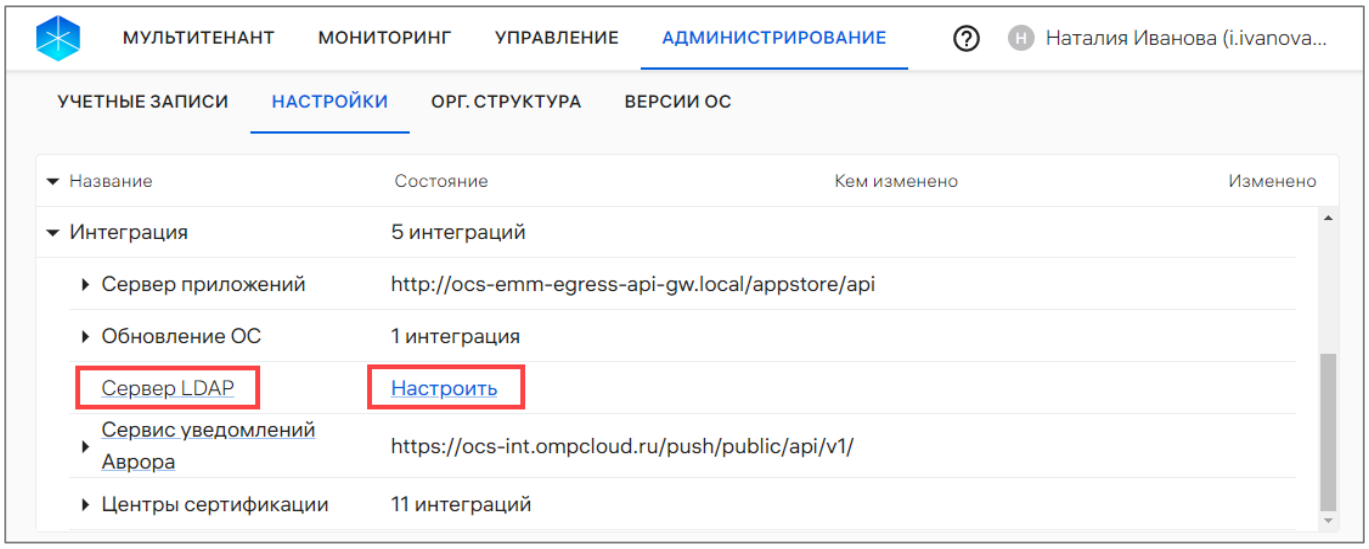

Рисунок 190

– задать настройки для подключения к LDAP-серверу (Рисунок 191 [1]) согласно таблице (Таблица 42);

Таблица 42

Поле	Описание
Использовать безопасное соединение (TLS/SSL)	Если необходимо использовать защищенное подключение к LDAP-серверу (с помощью SSL версии протокола LDAP – LDAPS), следует установить галочку в чекбоксе. По умолчанию флажок не установлен (используется версия протокола без SSL - LDAP
Адрес сервера	Ввести адрес LDAP-сервера

Поле	Описание
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

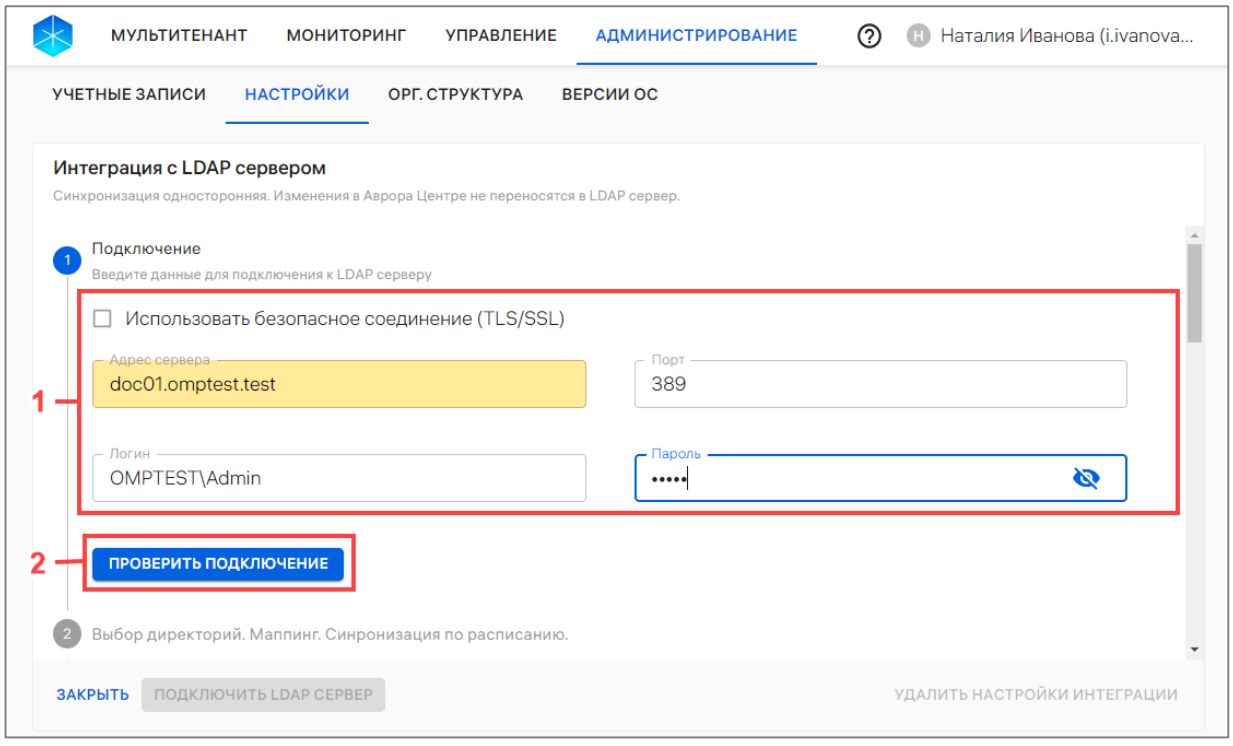

Рисунок 191

– нажать кнопку «Проверить подключение», чтобы проверить работоспособность подключения к LDAP-серверу с заданными настройками (Рисунок 191 [2]).

В случае успешной проверки отобразится сообщение «Подключение доступно» (Рисунок 192).

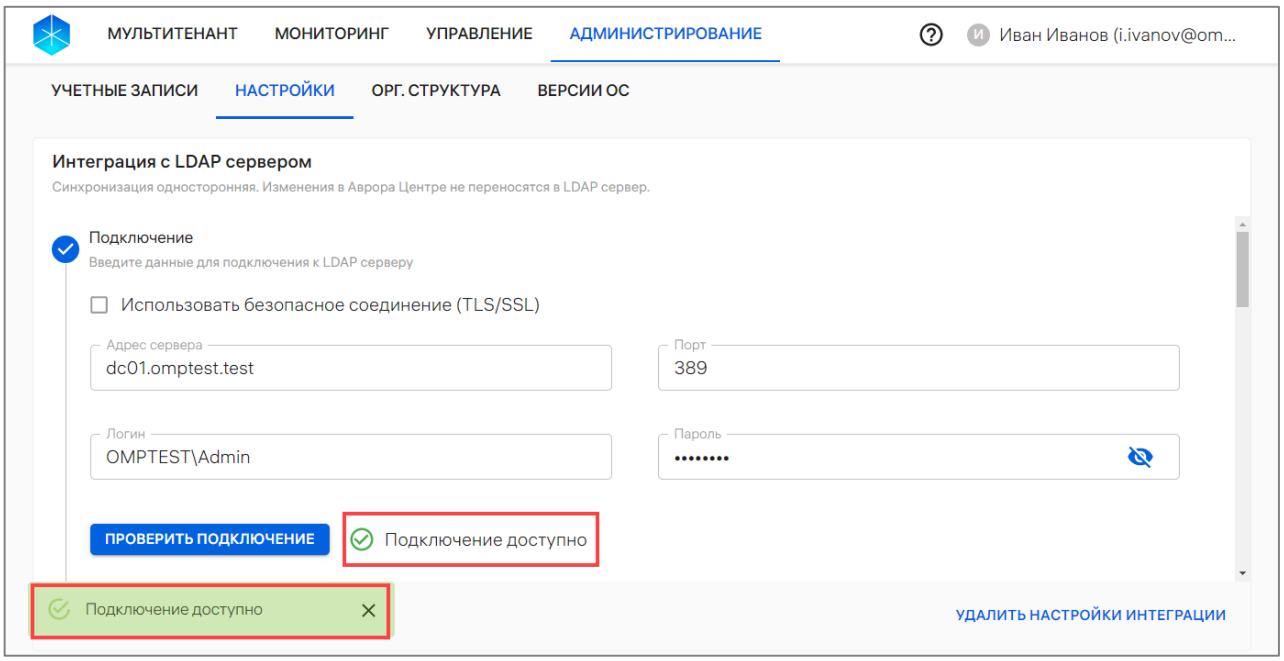

Рисунок 192

В случае неудачного завершения проверки отобразится сообщение об ошибке (Рисунок 193[1]), которую необходимо устранить и повторить проверку или обратиться к системному администратору/администратору LDAP.

Для ознакомления с полным текстом ошибки следует нажать «Подробнее» (Рисунок 193 [2]).

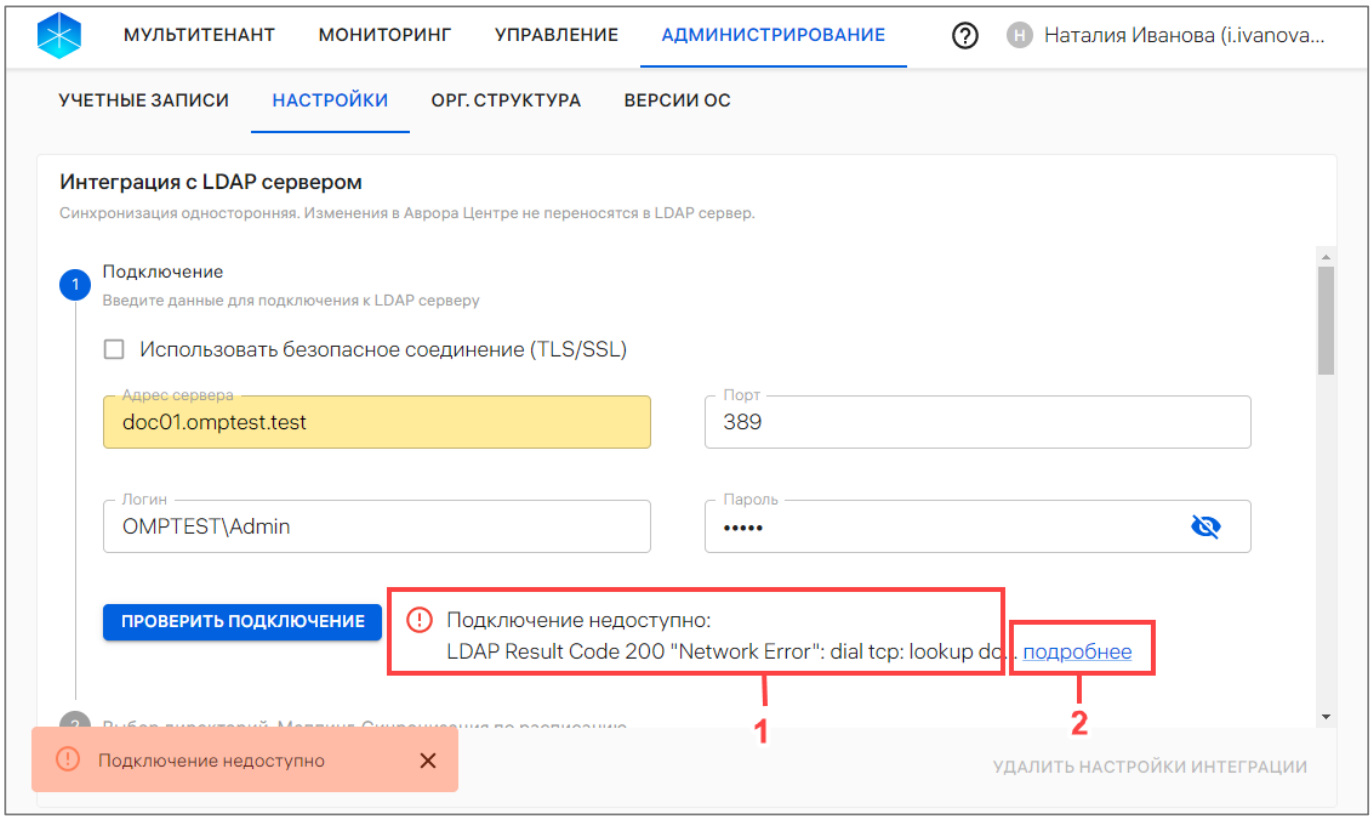

Рисунок 193

Задать область поиска в LDAP-сервере можно согласно таблице (Таблица 43), данные из которой будут синхронизироваться с ППО (Рисунок 194 [1]).

Таблица 43

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»

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.

При использовании фильтров необходимо выполнять следующие рекомендации:

1) Если для выбора необходимых пользователей и/или групп из юнита требуется задать несколько фильтров, то следует добавить еще 1 директорию (как указано ниже), затем в каждой строке ввести одинаковый «Base DN» и задать нужный фильтр;

2) Если требуется синхронизировать в ПУ уволенных сотрудников, то следует указать организационный юнит, в котором они хранятся, или задать фильтры для загрузки таких пользователей;

3) Если не требуется синхронизировать в ПУ уволенных сотрудников, то 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)`.

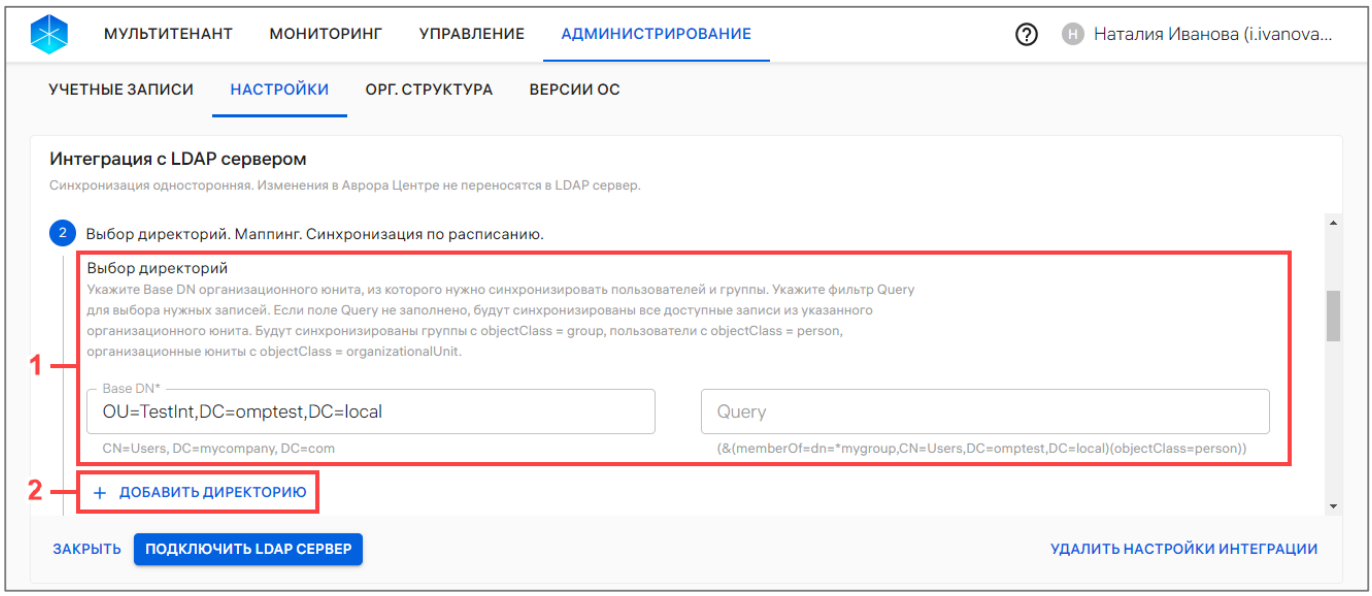

Рисунок 194

При необходимости добавить еще 1 директорию для синхронизации следует нажать «Добавить директорию» (см. Рисунок 194 [2]) и заполнить для нее поля «Base DN» и «Query» согласно таблице (см. Таблица 43).

По умолчанию в блоке «Маппинг» 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 195), приведенных в таблице (Таблица 44).

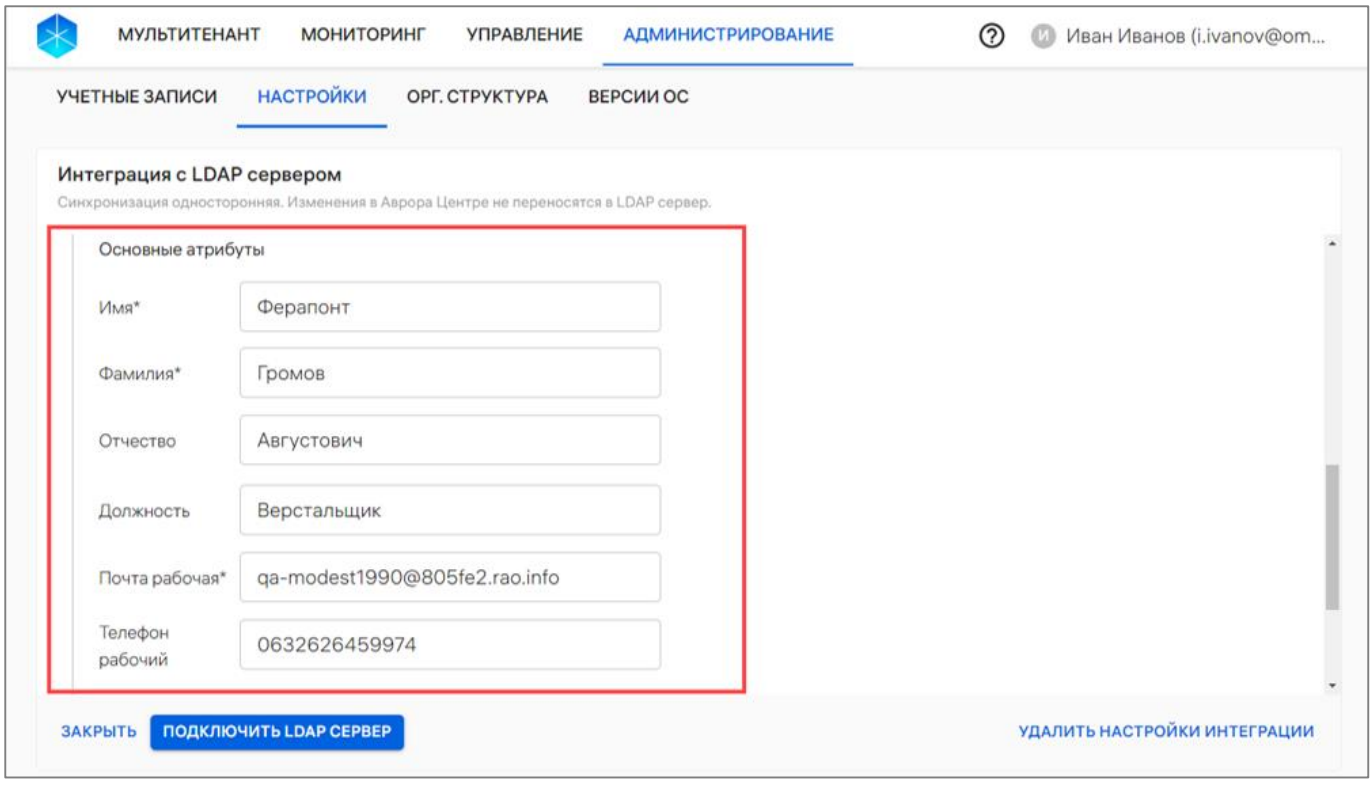

Рисунок 195

Таблица 44

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 45).

Таблица 45

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; a-z; А-Я; A-Z; -; пробел	Поле обязательно для заполнения
Фамилия	Фамилия пользователя устройства. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	Поле обязательно для заполнения
Отчество	Отчество пользователя устройства. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	Поле не является обязательным для заполнения
Должность	Должность пользователя устройства. Формат: от 2 до 256 символов. Символы: а-я; a-z; А-Я; A-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 196 [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.

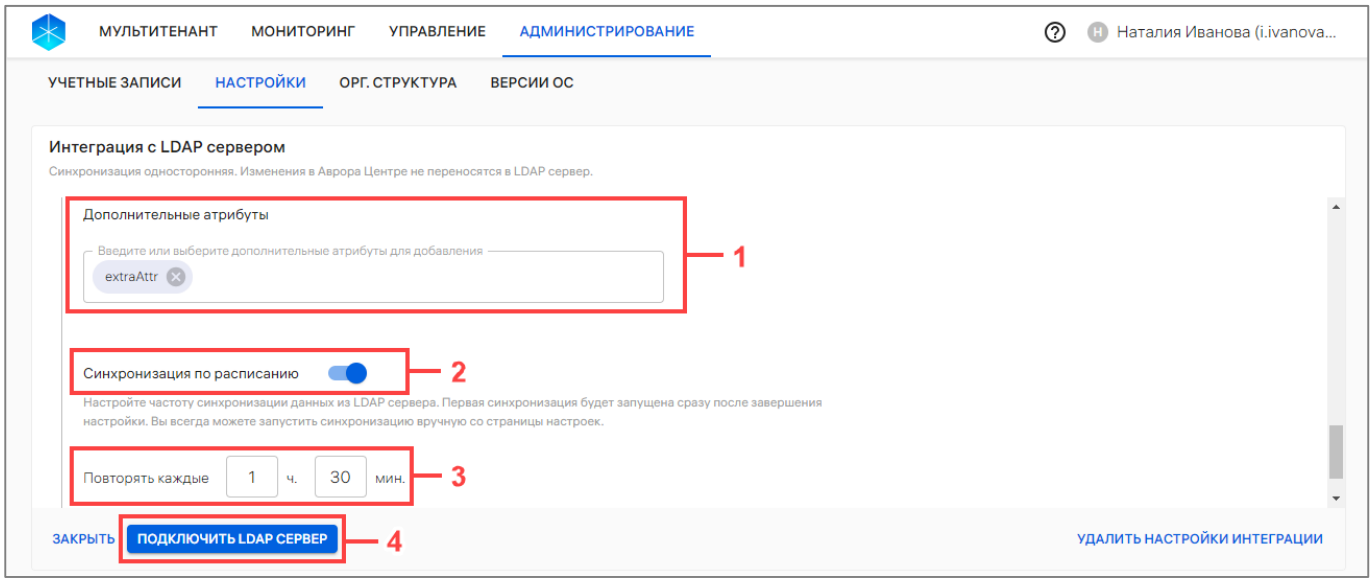

Рисунок 196

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» (Рисунок 196 [2]);

– изменить частоту синхронизации, то следует ввести нужный временной интервал в поле «Повторять каждые» (Рисунок 196 [3]).

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных.

Далее нажать «Подключить LDAP-сервер» (Рисунок 196 [4]).

В результате будет добавлена интеграция ПУ с LDAP-сервером и запущена первая синхронизация данных.

Для просмотра даты начала синхронизации и ее статуса необходимо нажать значок в раскрывающейся строке «Сервер LDAP» (Рисунок 197).

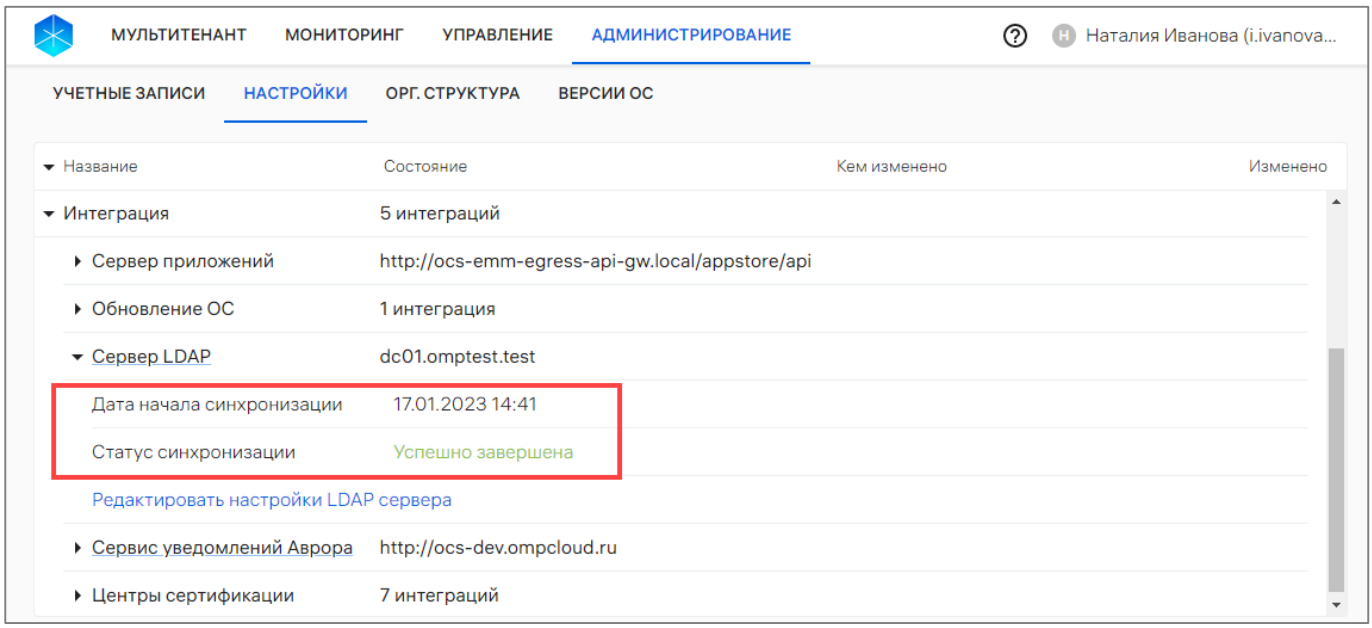

Рисунок 197

В случае ошибки синхронизации данных (Рисунок 198 [1]) для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (Рисунок 198 [2]).

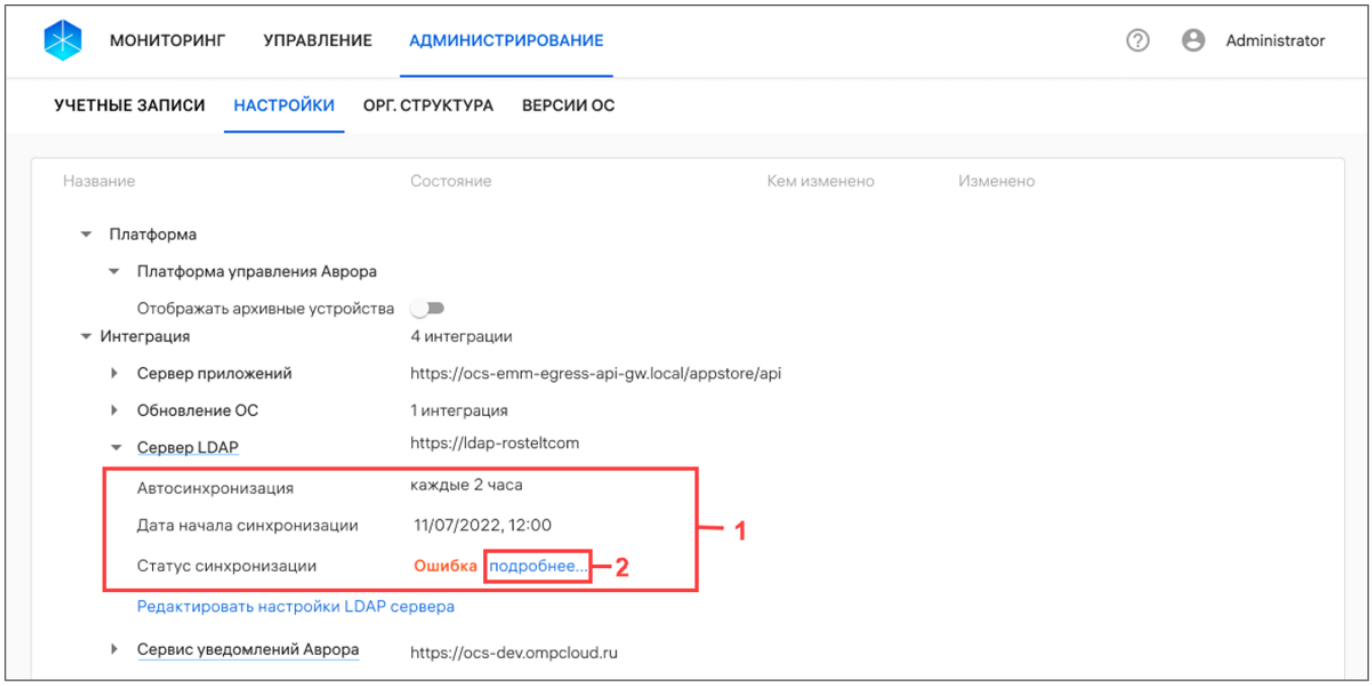

Рисунок 198

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» выбрать «Сервер LDAP» (Рисунок 199 [1]) или развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера» (Рисунок 199 [2]);

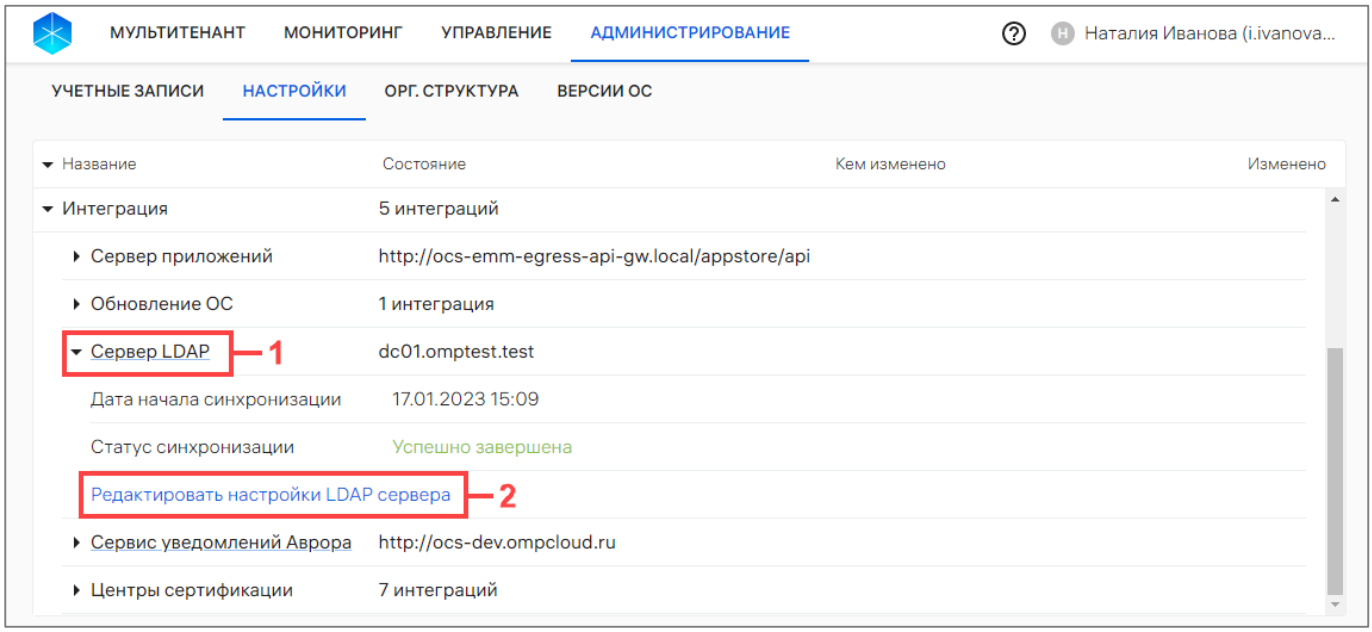

Рисунок 199

– при необходимости изменить настройки для подключения к LDAP-серверу, параметры маппинга данных и расписания синхронизации данных с ППО в соответствии с пп. 4.1.4.3.1.

В результате настройки интеграции ПУ с LDAP-сервером будут изменены.

4.1.4.3.3. Удаление интеграции с LDAP-сервером

При необходимости возможно удалить интеграцию ПУ с LDAP-сервером. В этом случае синхронизировать пользователей и группы с ППО будет возможно только после добавления новой интеграции с LDAP-сервером.

Для удаления интеграции с LDAP-сервером необходимо выполнить следующие действия:

– в раскрывающейся строке «Интеграция» выбрать «Сервер LDAP» (см. Рисунок 199 [1]) или развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера» (см. Рисунок 199 [2]);

– нажать кнопку «Удалить настройки интеграции» (Рисунок 200);

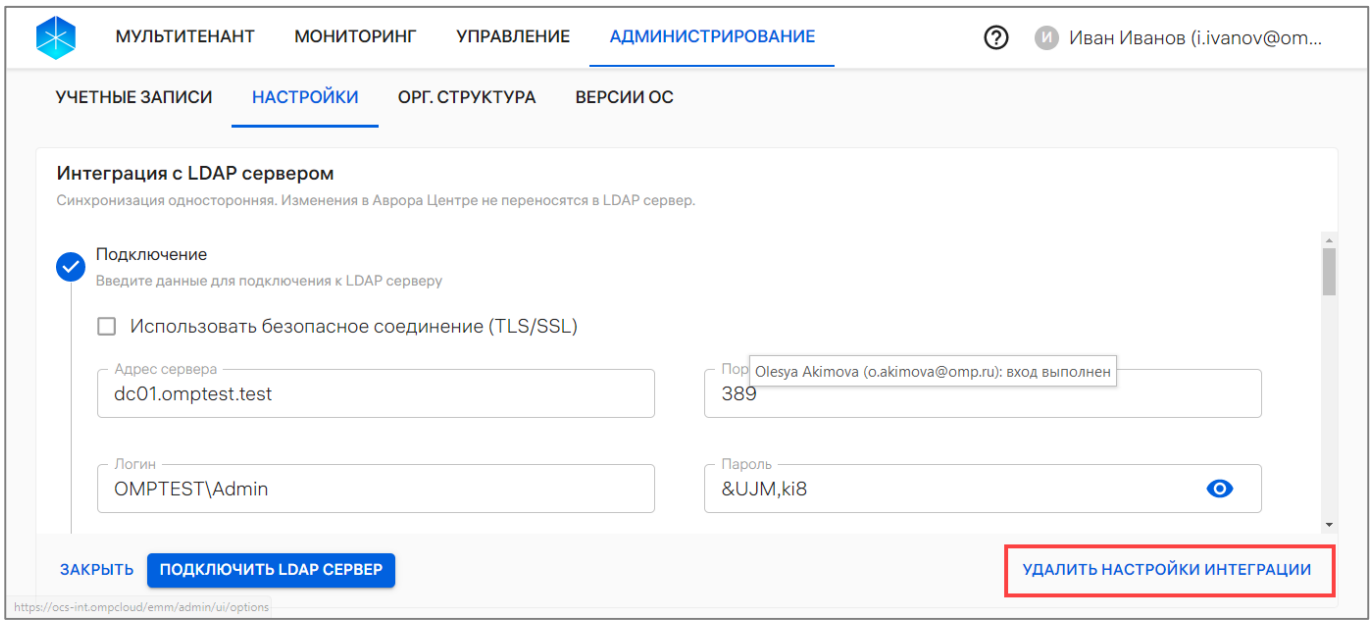

Рисунок 200

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 201).

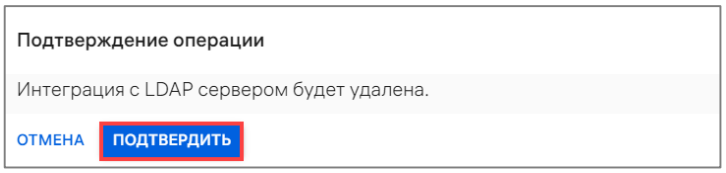

Рисунок 201

В результате подтверждения интеграция ПУ с LDAP-сервером будет удалена. Для синхронизации пользователей 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 доставки push-уведомлений на устройства приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора».

Описание работы ПСУ приведено в документе «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений».

Для просмотра настроек ПСУ необходимо нажать значок , в результате чего отобразятся параметры, приведенные в таблице (Таблица 46).

Таблица 46

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 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 202 [1]);

– нажать «Редактировать настройки Сервиса уведомлений Аврора» (Рисунок 202 [2]).

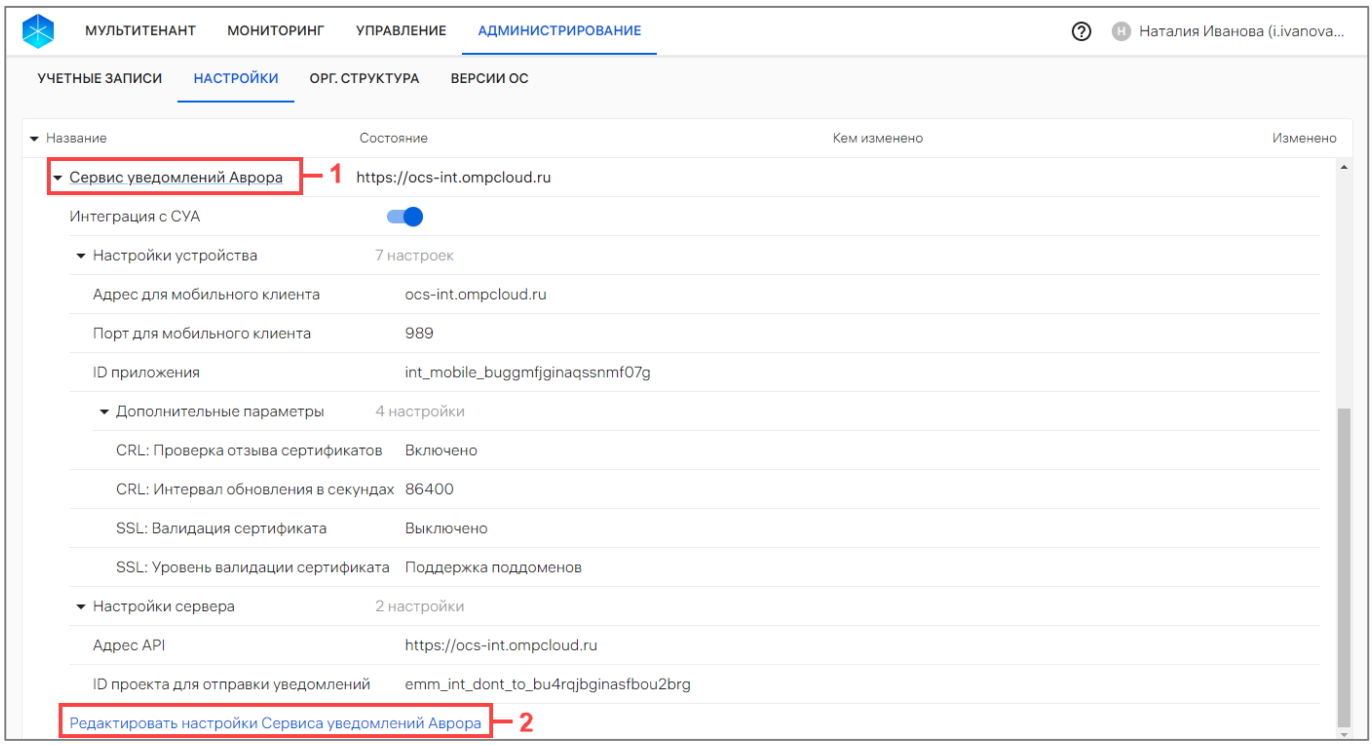

Рисунок 202

В результате выполнения одного из указанных действий будут доступны поля для редактирования настройки ПСУ одним из следующих способов (Рисунок 203):

– загрузка JSON-файлов с настройками нажатием кнопки «Загрузить файлы настроек»;

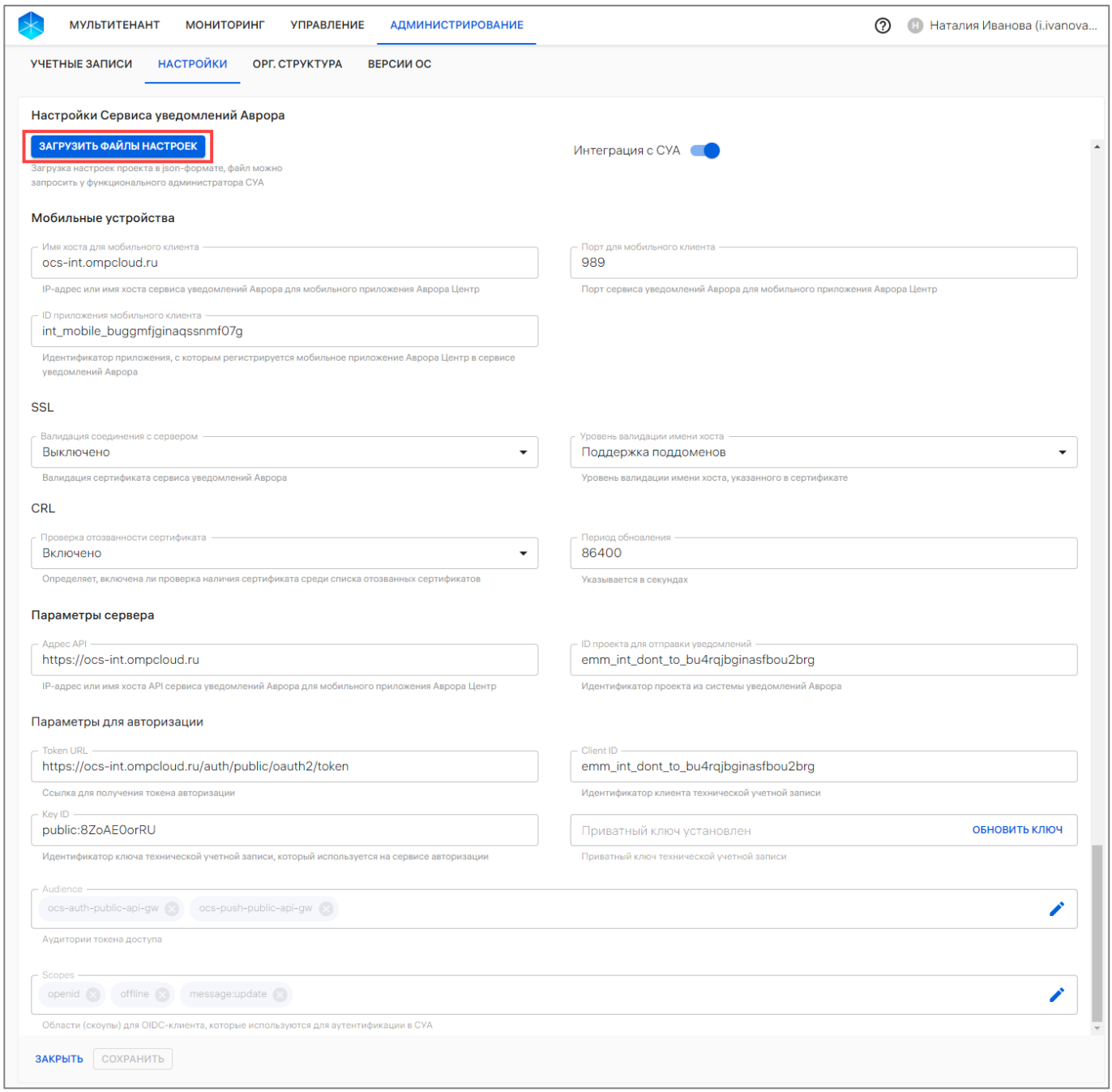

Рисунок 203

– внесение изменений вручную в соответствии с таблицей (Таблица 47).

После внесения уточнения в соответствии с таблицей (Таблица 47) необходимо подтвердить либо отменить действия.

Таблица 47

Поле	Описание
Интеграция с СУА	Данное поле предназначено для включения или выключения отправки настроек ПСУ для приложения «Аврора Центр» при помощи переключателя

Поле	Описание
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: – Выключено; – Включено
Уровень валидации имени хоста	Выбор из раскрывающегося списка уровень валидации имени хоста, указанного в ПСУ: – 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: – Выключено; – Включено
Период обновления	Ввод значения с клавиатуры временного интервала обновления списка отозванных сертификатов (в секундах)
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

Поле	Описание
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 ключиспользуется 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

4.1.4.5. Центры сертификации

В ППО доступна возможность добавить интеграцию с центром сертификации, который выпускает пользовательские сертификаты для подключения к беспроводным сетям.

ПРИМЕЧАНИЕ. ППО поддерживает интеграцию с центрами сертификации, имеющими тип сервера Microsoft Active Directory Certificate Services (AD CS).

Для просмотра списка интеграций с центрами сертификации необходимо нажать значок . Для добавления необходимо выполнить следующие действия:

- нажать «Добавить центр сертификации» (Рисунок 204);
- заполнить поля ввода, приведенные в таблице (Таблица 48);
- нажать кнопку «Создать».

В результате интеграция с центром сертификации будет добавлена в ППО.

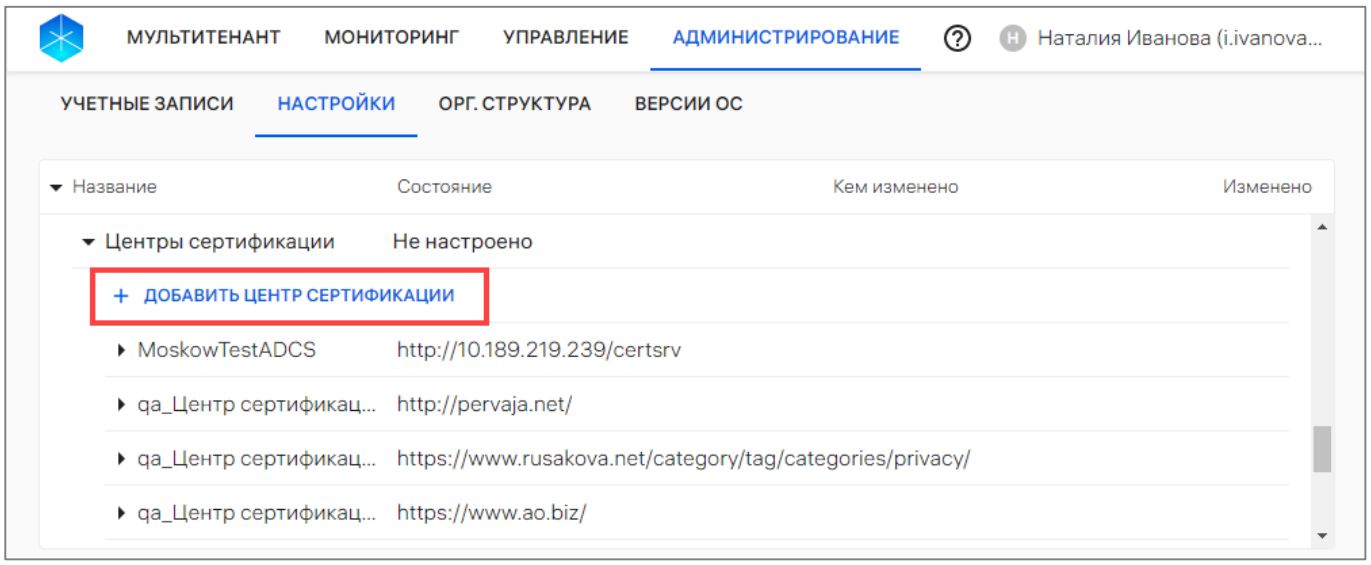

Рисунок 204

Таблица 48

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

4.1.5. Ссылка на приложение «Аврора Центр» для ОС Android

ВНИМАНИЕ! Ссылка для скачивания приложения «Аврора Центр» задается в конфигурационном файле и доступна только для устройств, функционирующих на ОС Android.

Для отображения ссылки необходимо в строке «Ссылка на приложение Аврора Центр для ОС Android» нажать значок (см. Рисунок 182 [5]).

При ошибке получения данных необходимо нажать на кнопку «Обновить» (Рисунок 205).

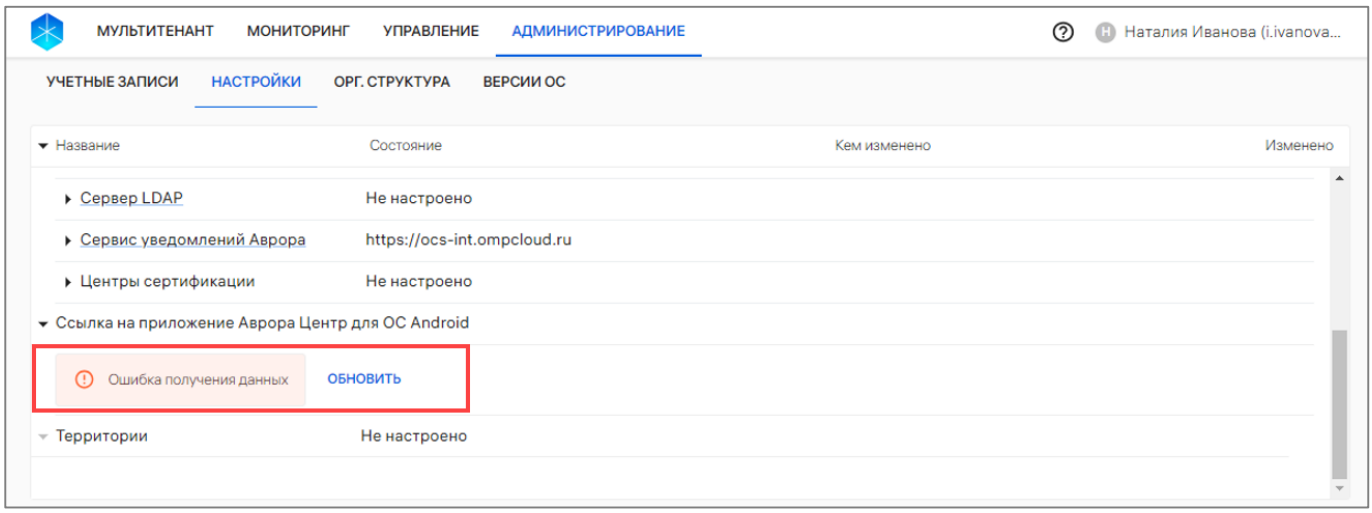

Рисунок 205

4.1.6. 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 182 [6]) отображается список территорий (Рисунок 206 [2]).

Если потребуется просмотреть территорию на карте, необходимо нажать на его название.

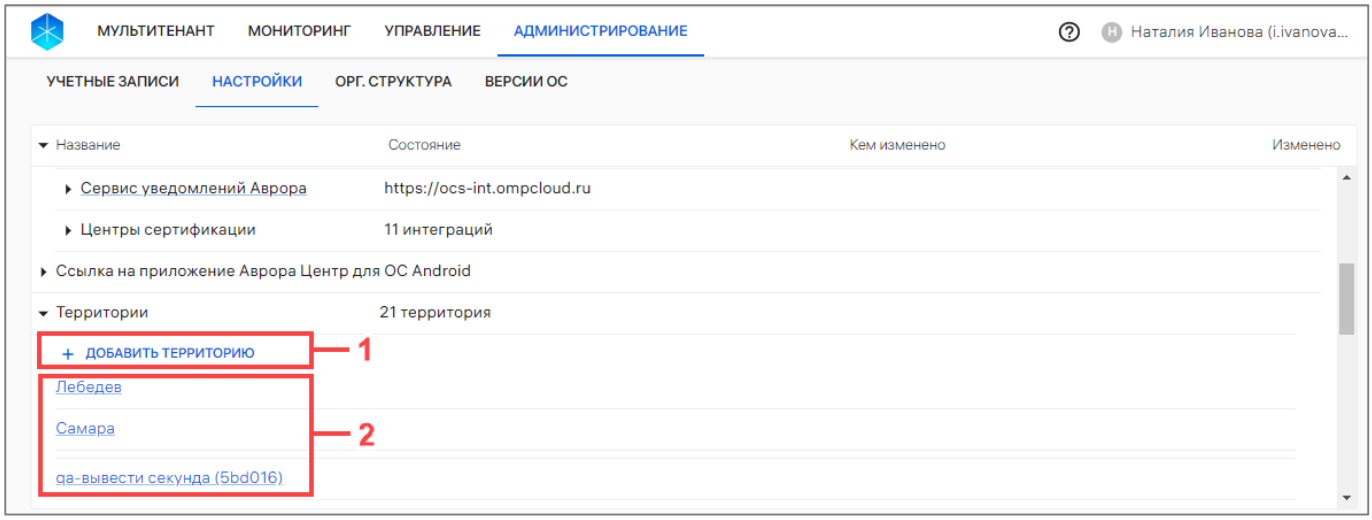

Рисунок 206

Для добавления территории необходимо выполнить следующие действия:

– нажать кнопку «Добавить территорию» (см. Рисунок 206 [1]);

– в отобразившемся окне необходимо ввести название территории в поле «Название» (Рисунок 207 [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 207 [3]);
- указать на карте 4 вершины полигина (Рисунок 207 [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 207 [4]);

– после ввода данных необходимо подтвердить либо отменить действие (Рисунок 207 [5]).

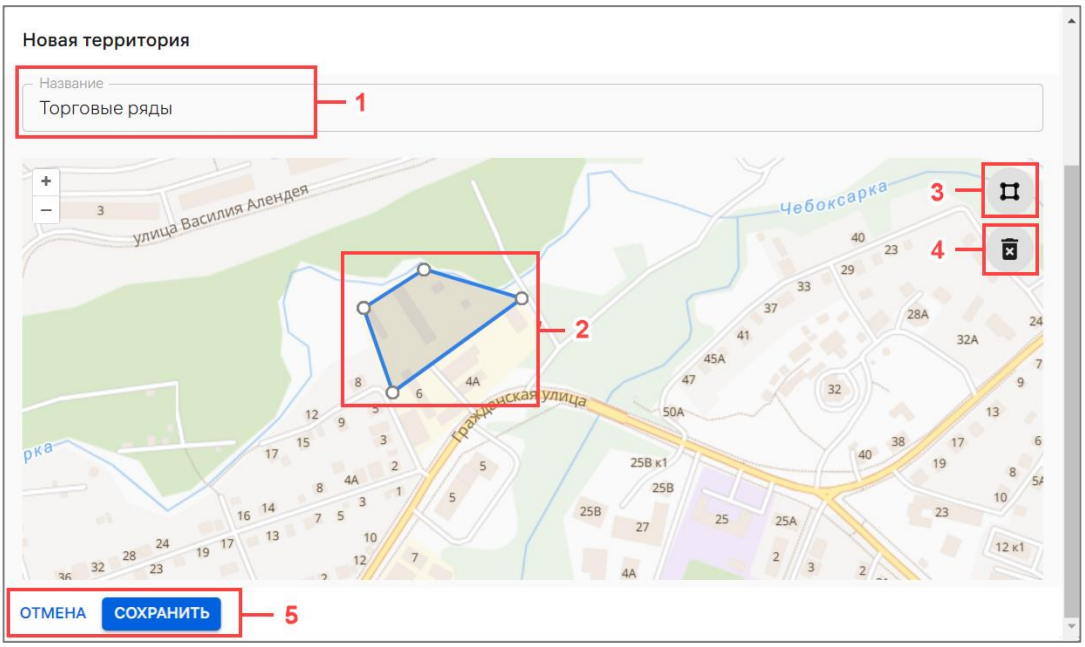

Рисунок 207

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».

4.2. 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 раздел «Администрирование», подраздел «Орг.структура». В результате отобразится основная информация о пользователях (сотрудниках) и о подразделениях пользователей в следующих столбцах:

– «Подразделение/Пользователь» - название группы или Ф.И.О. (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 208) либо при его отсутствии отобразится «Нет дочерних элементов».

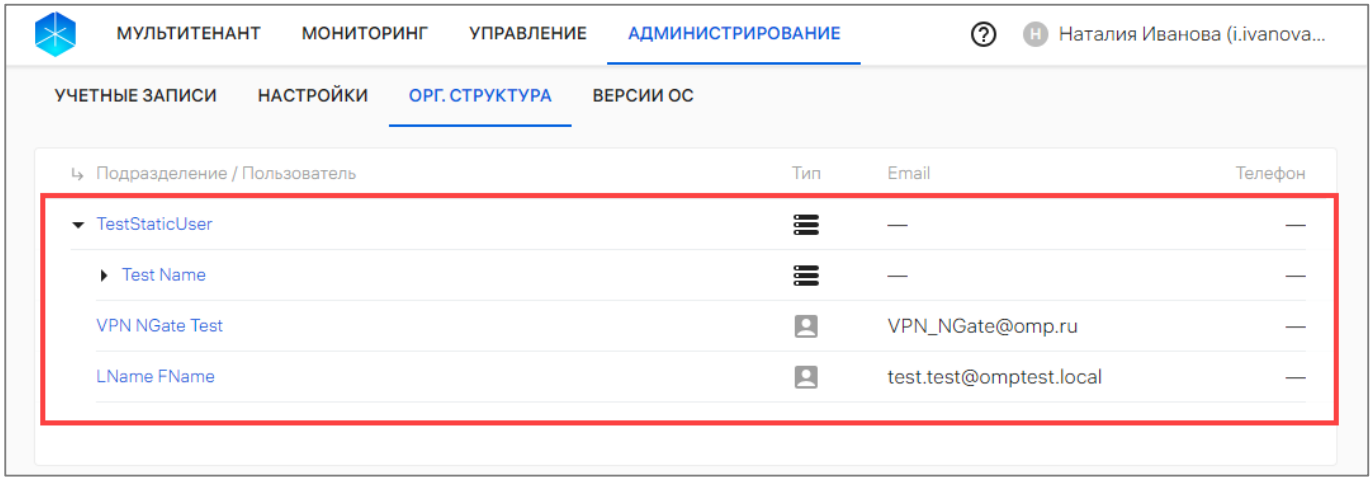

Рисунок 208

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 49).

Таблица 49

№ 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	Не найдено	Попытка обращения к несуществующему элементу управления. Необходимо обновить страницу
4	Доступ запрещен	Необходимо обратиться к Администратору учетных записей для назначения прав. У учетной записи пользователя нет необходимых прав доступа для просмотра выбранной страницы
5	Истекло время действия активной сессии. Обновите страницу	Авторизованная сессия завершена. Необходимо обновить страницу браузера
6	Истек срок действия загруженного Вами QR-кода. Загрузите другой или сгенерируйте новый	Загружен JSON-файл с истекшем сроком действия (`expiredAt`). Необходимо загрузить JSON-файл с актуальным сроком действия

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
7	Произошла ошибка на стороне сервера. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору
8	Не удалось считать данные из JSON. Попробуйте другой JSON файл или исправьте этот	Загрузка некорректного JSON-файла. Необходимо поверить корректность загружаемого файла
9	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
10	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: – `accountDomain`; – `gatewayURI`; – `clientID`
11	Устройство с таким MAC WLAN уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле
12	Устройство с таким IMEI уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле
13	Данное устройство было удалено из системы	Необходимо обратиться к администратору
14	Нельзя удалить группу, созданную в Active Directory	Невозможно удалить группу, созданную в Active Directory
15	Нельзя удалить непустую группу	Попытка удалить группу с назначенными устройствами или пользователями. Необходимо исключить все дочерние элементы из группы, затем произвести удаление

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
16	В JSON-файле не указан ID активации (`enrollmentID`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным `enrollmentID`
17	В JSON-файле не указан пароль (`password`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным паролем
18	В JSON-файле не указан адрес активации (`gatewayURI`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным адресом сервера активации
19	В JSON-файле не указан срок истечения (`expiredAt`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с актуальным сроком действия
20	Динамическая группа с такими условиями уже существует в системе	Попытка создания динамической группы с аналогичными условиями
21	Импорт уже запущен. Дождитесь окончания процесса	Повторная попытка запуска импорта из LDAP при ранее запущенном импорте. Необходимо дождаться завершения выполнения импорта
22	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
23	Не удалось создать офлайн-сценарий. Сообщите об этой ошибке администратору	Попытка создания сценария с невалидными параметрами. Необходимо обратиться к администратору
24	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
25	Пользователь с указанным Email уже существует	Попытка создать пользователя с существующим Email. Необходимо проверить корректность заполнения поля «Почта рабочая»
26	Группа с таким именем уже существует в системе	Попытка создать группу устройств с существующим наименованием. Необходимо изменить значение в поле «Наименование»
27	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
28	Редактирование динамических групп не допускается	Динамическая группа не подлежит редактированию
29	Проверьте корректность заполнения правил	Необходимо проверить корректность заполнения правил
30	Политика с таким именем уже существует в системе	Попытка создать политику с существующим наименованием. Необходимо изменить значение в поле «Наименование»
31	Проверьте корректность заполнения названия политики	Попытка создать политику с пустым наименованием. Необходимо заполнить поле «Наименование»
32	Ошибка при разборе файла. Убедитесь, что выбран нужный файл	Необходимо проверить корректность заполненных данных в CSV-файле
33	Некорректная структура файла. Проверьте файл на соответствие шаблону	Необходимо сверить заполненный CSV-файл с установленным шаблоном
34	Файл не содержит данных. Убедитесь, что выбран нужный файл	Необходимо загрузить CSV-файл с заполненными данными
35	Некорректная модель устройства	Необходимо проверить корректность заполненных данных в CSV-файле

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
36	Некорректный статус устройства в системе	Необходимо обратиться к администратору
37	Не удалось создать QR-коды	Необходимо повторить попытку позже или обратиться к системному администратору
38	Удаленные устройства привязать к группе не удалось	Дополнительно не предусмотрено выполнение каких-либо действий. Все устройства кроме архивных успешно привязались к группе
39	HTTP ERROR 400	Необходимо очистить кэш и cookies веб-браузера и повторить запрос. В случае повторения ошибки следует обратиться к администратору
40	Интеграция с центром сертификации уже существует	Необходимо использовать существующую интеграцию с центром сертификации или добавить новую с другим центром сертификации
41	Название пусто или больше 256 символов	Необходимо ввести название, содержащее от 1 до 256 символов
42	Проверка формата URL не пройдена	Необходимо ввести электронный адрес в формате URL. Например: `https://www.omp.ru/`
43	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
44	Логин пуст или больше 256 символов	Необходимо ввести логин, содержащий от 1 до 256 символов
45	Пароль пусто или больше 256 символов	Необходимо ввести пароль, содержащий от 1 до 256 символов
46	Ошибка при обработке полученных данных	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
47	Не удалось удалить настройки интеграции	Необходимо обновить страницу и повторить попытку или обратиться к системному администратору
48	Ошибка сохранения настроек интеграции	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее
49	Подключение недоступно	Необходимо нажать «Подробнее», чтобы посмотреть полный текст ошибки (пп. 4.1.4.3.1). Обратиться к системному администратору, администратору LDAP или повторить попытку позднее
50	Доступ запрещен	У учетной записи пользователя отсутствуют права доступа, требуемые для просмотра выбранной страницы. Для назначения прав необходимо обратиться к Администратору учетных записей
51	Загружен пустой CSV файл	Необходимо загрузить CSV-файл с заполненными данными
52	Указанные данные не прошли проверку. Скорректируйте данные перед отправкой	Указанные данные не прошли проверку. Необходимо скорректировать данные перед отправкой
53	Ошибка валидации заголовка. Указаны некорректные названия колонок. Правильные названия колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
54	Ошибка валидации заголовка. Указаны не все колонки. Количество колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
55	Ошибка валидации заголовка. Неправильный порядок колонок. Правильный порядок колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
56	Ошибка при разборе файла. Убедитесь, что выбран нужный файл	Необходимо проверить корректность выбранного CSV-файла для импорта

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
57	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
58	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Необходимо проверить корректность заполненных данных в CSV-файле
59	WLAN MAC устройства (WLAN_MAC). Ошибка валидации значения. Рекомендуем проверить указанное значение на соответствие WLAN MAC устройства	Необходимо проверить корректность заполненных данных в CSV-файле, в частности WLAN_MAC
60	IMEI устройства (IMEI). Ошибка валидации значения. Рекомендуем проверить указанное значение на соответствие IMEI устройства	Необходимо проверить корректность заполненных данных в CSV-файле, в частности IMEI
61	Комментарий (COMMENT). Ошибка валидации значения. Длина должна быть до 512 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности COMMENT
62	Ошибка импорта устройства. Значение IMEI или WLAN MAC не соответствует заведенному в базе	Необходимо проверить корректность заполненных данных в CSV-файле, в частности IMEI и WLAN_MAC
63	Модель устройства (MODEL_CODE). Ошибка валидации значения. Указанное значение не соответствует коду модели устройства из справочника устройств	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, MODEL_CODE
64	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 3 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, GROUP

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
65	Ошибка поиска устройства. Для поиска устройства необходимо наличие IMEI и WLAN_MAC	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, IMEI и WLAN_MAC
66	Фамилия (LAST_NAME). Ошибка валидации значения. Фамилия может содержать: а-я ё a-z А-Я Ё A-Z – ' пробел	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, LAST_NAME
67	Отчество (PATRONYMIC). Ошибка валидации значения. Отчество может содержать: а-я ё a-z А-Я Ё A-Z - ' пробел	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, PATRONYMIC
68	Электронная почта (EMAIL). Ошибка валидации значения. Электронная почта состоит из 2 частей (логина пользователя и доменного имени сервера), разделенных символом «@». Пример: example@example.ru	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, EMAIL
69	Должность (JOB_TITLE). Ошибка валидации значения. Должность может содержать: а-я ё a-z А-Я Ё A-Z - пробел	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, JOB_TITLE
70	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Номер телефона должен состоять из цифр	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, PHONE_NUMBER
71	Имя (FIRST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, FIRST_NAME
72	Фамилия (LAST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, LAST_NAME

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
73	Отчество (PATRONYMIC). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, PATRONYMIC
74	Должность (JOB_TITLE). Ошибка валидации значения. Длина должна быть от 2 до 256 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, JOB_TITLE
75	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, PHONE_NUMBER
76	Электронная почта (EMAIL). Ошибка валидации значения. Длина должна быть от 1 до 256 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, EMAIL
77	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, GROUP
78	MAC WLAN. Ошибка валидации значения. MAC WLAN необходимо переписать из параметров устройства	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, MAC WLAN
79	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, IMEI
80	Ошибка импорта. Файл содержит только заголовок. Файл должен быть заполнен данными	Необходимо проверить корректность заполненных данных в CSV-файле
81	Ошибка импорта пользователя. Пользователь получен из LDAP, изменение его данных недоступно. Для продолжения импорта удалите данную строку из файла	Необходимо проверить корректность заполненных данных о пользователе в CSV-файле
82	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Необходимо проверить корректность заполненных данных в CSV-файле

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 50).

Таблица 50

№ 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	Разделители должны соответствовать разделителям первой строки
15	Комментарий (COMMENT). Ошибка валидации значения. Длина должна быть до 512 символов	Длина должна быть до 512 символов
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

№ п/п	Текст ошибки	Действие для устранения ошибки
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 51).

Таблица 51

№ 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 отсутствии
2	Имя (FIRST_NAME). Ошибка валидации значения. Имя может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение
3	Фамилия (LAST_NAME). Ошибка валидации значения. Фамилия может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение
4	Отчество (PATRONYMIC). Ошибка валидации значения. Отчество может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
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 a-z A-Я Ё A-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
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

№ п/п	Текст ошибки	Действие для устранения ошибки
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 выделяют следующие ограничения, приведенные в таблице (Таблица 52).

Таблица 52

№ п/п	Ограничение	Решение
1	Офлайн-сценарии могут отработать некорректно при ускоренной активации устройства	Рекомендуется назначать офлайн-сценарии после прохождения ускоренной активации
2	Устройство может не подключиться к ПУ, если после его перезагрузки не ввести пароль для разблокировки в течение 1 и более минуты	Перезагрузить устройство повторно и ввести пароль
3	При назначении политики на группу устройств из большого количества устройств (более 10 тысяч) возможно появление в интерфейсе ошибки INTERNAL_ERROR. При этом само назначение политики выполнится в фоновом режим	Оперировать группами с таким количеством устройств, которое позволит назначить на них политики за 1 минуту, оптимальное количество 2 тысячи устройств
4	При обновлении ОС с помощью политики устройство может запрашивать ввод пароля для разблокировки	Ввести пароль для разблокировки и дождаться установки обновления ОС
5	В процессе повторной активации устройство может подключаться к ПУ и получать от нее команды	– **Вариант 1**. Необходимо закончить повторную активацию устройства, отсканировав QR-код. В результате устройство подключится к ПУ и будет получать операции с новым токеном; – **Вариант 2**. Необходимо подождать 1 час, не назначая политики и не отправляя push-уведомления. В результате Device API Gateway больше не будет считать токен валидным и проверит токен в ПБ

№ п/п	Ограничение	Решение
6	Возможна рассинхронизация времени сервера и приложения «Аврора Центр», установленного на устройствах, вследствие чего некорректно работают временные команды оперативного управления	Необходимо воспользоваться одним из способов: – перейти в настройки времени и даты устройства: • если автоматическое обновление времени выключено, необходимо включить его и перезагрузить устройство; • если автоматическое обновление времени включено, необходимо выключить и включить его повторно, перезагрузить устройство; – на группу устройств или группу пользователей, в которую входит устройство, дополнительно назначить политику с правилом, запрещающим изменение даты и времени на устройстве; – вместо блокировки устройства с помощью оперативной команды назначить на группу устройств или группу пользователей, в которую входит устройство, офлайн-сценарий с блокировкой устройства по отсутствию связи с сервером на минимальное значение времени
7	Если при скачивании обновления сертифицированной версии ОС Аврора переключить режим устройства (из режима Администратор в режим Пользователь или наоборот), скачивание может прерваться и, как следствие, обновление не установится	Дождаться завершения обновления ОС и затем переключать режим устройства

№ п/п	Ограничение	Решение
8	Если устройство с обновленным приложением «Аврора Центр» было активировано в тенанте, созданном из дефолтного, а затем очищено, то для его повторной активации в тенанте необходимо обновить приложение «Аврора Центр» через политику в дефолтном тенанте	Необходимо выполнить следующие действия: 1. Активировать устройство в дефолтном тенанте; 2. Назначить на устройства политику с обновлением приложения «Аврора Центр» (с помощью `omp-ocs-updater`); 3. После установки обновления приложения активировать устройство в тенанте, созданном из дефолтного
9	При назначении офлайн-сценариев с событиями «Вне зоны действия WLAN» и «Нахождение в зоне WLAN» на большое количество устройств с ОС Аврора могут быть задержки во времени при выполнении на устройствах назначенных операций (политик, оперативных команд и офлайн-сценариев)	Рекомендуется дождаться выполнения всех назначенных операций (политик, оперативных команд и офлайн-сценариев). Проблема будет устранена в следующих релизах ППО
10	Устройство Mashtab TrustPhone T1 будет иметь статус «Не соответствует политике», если на него назначено правило «Использование камеры – Разрешено» или «Использование микрофона – Разрешено», но при этом пользователь вручную отключил камеру и микрофон с помощью кнопки на корпусе устройств	Необходимо выполнить следующие действия: 1. Включить микрофон и камеру с помощью кнопки на корпусе; 2. Получить состояние устройства с помощью оперативной команды или дождаться следующего взаимодействия устройства с сервером ПУ
11	При изменении времени на устройствах могут некорректно работать оперативное управление и сертификаты для установки соединения с сервером ПУ	Для избежания проблем в работе оперативного управления и сертификатов для установки соединения с сервером ПУ рекомендуется назначить на устройства политику с правилом «Управление датой и временем – Запрещено»

№ п/п	Ограничение	Решение
12	В ОС Android при предельной загрузке оперативной памяти ОС начинает принудительно завершать процессы приложения, исходя из степени важности приложения. Так же могут быть завершены и процессы приложения «Аврора Центр», после чего могут возникнуть следующие проблемы: – приложение «Аврора Центр» не перезапустилось автоматически; – приложение «Аврора Центр» не получает обновленные политики	Необходимо выполнить следующие действия: 1. Перезагрузить устройство; 2. Для получения обновленных политик открыть приложение «Аврора Центр» и нажать кнопку «Обновления»
13	В приложении «Аврора Центр» на ОС Android не поддерживается переустановка приложения с понижением версии	Если приложение уже установлено, установить более раннюю версию этого приложения с помощью политики невозможно
14	Если на устройствах на базе ОС Android включена Play Защита, она будет срабатывать при установке приложения с помощью политик. Play Защита будет требовать подтверждения установки каждого приложения, устанавливаемого с помощью политики. Если пропустить окно с подтверждением (например, при выключенном экране), требуемое приложение не будет установлено	Отключить Play Защиту перед установкой приложения с помощью политик

№ п/п	Ограничение	Решение
15	Из-за особенностей ОС Android при назначении политики с правилом «Режим работы bluetooth – Выключен» происходит отключение функции Bluetooth® на устройствах	Необходимо учитывать ограничение. Иначе это может привести к тому, что при назначении второго правила «Управление bluetooth – Включон»: – Bluetooth® будет перманентно отключен; – устройство будет находиться в статусе «Не соответствует политике», т.к. текущее состояние устройства со свойством «Управление bluetooth» будет находиться постоянно в значении «Недоступно»
16	Пользователь может вручную остановить работу приложения «Аврора Центр» для ОС Android через параметры для разработчика	Необходимо учитывать это ограничение в работе с устройствами на базе ОС Android
17	На устройствах с ОС Аврора версии 5.1.0 и выше не поддерживается даунгрейд приложений	**ВНИМАНИЕ!** На устройствах с ОС Аврора версии 5.1.0 и выше не поддерживается обновление приложений с понижением версии. Проблема будет устранена в следующих версиях ППО и ОС Аврора
18	Если одноразовый пароль пользователя/администратора не был применен на устройстве, то повторная отправка того же пароля приведет к ошибке «Ошибка при смене пароля пользователя»/«Ошибка при смене пароля администратора»	– **Вариант1**. Необходимо убедиться, что отправленный одноразовый пароль был применен на устройствах, и повторить отправку; – **Вариант 2**. Необходимо отправить на устройствах одноразовый пароль пользователя/администратора, отличный от предыдущего

№ п/п	Ограничение	Решение
19	ПУ поддерживает управление устройств с 1 администратором и 1 пользователем в ОС. Если в ОС на устройствах создано несколько пользователей, то состояние устройства может не соответствовать ожидаемому поведению. Подключения, для которых были созданы и выпущены пользовательские сертификаты, не будут работать на устройствах, если пользователь не будет совпадать с указанным в сертификате	Необходимо учитывать это ограничение при назначении политик на устройствах

20	После переактивации устройства на другом сервере могут не устанавливаться приложения	Проблема актуальна для устройств с ОС Аврора версий 4.0.2 update 5, 4.0.2 update 6, 4.0.2 update 7 и 5.0.1.
		Приложения могут не устанавливаться как локально (через RPM-файл), так и из политики. Для решения проблемы необходимо:
		1) Установить `zypper` с помощью команды:
		`devel-su pkcon install zypper`
		2) Просмотреть список репозиториев с помощью команды: `zypper lr`
		3) В списке репозиториев найти репозитории PK_TMP_DIR и узнать его номер (будет указан перед репозиторием). Удалить репозиторий с помощью команды:
		`zypper rr <номер репозитория>`

№ п/п	Ограничение	Решение
21	Через 5 секунд после получения команды на очистку осуществляется отправка обновленного состояния устройства и его сброс к заводским настройкам. Если за эти 5 секунд обновленное состояние по каким-то причинам не отправилось (например, из-за недоступности сервера ПУ), то при следующем подключении к серверу устройство снова получит операцию на очистку. **ПРИМЕЧАНИЕ.** Описанный процесс может повторяться более одного раза	Необходимо учитывать данную особенность при отправке операции по очистке устройства. Выполнение операции будет усовершенствовано в следующих версия ППО
22	В режиме киоска не открываются веб-страницы при нажатии на ярлыки	Если браузер включен в список приложений режима киоска, необходимо: – открыть его и пройти все необходимые шаги знакомства (onboarding); – открыть ярлык нужной веб-страницы
23	При выполнении бизнес-сценария по выводу из эксплуатации устройство не архивируется	Необходимо учитывать это ограничение при вызове бизнес-сценария по выводу устройства из эксплуатации. Выполнение операции будет усовершенствовано в следующих версия ППО
24	Устройство на базе ОС Аврора версии 4.1.0 блокируется навсегда при его выключении или перезагрузки во время действия блокировки через ПУ	Необходимо учитывать данную особенность при блокировке устройства через ПУ. Выполнение операции будет усовершенствовано в ОС Аврора версии 4.1.0 update1

№ п/п	Ограничение	Решение
25	Особенность использования сертификатов при активации и самостоятельной регистрации устройств	Если для активации или самостоятельной регистрации устройств используются сертификаты, загруженные в приложение «Аврора Центр», то при установке соединения сервером будут использованы только эти сертификаты, а сертификаты ОС будут проигнорированы. Необходимо учитывать эту особенность, иначе при активации или самостоятельной регистрации устройства возможна ошибка «Server reply 5: Operation canceled» в журнале приложения «Аврора Центр» на устройстве
26	Приложение RustDesk для удаленного подключения может быть отключено на устройстве ОС Android версии 7 самостоятельно из-за сбоя	На устройствах с ОС Android версии 7, на которой установлено приложение RustDesk версии 1.2.3, может периодически прерываться сеанс удаленного подключения из-за падения приложения RustDesk. Проблема подтверждена разработчиками приложения RustDesk: – [Crash] app often crashes (Android 6.0 and Android 7.1 , armv7) #4118; – Android HMI crashes at "input" Android 7.1.2 #6140; – Android app crash Version 1.2.3 #8124. В этом случае необходимо повторно сконфигурировать сеанс удаленного подключения через интерфейс ППО и повторить подключение к рабочему столу устройства. Проблема будет устранена в следующих версиях Аврора Центр и приложения RustDesk

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 53).

Таблица 53

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: – 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

ПРИЛОЖЕНИЕ 1

Описание используемых значков

Значок	Описание	Примечание
Тип 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	
Тип группы устройств		
	Динамическая группа	Группа, в которую устройства добавляются автоматически согласно выбранному алгоритму добавления
	Статическая группа	Группа, в которую можно добавлять отдельные устройства
Тип пользователя		
	Пользователь	Пользователь, добавленный в ПУ вручную или с помощью импорта CSV-файла
	Пользователь из орг.подразделения	Пользователь, полученный из LDAP
Тип группы пользователей		
	Группа пользователей	Группа пользователей, созданная вручную или с помощью импорта CSV-файла
	Организационное подразделение	Группа пользователей, полученная из LDAP

Значок	Описание	Примечание
Статус жизненного цикла		
	Зарегистрировано	Устройство, добавленное в ПУ
	В процессе активации	Сгенерирован QR-код для устройств
	Активировано	Устройство активировано
	Очищено	Устройство очищено (сброшено к заводским настройкам)
	Архивное	Устройство архивировано (удалено)
Соответствие назначенной политике		
	Соответствует политике	Устройство активировано и соответствует назначенным политикам
	Не соответствует политике	Устройство активировано и не соответствует хотя бы 1 назначенной политике
	Не управляется	Устройство не управляется ПУ
	Управление политиками доступно только для активированных устройств	
Тип сообщения о событии		
	Информационное	
	Предупреждение	
	Критическое	
	Отладочное	

ПРИЛОЖЕНИЕ 2

Рекомендации по конвертации CSV-файла в книгу Excel

Для успешной конвертации экспортированного CSV-файла (п. 2.2.5) в книгу Excel необходимо выполнить следующие дейтсвия:

– открыть CSV-файл с помощью MS Excel;

– перейти во вкладку «Данные» (Рисунок 209);

– на панели инструментов выбрать «Получить данные»;

– в раскрывающемся списке выбрать «Из файла», далее «Из текстового/CSV-файла»;

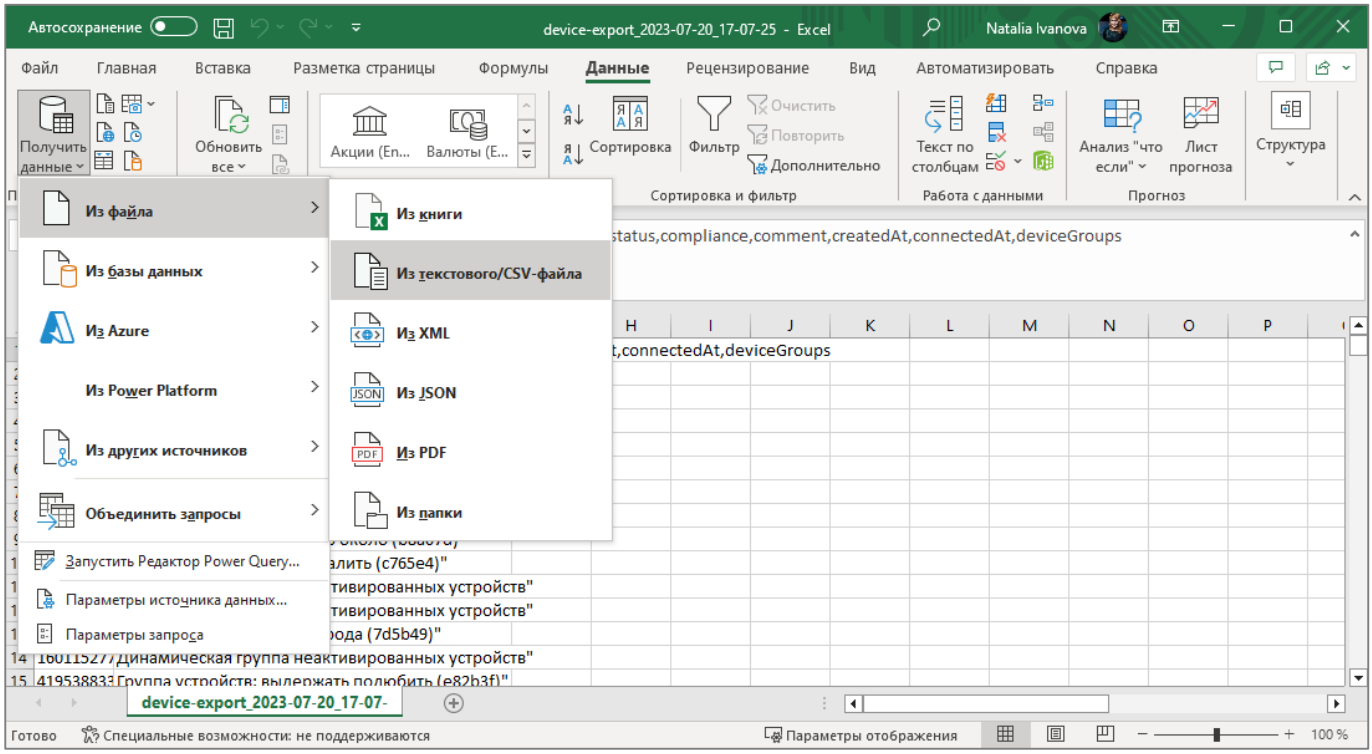

Рисунок 209

– выбрать файл экспорта и нажать кнопку «Импорт» (Рисунок 210);

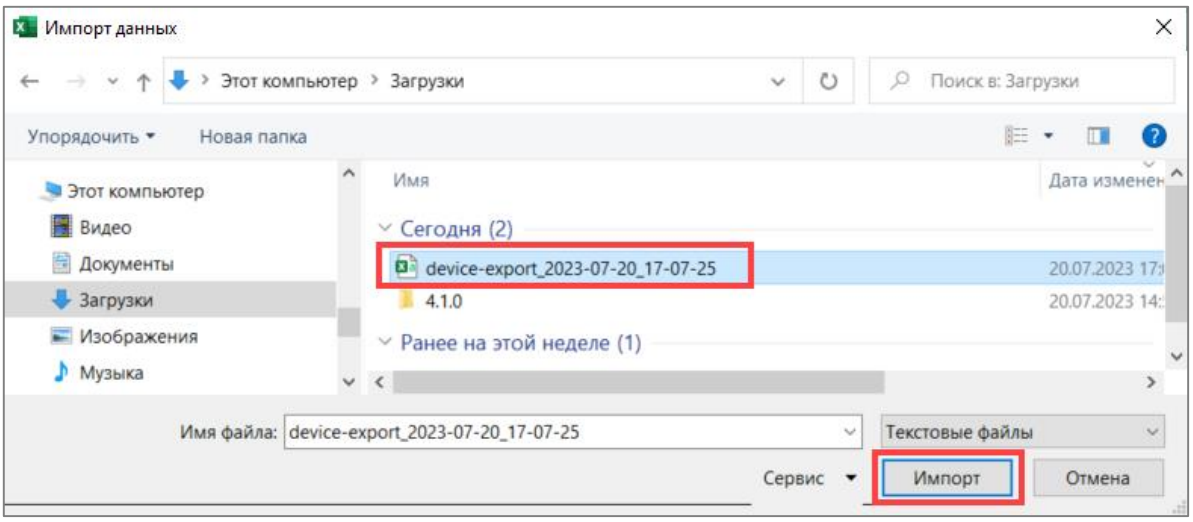

Рисунок 210

– убедиться, что в поле «Разделитель» выбрано значение «Запятая», и нажать на кнопку «Преобразовать данные» (Рисунок 211);

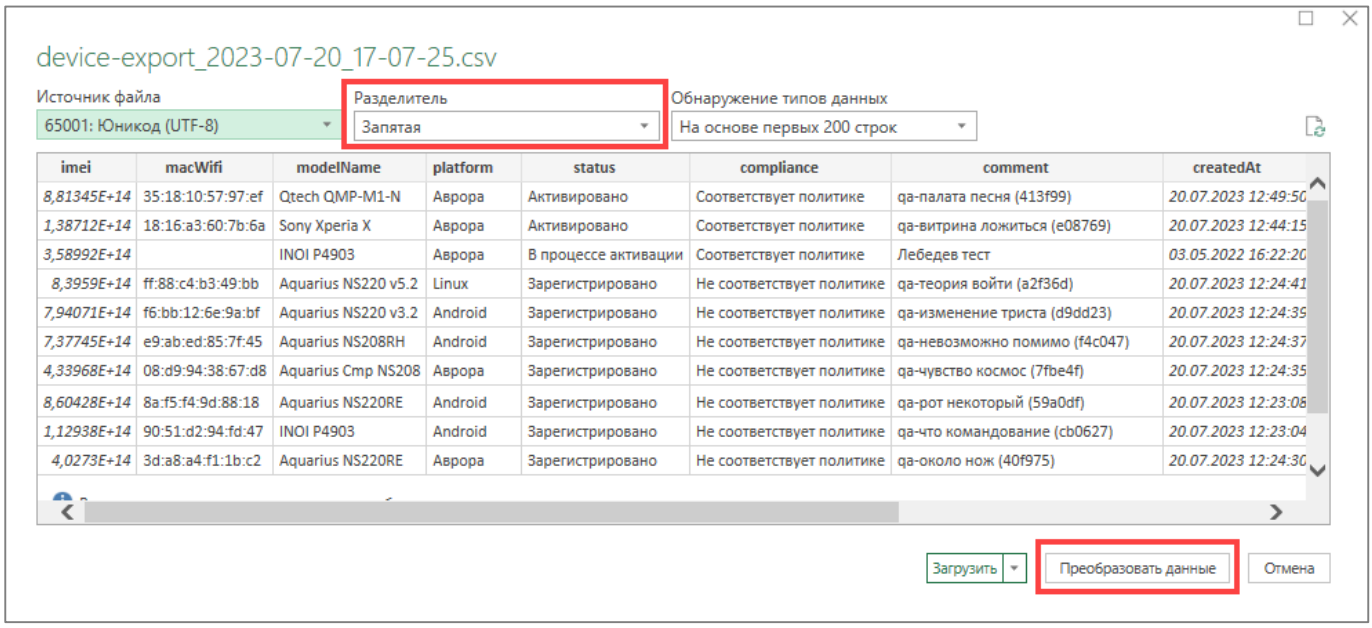

Рисунок 211

– убедиться, что в столбце «deviceGroups» отображаются связки групп (группы, перечисленные через точку с запятой) (Рисунок 212);

– нажать «Закрыть и загрузить».

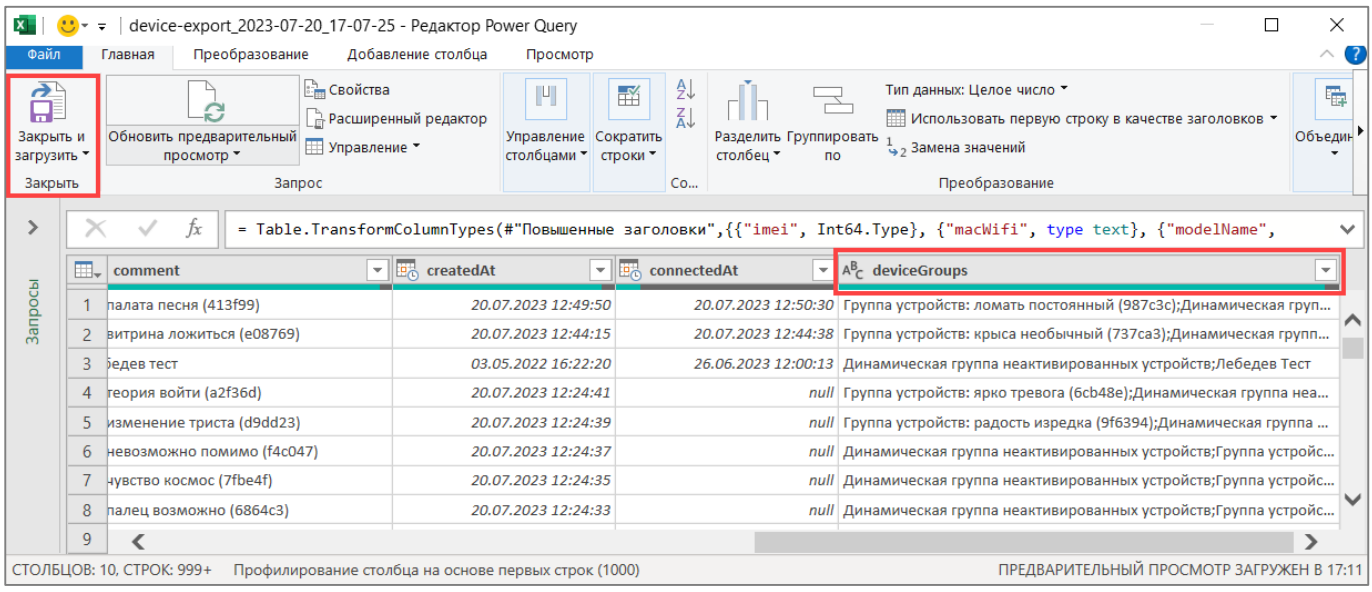

Рисунок 212

В результате отобразится книга Excel, сконвертированная из CSV-файла экспорта.

Если необходимо отфильтровать устройства по группе, то необходимо:

– нажать на значок фильтра справа от названия столбца (Рисунок 213 [1]);
– ввести название группы;
– выбрать все результаты, содержащие название группы (Рисунок 213 [2]);
– нажать кнопку «ОК» (Рисунок 213 [3]).

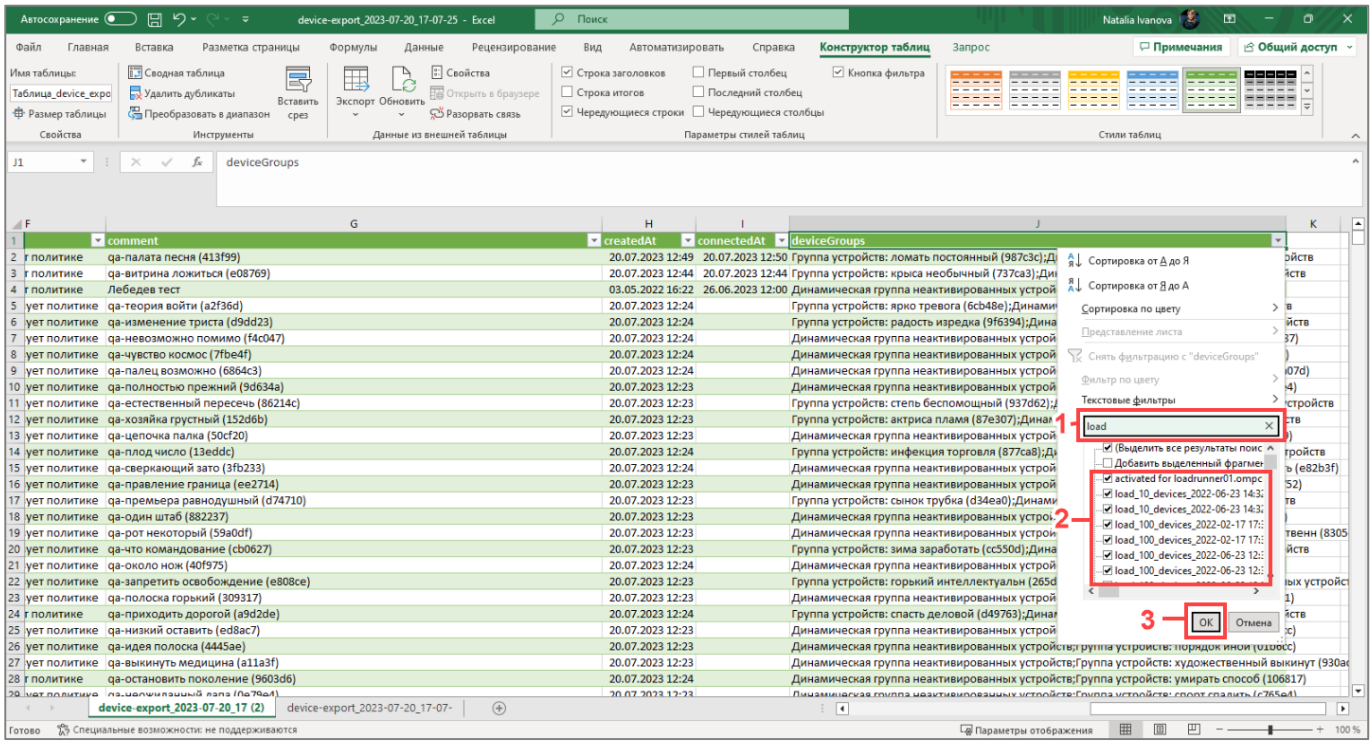

Рисунок 213

ПРИЛОЖЕНИЕ 3

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).

ПРИЛОЖЕНИЕ 4

Подготовка устройства на базе ОС Android к удаленному подключению

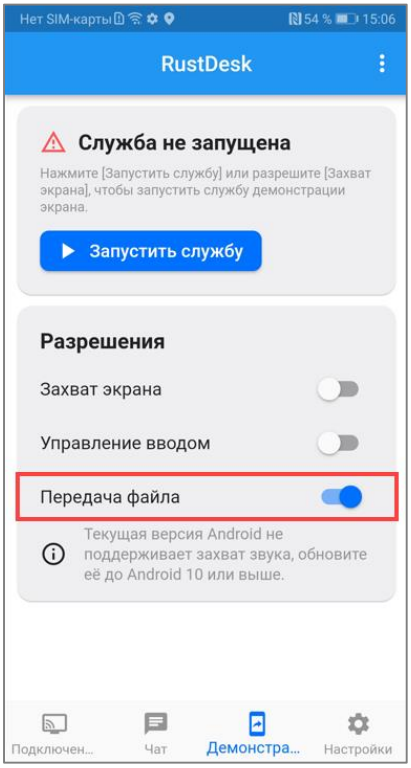

Рисунок 214

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 214). 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 215);

– перейти в системные настройки (Рисунок 216);

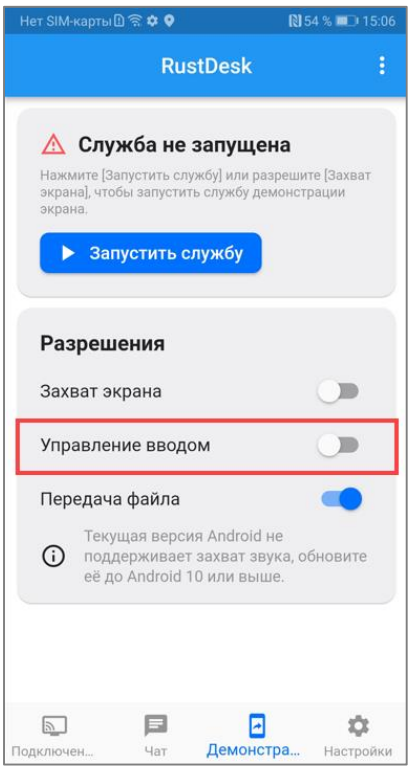

Рисунок 215

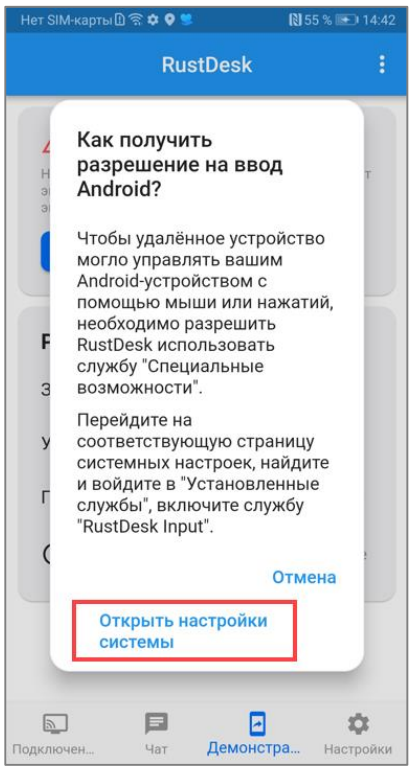

Рисунок 216

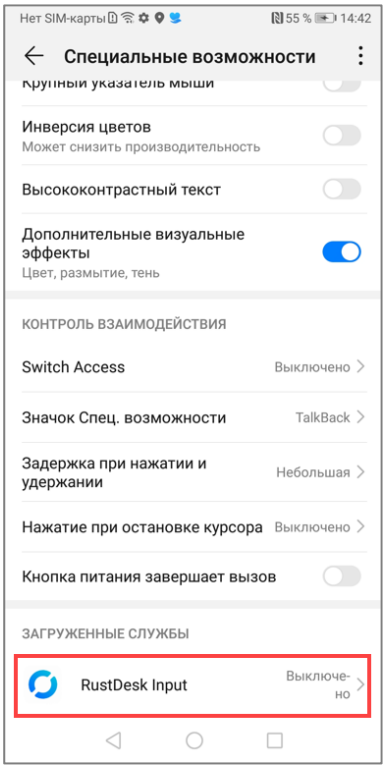

Рисунок 217

– коснуться на RustDesk Input (Рисунок 217), перевести переключатель RustDesk Input в положение «Включено» (Рисунок 218) и подтвердить включение (Рисунок 219).

ПРИМЕЧАНИЕ. Разрешение на управление вводом выдается единожды, положение переключателя будет сохранено для последующих запусков приложения RustDesk;

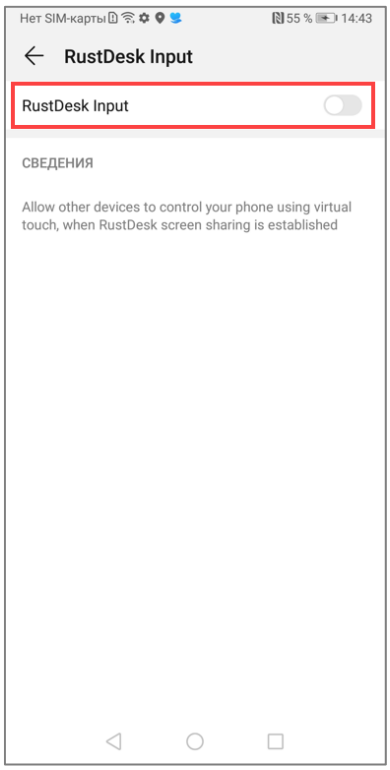

Рисунок 218

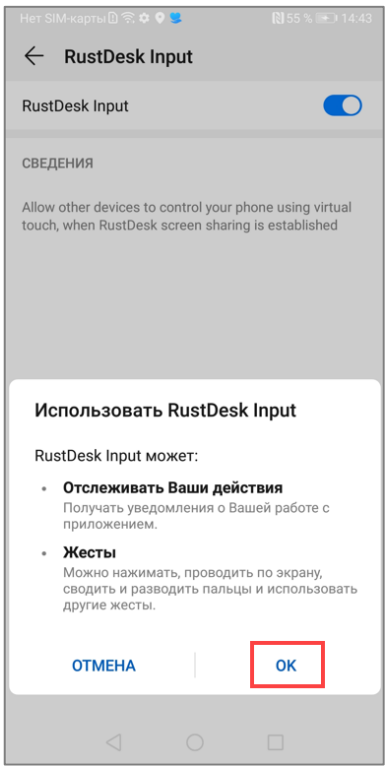

Рисунок 219

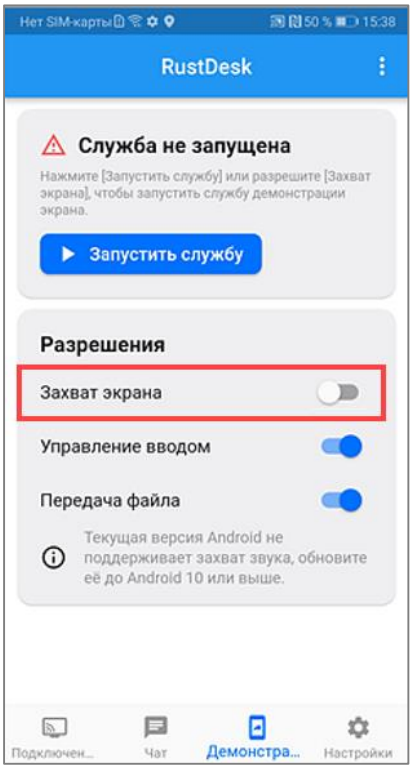

Рисунок 220

4) Выдать разрешение на захват экрана (применимо для ОС Android версий 7-9). Для этого необходимо:

– перевести переключатель «Захват экрана» в положение «Включено» (Рисунок 220);

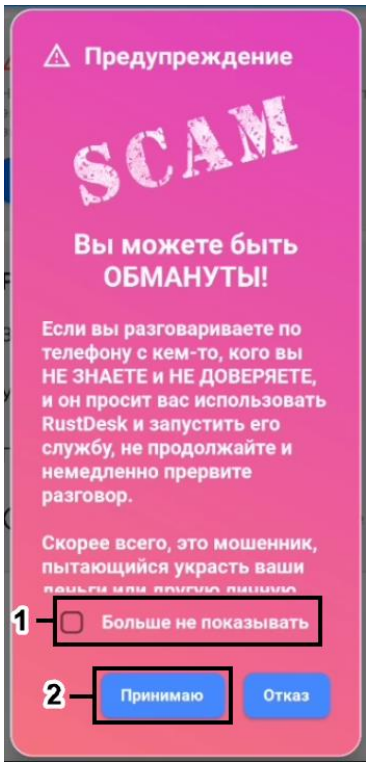

Рисунок 221

– ознакомиться с предупреждением о возможном мошенничестве (Рисунок 221);

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 221 [1]) и выбрать «Принимаю» (Рисунок 221 [2]);

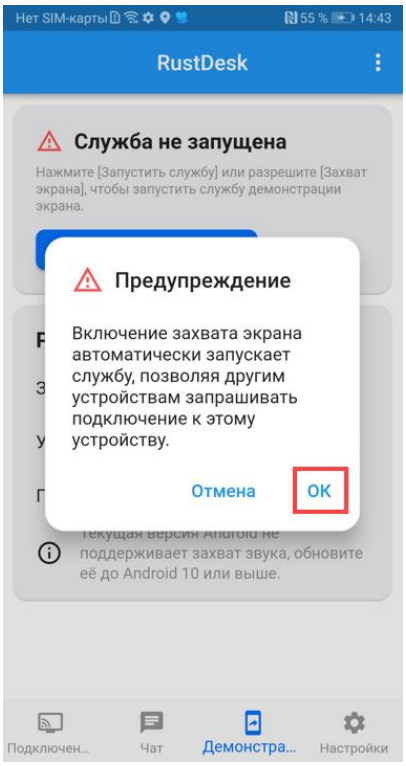

Рисунок 222

– ознакомиться с предупреждением, что включение захвата экрана автоматически запускает приложение RustDesk, и коснуться «OK» (Рисунок 222);

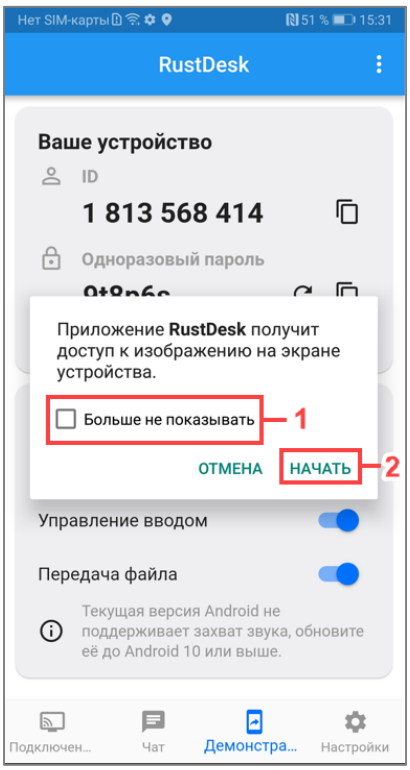

Рисунок 223

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 223 [1]) и коснуться «Начать» (Рисунок 223 []2).

В результате устройство будет готово к удаленному подключению.

ПРИМЕЧАНИЕ. 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 224).

Рисунок 224

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Содержание изменения	ФИО	Дата
1.0	Начальная версия	Лебедев А. Иванова Н.	27.05.2024 г.
1.1	Внесены изменения	Лебедев А. Иванова Н.	06.06.2024 г.
1.2	Внесены изменения	Иванова Н.	10.12.2024 г.