УТВЕРЖДЕН

АДМГ.20134-01 90 01-1-ЛУ

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство пользователя

Часть 3

Подсистема Платформа управления

АДМГ.20134-01 90 01-3

Листов 277

2023

АННОТАЦИЯ

Настоящий документ является третьей частью руководства пользователя Прикладного программного обеспечения «Аврора Центр» АДМГ.20134-01 релиз 4.0.0 (далее – ППО) и содержит описание функционирования подсистемы Платформа управления (ПУ), входящей в состав ППО.

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

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

– управления жизненным циклом мобильных приложений;

– отправки push-уведомлений на мобильные устройства;

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

– автоматизированной обработки следующих видов информации:

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

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

ПРИМЕЧАНИЯ:

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

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

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

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

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

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

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

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

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

Описание работы приложений приведено в документах:

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

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

ВНИМАНИЕ! В зависимости от вариантов поставки интерфейс ППО может отличаться от приведенного на рисунках в настоящем документе. Клиентские приложения «Аврора Маркет»/«Аврора Центр», функционирующие под управлением ОС Android, а также ОС семейства Linux, в комплект поставки не входят. Описание возможных вариантов поставки приведено в документе АДМГ.20134-01 30 01.

СОДЕРЖАНИЕ

1. ПОДГОТОВКА К РАБОТЕ

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

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

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

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

1.1. Описание принципов безопасной работы средства

1.1.1. Общая информация

ППО реализует следующие функции безопасности:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– регистрация событий безопасности.

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

– соблюдение парольной политики;

– соблюдение требования, согласно которому пароль не должен включать в себя легко вычисляемые сочетания символов;

– отсутствие у пользователя права передачи личного пароля третьим лицам;

– обязанность пользователя при вводе пароля исключить возможность его перехвата третьими лицами и техническими средствами.

При эксплуатации ППО запрещается:

– оставлять без контроля незаблокированные программные средства и/или ППО;

– разглашать пароли, выводить их на экран, принтер или иные средства отображения информации.

1.1.2. Компрометация паролей

Под компрометацией паролей необходимо понимать следующее:

– физическую утрату носителя с парольной информацией;

– передачу идентификационной информации по открытым каналам связи;

– перехват пароля при распределении идентификаторов;

– сознательную передачу информации третьим лицам.

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

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

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

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

1.2. Лицензионное соглашение

Перед использованием ППО пользователю необходимо ознакомиться с условиями Лицензионного соглашения, 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 АДМГ.20134-01 91 01.

Для аутентификации в Консоли администратора ПУ необходимо выполнить следующие действия:

– в веб-браузере перейти по адресу Консоли администратора ПУ;

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

– на странице аутентификации выполнить следующие действия:

- заполнить поля «Логин» и «Пароль»;
- выбрать язык интерфейса (по умолчанию интерфейс отображается на языке браузера пользователя);
- 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 АДМГ.20134-01 90 01-1.

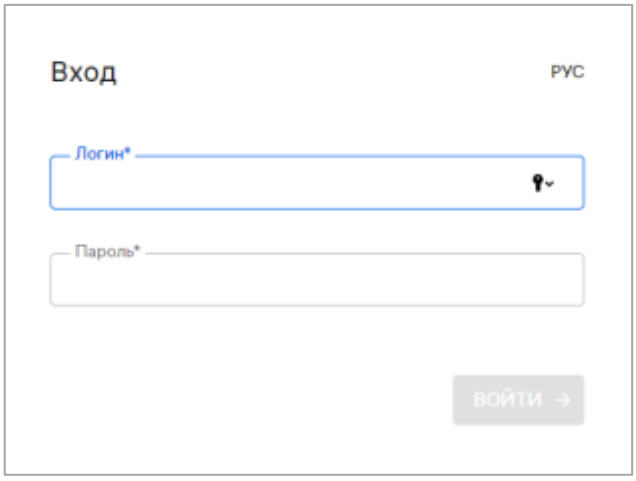

Рисунок 1

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

- ввести текущий пароль;
- ввести новый пароль;
- повторно ввести новый пароль;
- выбрать язык интерфейса;
- нажать кнопку «Продолжить» (Рисунок 2).

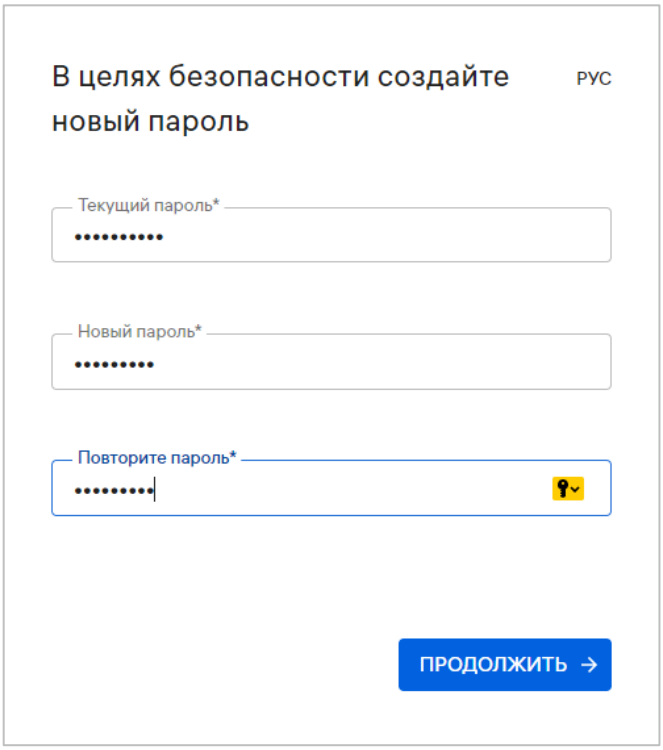

Рисунок 2

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 ПБ;

– нажать кнопку «Отмена», в результате чего все текущие сессии останутся активными и отобразится окно входа в Консоль администратора ПБ.

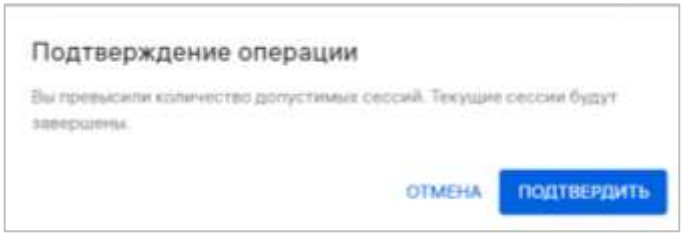

Рисунок 3

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[1] ППО состав разделов верхней панели интерфейса ППО может отличаться.

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

1.4.1. Верхняя панель

Верхняя панель позволяет выполнить следующие действия:

1) осуществлять навигацию между подсистемами ППО (Рисунок 4 [1]);

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

– «Мониторинг» (раздел 3), включающем в себя подраздел «Индикаторы» (подраздел 3.1);

– «Управление» (раздел 2), включающем в себя следующие подразделы:

- «Устройства» (подраздел 2.2);
- «Пользователи» (подраздел 2.3);
- «Политики» (подраздел 2.4);
- «Сценарии» (подраздел 2.5);

– «Администрирование» (раздел 4), включающем в себя следующие подразделы:

- «Настройки» (подраздел 4.1);
- «Орг.структура» (подраздел 4.2).

[1] Описание возможных вариантов поставки приведено в документе АДМГ.20134-01 91 01.

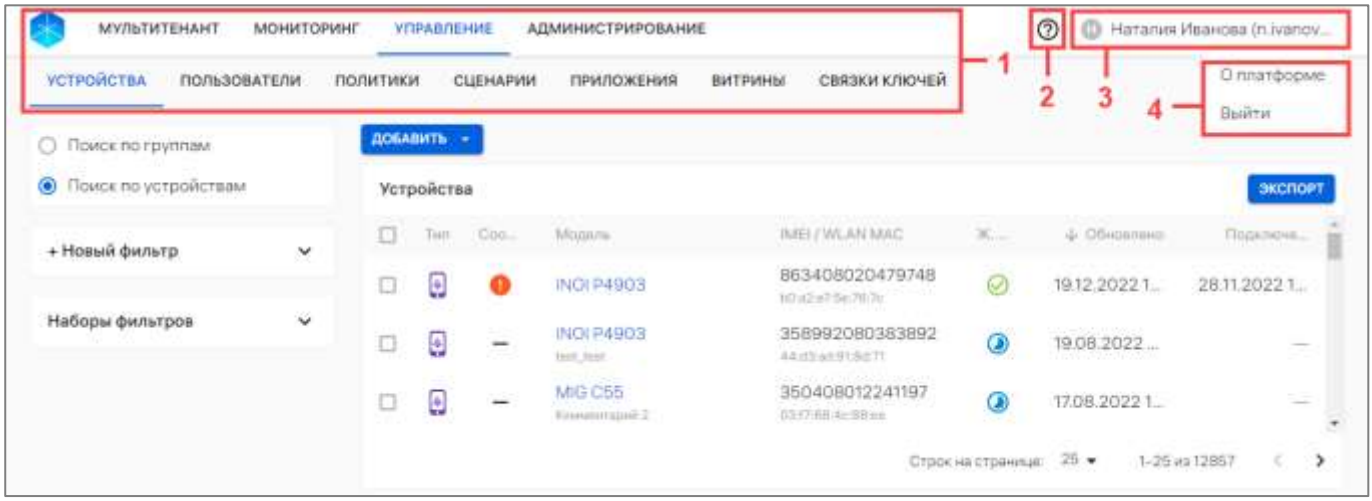

Рисунок 4

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 Н 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».

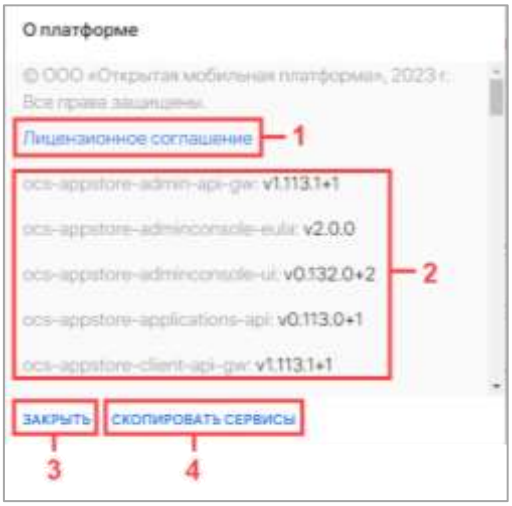

Рисунок 5

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

– привязка устройств к пользователю и его отвязка (вручную, с помощью CSV-файла);

– блокировка и разблокировка устройств;

– очистка содержимого устройства;

– блокировка и разблокировка камеры устройства;

– получение списка системных сообщений с устройств и событий безопасности;

– назначение и отслеживание политик, назначенных на пользователей, группу пользователей, устройств 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.

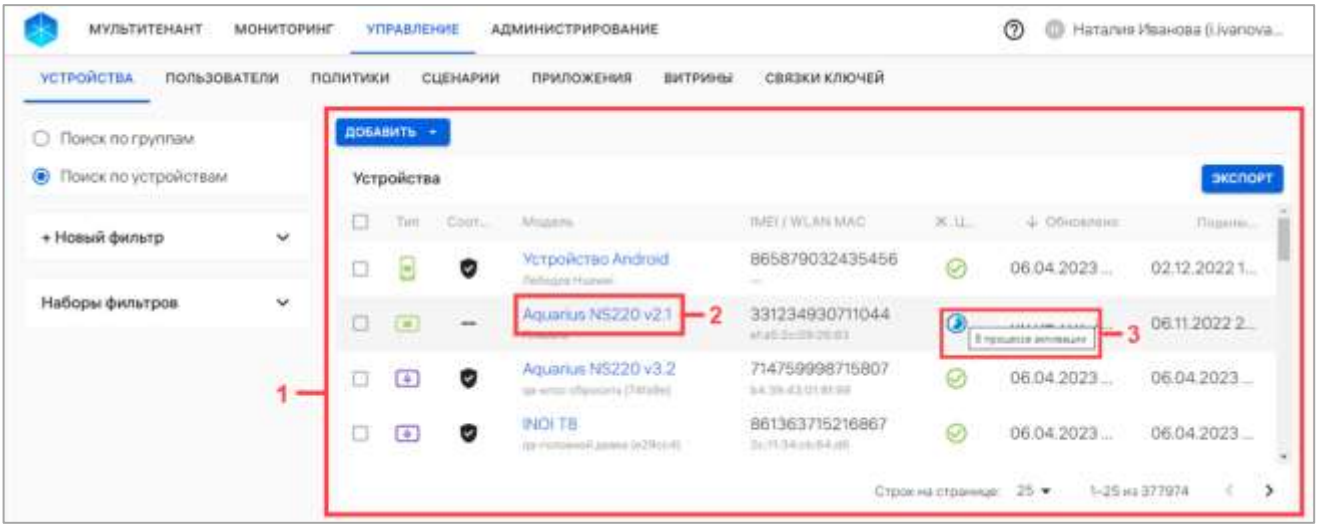

Рисунок 6

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

Таблица 1

Подраздел	Значок	Наименование значка	Назначение	Подробное описание
Устройства				
Устройства		Привязать устройства к пользователям	Привязка устройства к пользователю устройств	пп. 2.2.5.1
		Привязать устройства к группам	Привязка устройства к группе устройств	пп. 2.2.6.1
		Активация устройств	Активация устройств	пп. 2.2.7.2
		Архивировать	Архивирование устройства	пп. 2.2.10.1
Группы устройств				
ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам»		Активация устройств	Активация групп устройств с помощью JSON-файла	пп. 2.2.7.4
Пользователи				
Пользователи		Привязать пользователей к группам	Привязка пользователей к группе пользователей	пп. 2.3.4.1
		Привязать устройства к пользователям	Привязка устройства к пользователям	пп. 2.3.5.1
		Архивировать пользователя	Архивирование пользователя	п. 2.3.6

Подраздел	Значок	Наименование значка	Назначение	Подробное описание
Группы пользователей				
		Привязать пользователей к группам	Привязка пользователей к группе пользователей	пп. 2.3.4.1
Офлайн-сценарии				
		Назначить офлайн-сценарии на группу пользователей	Назначение офлайн-сценариев на группу пользователей	пп. 2.5.2.2
		Назначить офлайн-сценарии на группу устройств	Назначение офлайн-сценариев на группу устройств	пп. 2.5.2.2
		Удалить сценарий	Удаление офлайн-сценария	п. 2.5.4

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

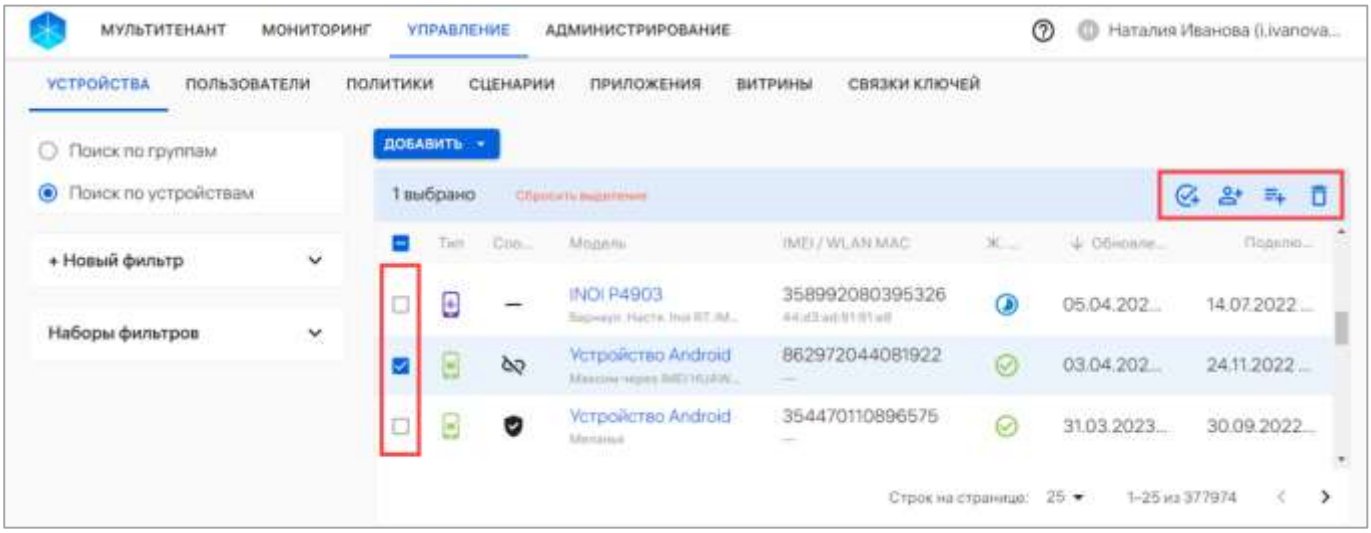

Рисунок 7

1.5. Работа с фильтрами

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

– «Устройства» - поиск устройств, групп устройств и событий безопасности устройств;

– «Пользователи» - поиск пользователей устройств, групп пользователей;

– «Политики» - поиск политик.

В таблице (Таблица 2) приведены фильтры для поиска информации по каждому из подразделов раздела «Управление».

Таблица 2

Подраздел	Фильтры	Доступные значения
Поиск по устройствам		
Подраздел «Устройства» (поиск работает и внутри карточки группы устройств – предусмотрена возможность найти устройство, входящее в конкретную группу)	По IMEI	Поиск по IMEI устройства. Ввод значения с клавиатуры
	По MAC WLAN	Поиск по MAC-адресу WLAN устройства. Ввод значения с клавиатуры. Например, «00:aa:00:00:a0:00»
	По ID	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

Подраздел	Фильтры	Доступные значения
	По дате создания	Поиск по дате и времени добавления устройства за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате и времени обновления устройства за выбранный период. Выбор значения из календаря
	По модели	Выбор модели устройства из списка
	По платформе	ВНИМАНИЕ! При выборе платформы необходимо выбрать «Аврора» т.к. ОС Android, а также ОС семейства Linux, в комплект поставки не входят
	По группе	Поиск устройства по заданной группе. Ввод значения с клавиатуры
	По комментарию	Поиск устройства по комментарию. Ввод значения с клавиатуры
Поиск событий безопасности		
Подраздел «Устройства» → карточка устройства → вкладка «События безопасности»	По типу события	Поиск по типу события безопасности. Выбор значения из списка: – Информационное; – Отладочное; – Предупреждение; – Критическое
	По имени события	Поиск по названию события безопасности. Выбор значения из списка
	По дате получения	Поиск по дате и времени получения события безопасности за выбранный период. Выбор значения из календаря
	По дате возникновения	Поиск по дате и времени 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 дате создания	Поиск по дате и времени добавления группы устройств за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате и времени обновления группы устройств за выбранный период. Выбор значения из календаря

Подраздел	Фильтры	Доступные значения
Поиск по пользователям		
Подраздел «Пользователи» → «Поиск по пользователям»	По email	Поиск по адресу рабочей почты пользователя
	По имени	Поиск по имени, фамилии, отчеству
	По фамилии	
	По отчеству	
	По дате создания	Поиск по дате добавления пользователя за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления пользователя за выбранный период. Выбор значения из календаря
Поиск по группам пользователей		
Подраздел «Пользователи» → «Поиск по группам»	По названию	Поиск группы пользователей устройств по названию. Ввод значения с клавиатуры
	По типу группы	Поиск группы пользователей по типу группы: – Группа пользователей; – Орг.подразделение
	По 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 и времени добавления политики за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате и времени 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 25))

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

Для поиска по заданным критериям требуется выполнить следующие действия:

– перейти в необходимый подраздел интерфейса ППО;

– в области фильтров нажать на раскрывающийся список «Новый фильтр»;

– в поле «Тип фильтра» выбрать из раскрывающегося списка один из фильтров для поиска и задать параметры (Рисунок 8).

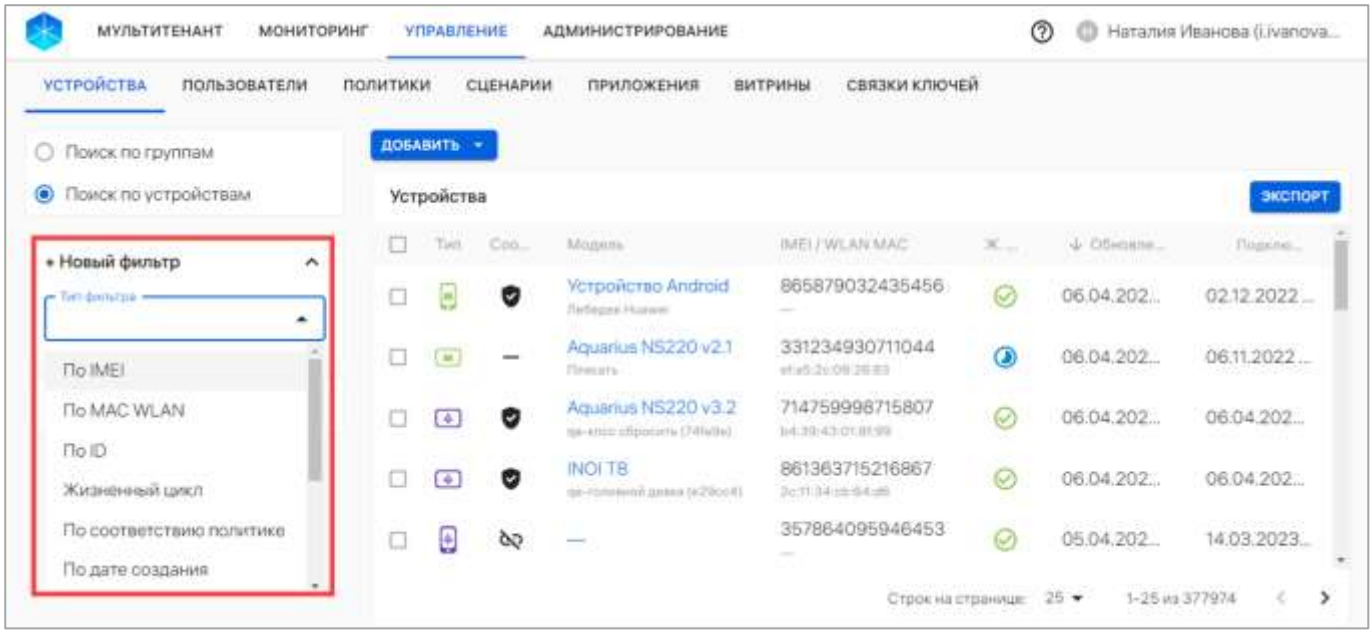

Рисунок 8

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]);

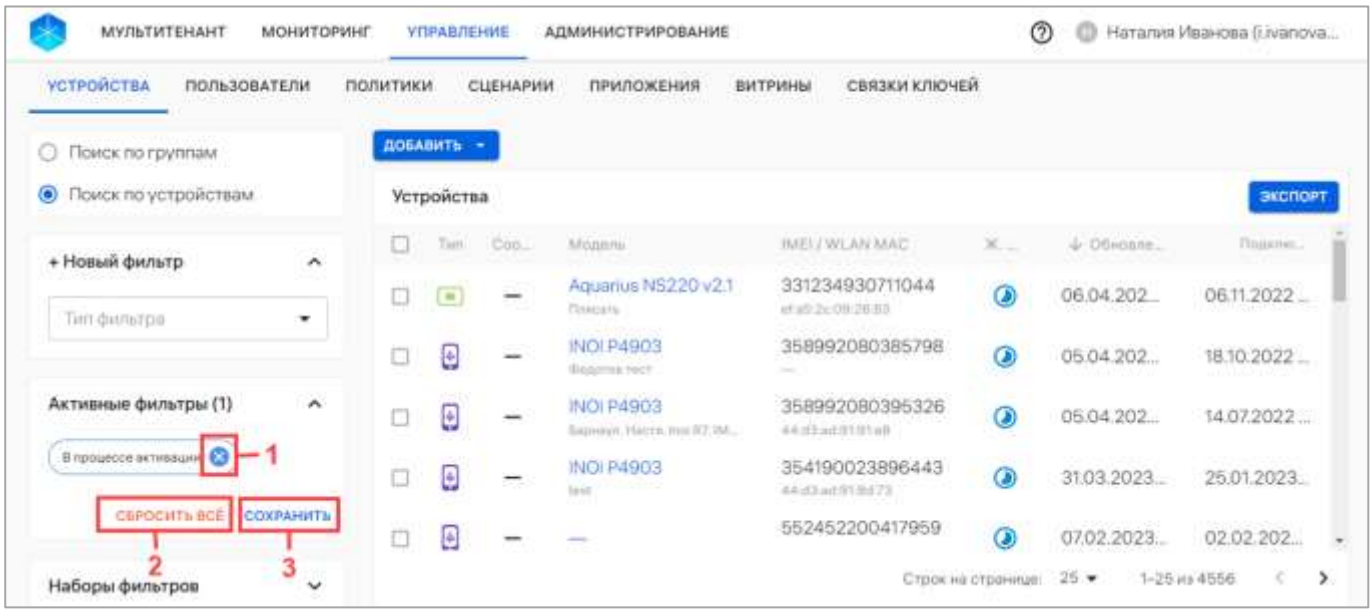

Рисунок 9

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

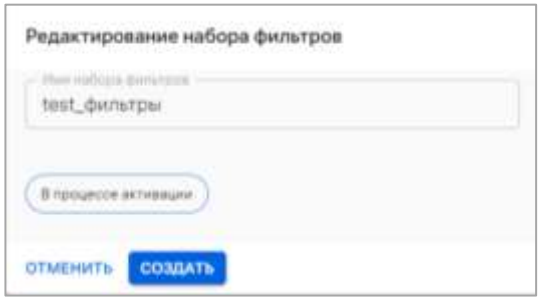

Рисунок 10

– 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 ✎.

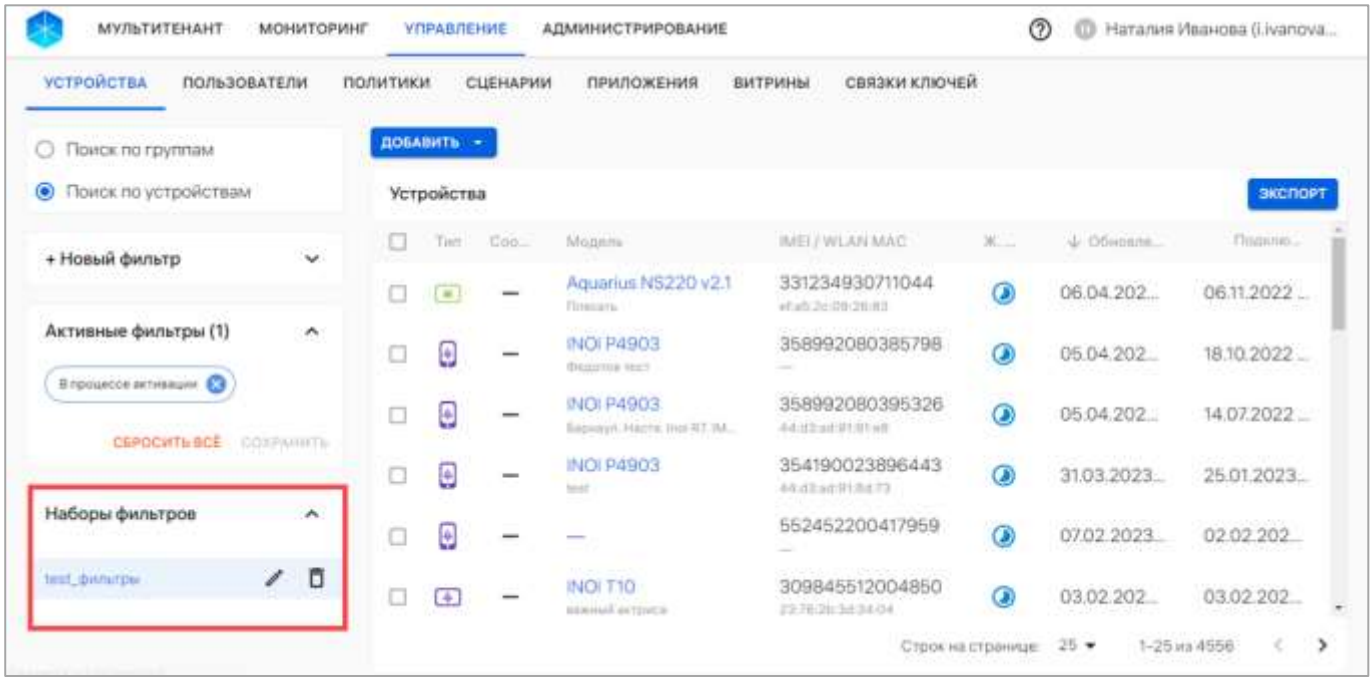

Рисунок 11

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;

– 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»;

– выбрать устройство либо воспользоваться фильтром.

В результате откроется карточка устройства, интерфейс которой включает следующие области:

– шапка (Рисунок 12);

– вкладки. В карточке устройства доступен переход во вкладки:

- «Состояние» (пп. 2.1.1.2);
- «Управление» (пп. 2.1.1.3);
- «Пользователи» (пп. 2.1.1.4);
- «Группы» (пп. 2.1.1.5);

- «Политики» (пп. 2.1.1.6);
- «Сценарии» (пп. 2.1.1.7);
- «События безопасности» (пп. 2.1.1.8);
- «Приложения» (пп. 2.1.1.9).

2.1.1.1. Шапка карточки

В шапке карточки устройства отображается название, тип устройства, платформа, комментарий к устройству, а также следующая информация (Рисунок 12):

– «Статус» — статус жизненного цикла устройства/соответствия политике;

– «Клиент Аврора Центр» — версия клиентского приложения «Аврора Центр» подсистемы ППО, которое установлено на устройство;

– «Клиент Аврора Маркет» — версия клиентского приложения «Аврора Маркет» подсистемы ППО, которое установлено на устройство;

– «IMEI» — IMEI устройства;

– «WLAN MAC» — MAC-адрес WLAN устройства;

– «ID» — идентификатор устройства, который можно скопировать, нажав значок ;

– «Создано» — дата и время добавления устройства;

– «Обновление» — дата и время последнего обновления информации об устройстве;

– «Подключение» — дата и время последнего подключения устройства.

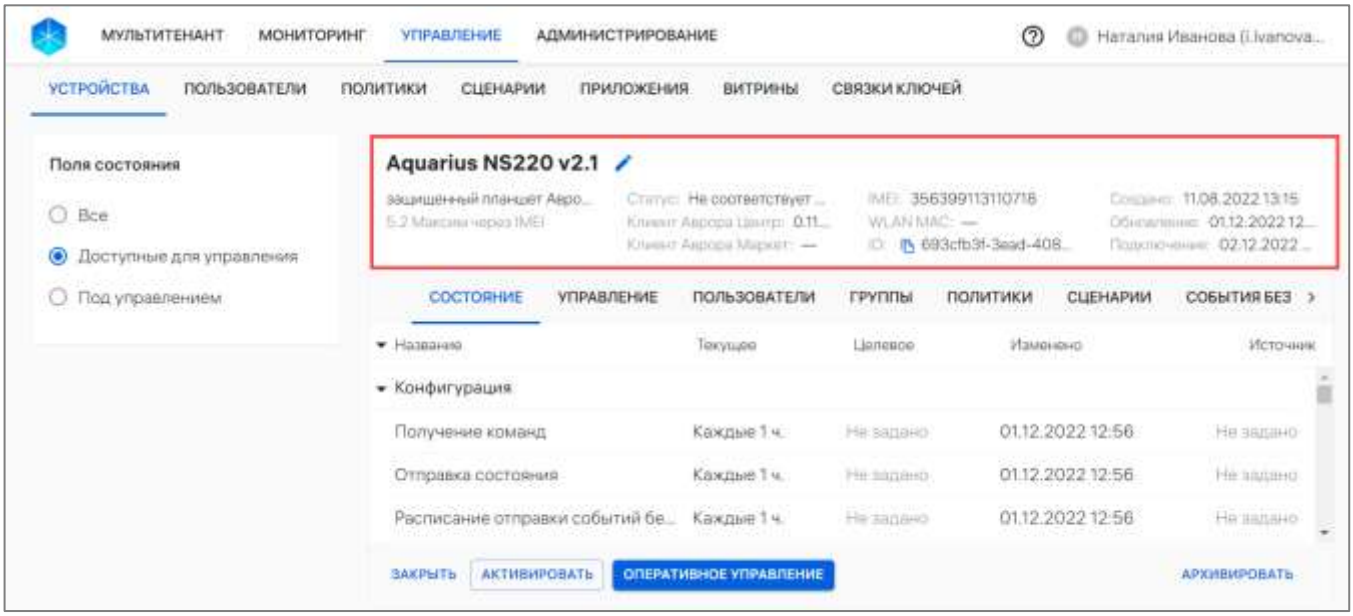

Рисунок 12

В шапке карточки устройства предусмотрена возможность редактирования следующей информации:

– модель устройства;

– комментарий.

Для редактирования шапки карточки необходимо выполнить следующие действия:

– нажать значок ✎ «Редактировать» (см. Рисунок 12);

– в открывшемся окне «Редактирование устройства» отредактировать доступные поля;

– сохранить изменения либо отменить действия (Рисунок 13).

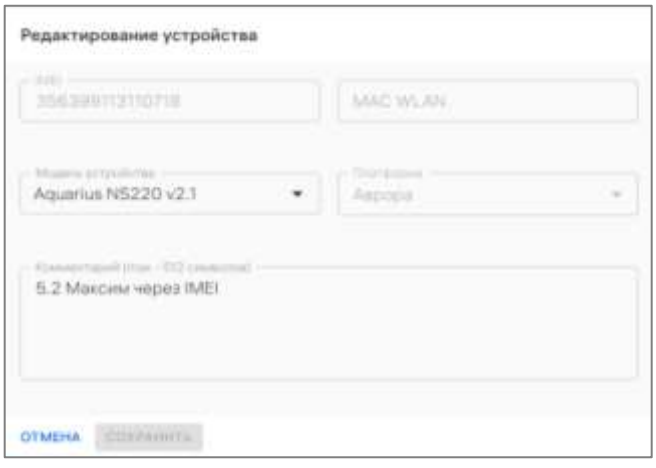

Рисунок 13

В результате успешного сохранения данные в шапке карточки устройства будут обновлены.

2.1.1.2. Вкладка «Состояние»

Во вкладке «Состояние» возможно выполнить следующие действия (Рисунок 14 [3]):

– активировать устройство, нажав кнопку «Активировать» (пп. 2.2.7.1);

– отправить оперативные команды на устройство, нажав кнопку «Оперативное управление» (п. 2.2.8);

– удалить устройство из списка устройств, нажав кнопку «Архивировать» (пп. 2.2.10.2);

– выйти из карточки устройства, нажав кнопку «Закрыть».

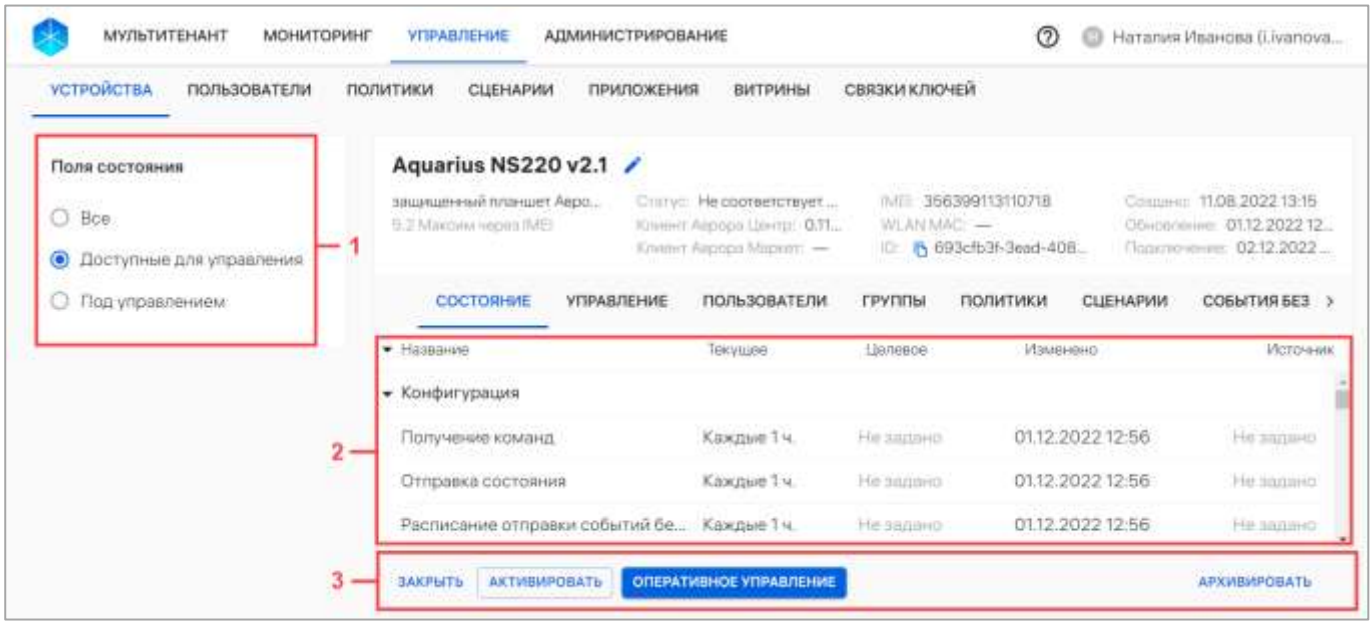

Рисунок 14

Во вкладке «Состояние» в области фильтров предусмотрена возможность управлять отображением полей состояния по следующим параметрам (Рисунок 14 [1]):

– «Все» — отображаются все поля состояния;

– «Доступные для управления» — отображаются поля, значения которых могут задаваться политиками, оперативным управлением, офлайн-сценариями;

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

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 (Рисунок 14 [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 состояния устройства не будут совпадать. Несоответствия выделяются красным цветом, и отображается значок (Рисунок 15).

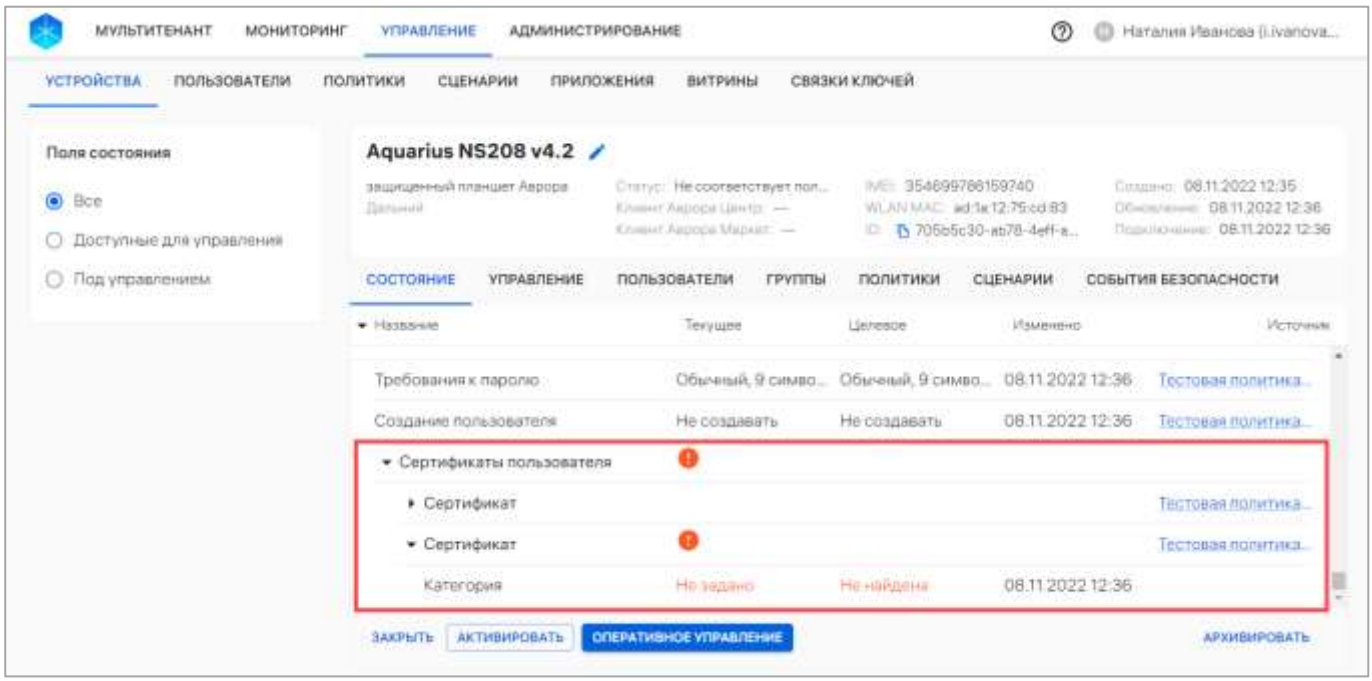

Рисунок 15

Во вкладке «Состояние» возможно просмотреть и задать состояния на устройство, подробное описание которых приведено в таблице (Таблица 3).

Таблица 3

Название группы политик / состояний	Описание	Доступные значения
Свойства		
Настройки Сервиса уведомлений Аврора		
ID приложения	Идентификатор клиентского приложения, с которым клиентское приложение «Аврора Центр» регистрируется в ПСУ	Пример: `int_mobile_buggmfjginaqssnmf07g`
Адрес	IP-адрес или имя хоста ПСУ для клиентского приложения «Аврора Центр»	Пример: 95.181.193.6
Порт	Номер порта для подключения клиентского 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

Название группы политик / состояний		Описание	Доступные значения
	CRL: Проверка отзыва сертификата	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»
	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`
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	

Название группы политик / состояний		Описание	Доступные значения
Расписание отправки событий безопасности		Расписание отправки сообщений о событиях безопасности, произошедших на устройстве	
Исключения событий безопасности		Уровень событий безопасности процесса, которые не будут отправляться в Аврора Центр	Пример: «Информационное»
Хранение логов на устройстве		Тип хранения системных сообщений на устройствах	Возможные значения: – «Временное»; – «Постоянное»
	Корневые сертификаты (количество сертификатов)		
	Название сертификата	В столбце «Текущее»/«Целевое» отображается цифровой отпечаток (Fingerprint) доверенного сертификата	Пример: 1a245f158147714f93d04428a6b5593fc0ea88de
	Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат	Пример: OMP
	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:
Снимки экрана		Разрешение или запрет на создание снимков экрана	

Название группы политик / состояний	Описание	Доступные значения
Управление датой и временем	Разрешение или запрет на внесение изменений в настройки даты и времени	– «Разрешен(но)»; – «Запрещен(но)». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
Режим разработчика	Разрешение или запрет на использование режима разработчика	
Сброс к заводским настройкам	Разрешение или запрет на сброс устройства к заводским настройкам	
Использование микрофона	Разрешение или запрет на использование микрофона	
Голосовые вызовы		
Исходящие вызовы	Разрешение или запрет выполнения исходящих звонков с устройства	Возможные значения: – «Разрешены»; – «Запрещены». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
Входящие вызовы	Разрешение или запрет принятия входящих на устройства вызовов	Возможные значения: – «Разрешены»; – «Запрещены». Если значение целевого состояния устройства не отправлено, отображается «Не задано»

Название группы политик / состояний		Описание	Доступные значения
Параметры устройства			
	Память (список хранилищ устройств)		
	Общий объем	Общий объем модуля памяти устройства	Размер в 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». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
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	

Название группы политик / состояний			Описание	Доступные значения
	WLAN			
	Работа WLAN		Разрешение или запрет на использование сети WLAN	Возможные значения: – «Включен»; – «Выключен». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	Управление WLAN		Разрешение или запрет изменения состояния адаптера сети WLAN	Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	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
	WLAN MAC		MAC-адрес WLAN устройства	Пример: 00:02:50:c0:2b:20
		Подключения (созданные на устройствах подключение к сети WLAN)		
		Название беспроводной сети (Service Set Identifier) для подключения		
		Скрытая сеть	Определяет, транслируется ли название беспроводной сети	Возможные значения: – «Да»; – «Нет»

Название группы политик / состояний			Описание	Доступные значения
		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: s2YaBGWeY4MRyDrqh60nNc6lw4yEBtgLGxukl7dylV8
		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	Например: WI-FI-сеть
		Идентификатор	Идентификатор пользователя для подключения к беспроводной сети. **ПРИМЕЧАНИЕ**. Отображается для сети с WPA-EAP	Например: ivanov@omp.ru

Название группы политик / состояний		Описание	Доступные значения
	VPN		
	Подключения		
	Название (тип подключения)	Название подключения VPN (тип подключения Cisco AnyConnect или КриптоПро NGate R2)	Например: Test
	Адрес сервера	Адрес сервера VPN	Например: 1.1.1.1
	Тип	Тип соединения VPN	Возможные значения: – Cisco AnyConnect; – КриптоПро NGate R2
	Протокол (доступно для типа Cisco AnyConnect)	Протокол безопасности соединения VPN. Доступен только один протокол безопасности - SSL	SSL
	Категория сертификата (доступно для типа Cisco AnyConnect)	Название категории пользовательских сертификатов, в рамках которой выпущен сертификат для подключения VPN	Например: `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	Например: `ivanivanov`
	Автозапуск VPN (доступно для типа КриптоПро NGate R2)	Переключатель для автоматического подключения устройства к VPN	

Название группы политик / состояний		Описание	Доступные значения
	Хэш серийного номера лицензии (доступно для типа КриптоПро NGate R2)	Хэш-значение серийного номера лицензии пользователя	Например: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». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	Работа Bluetooth	Разрешение или запрет возможности использования Bluetooth®	Возможные значения: – «Включен»; – «Выключен». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	Геопозиция		
	Режим работы	Режим работы геопозиционирования	Возможные значения: – Не задано; – Выключено; – Пользовательские настройки; – Сохранение заряда аккумулятора;

Название группы политик / состояний		Описание	Доступные значения
			– Только спутники; – Высокая точность
	Изменение настроек	Разрешение или запрет на внесение изменений в настройки геопозиционирования	Возможные значения: – «Включен»; – «Выключен». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	Работа геопозиции (GPS модуль)	Разрешение или запрет возможности внесения изменений в настройки геопозиции	Возможные значения: – «Включена»; – «Выключена». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	AGPS	Наличие и отсутствие AGPS-модуля, если он есть на устройствах	Возможные значения: – «Доступен»; – «Недоступен»
	Активность AGPS	Активность AGPS-модуля при его наличии на устройствах	Возможные значения: – «Включен»; – «Выключен». Если значение целевого состояния устройства не отправлено, отображается «Не задано»

Название группы политик / состояний			Описание	Доступные значения
	GPS-координаты		Географические координаты устройства (широта и долгота)	Пример: 55.739604, 37.496983
	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». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
		Защищена PIN-кодом	Защита SIM-карты PIN-кодом	
		Голосовые вызовы	Разрешение или запрет голосовых вызовов	Возможные значения: – «Разрешена(ны)»; – «Запрещена(ны)». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
		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	

Название группы политик / состояний		Описание	Доступные значения
Управление приложениями			
Установка приложений		Разрешение или запрет установки клиентского приложения на устройства	Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
	Приложения		
	Витрина	В разделе текущего состояния отображается название витрины установленного клиентского приложения на устройстве. В разделе целевого состояния отображается название витрины клиентского приложения, указанного в политике, назначенной на устройствах	Название витрины. Если витрина не выбрана, отображается «Не задано»
	Наименование	В разделе текущего состояния отображается наименование установленного клиентского приложения на устройстве. В разделе целевого состояния отображается название клиентского приложения, указанного в политике, назначенной на устройствах	Пример: «Документы». Если клиентское приложение не установлено, отображается «Не задано». Пример: «Документы». Если политика не назначена на устройства, отображается «Не задано»

Название группы политик / состояний		Описание	Доступные значения
	Версия	В разделе текущего состояния отображается версия установленного клиентского приложения на устройстве. В разделе целевого состояния отображается версия клиентского приложения, указанного в политике, назначенной на устройствах	Пример: 10.68. Если клиентское приложение не установлено, отображается «Не задано» Пример: 10.68. Если политика не назначена, отображается «Не задано»
	Автозапуск	Определяет включение автозапуска приложения	Возможные значения: – «Не задано»; – «Да»; – «Нет»
Дистрибутив ОС			
ОС		Название ОС	Пример: Аврора
Версия ОС		Номер версии ОС	Пример: 3.2.3.15
Вариант ОС		Название варианта ОС	Пример: omp
Дата сборки		Дата сборки дистрибутива ОС	Пример: 22.11.2019 10:32
Обновление ОС		Разрешение или запрет обновления ОС Аврора	Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»
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
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	Например: OCSEMM
Фингерпринт	Цифровой отпечаток (Fingerprint) сертификата	Например: 1a245f158147714f93d04428a6b5593fc0ea88de
Хэш-алгоритм запроса	Алгоритм хэширования	Например: sha512

Название группы политик / состояний			Описание	Доступные значения
	Тип шифрования и длина ключа		Алгоритм шифрования приватного ключа	Например: 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	Например: 11223344
Приложения			Названия пакетов приложений, которые будут доступны пользователю в режиме киоска	Например: com.android.chrome
	Ярлыки веб-страниц			
	Название ярлыка		Названия ярлыка веб-страницы	Например: omp
	URL		Электронный адрес сайта/веб-страницы в формате URL	Например: https://www.omp.ru/

2.1.1.3. Вкладка «Управление»

Во вкладке «Управление» отображается список правил из назначенных на устройство политик, офлайн-сценариев и оперативных команд (Рисунок 16 [1]), а также в случае конфликта правил отображается действующее правило (Рисунок 16 [2]).

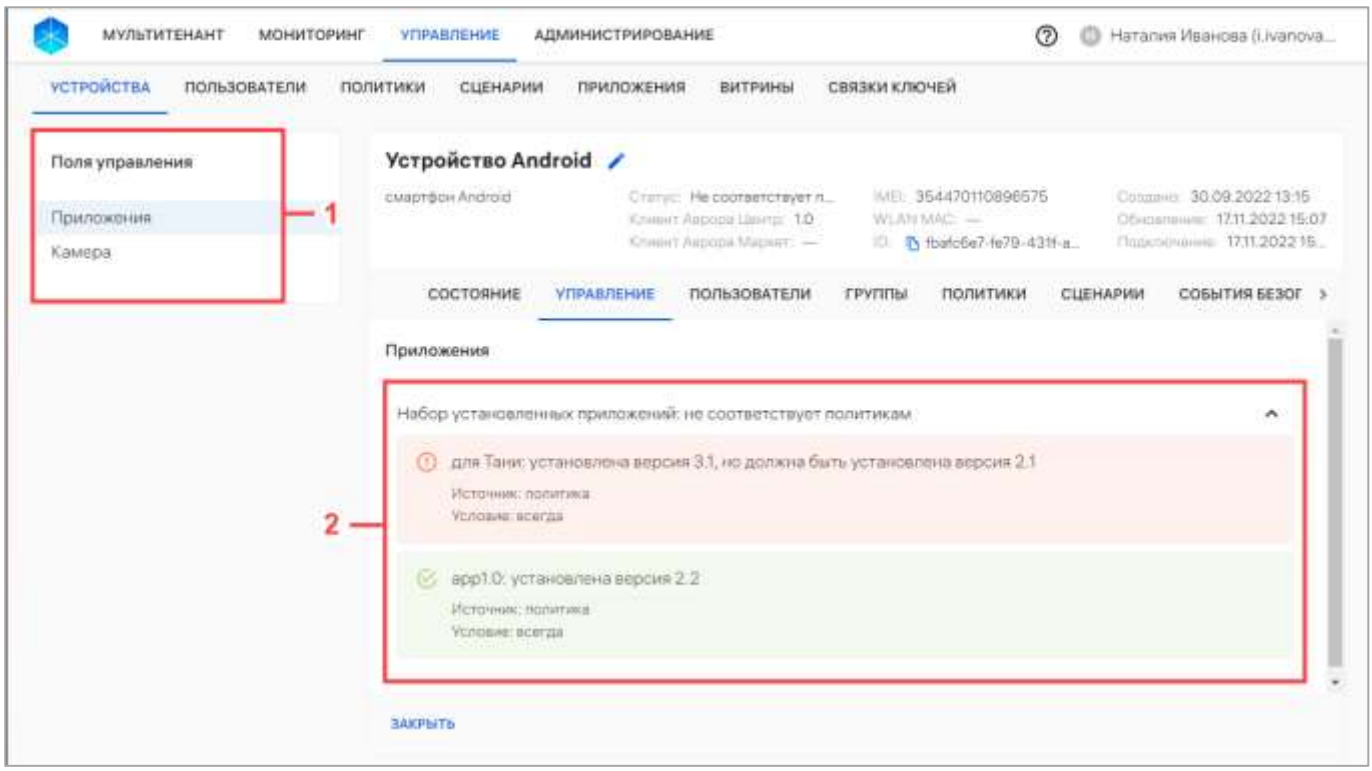

Рисунок 16

ПРИМЕЧАНИЕ. Одновременно назначенные на устройство правила имеют следующий приоритет:

1) Оперативная команда;

2) Офлайн-сценарий;

3) Политика.

2.1.1.4. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список привязанных к устройству пользователей (Рисунок 17).

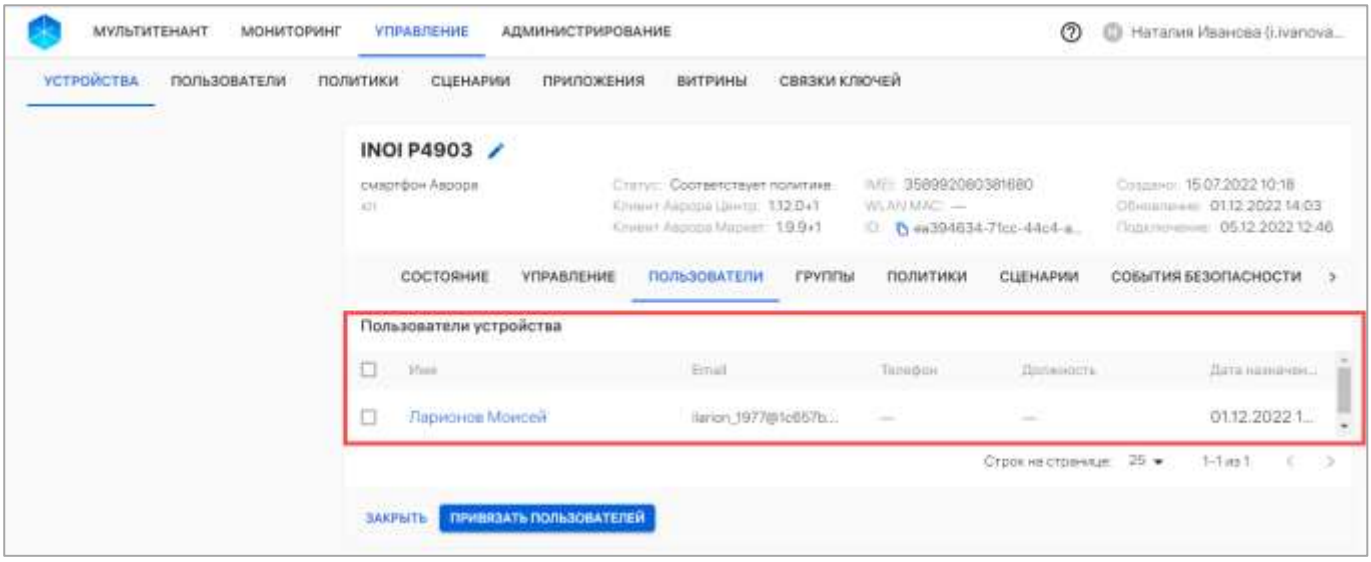

Рисунок 17

Информация о пользователях отображается в следующих столбцах:

– «Имя» — фамилия, имя и отчество пользователя;

– «Email» — рабочая почта пользователя;

– «Телефон» — номер телефона пользователя;

– «Должность» — должность пользователя;

– «Дата назначения» — дата и время привязки устройства к пользователю.

Список пользователей сортируется по дате обновления информации о пользователях устройства.

Устройство можно привязать к пользователю из карточки с помощью кнопки «Привязать к пользователю» (пп. 2.2.5.2).

Фамилия, имя и отчество пользователя представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке пользователя (п. 2.1.3).

При отсутствии привязанных к устройству пользователей отображается сообщение «Устройство не привязано ни к одному пользователю».

2.1.1.5. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к устройству групп устройств (Рисунок 18).

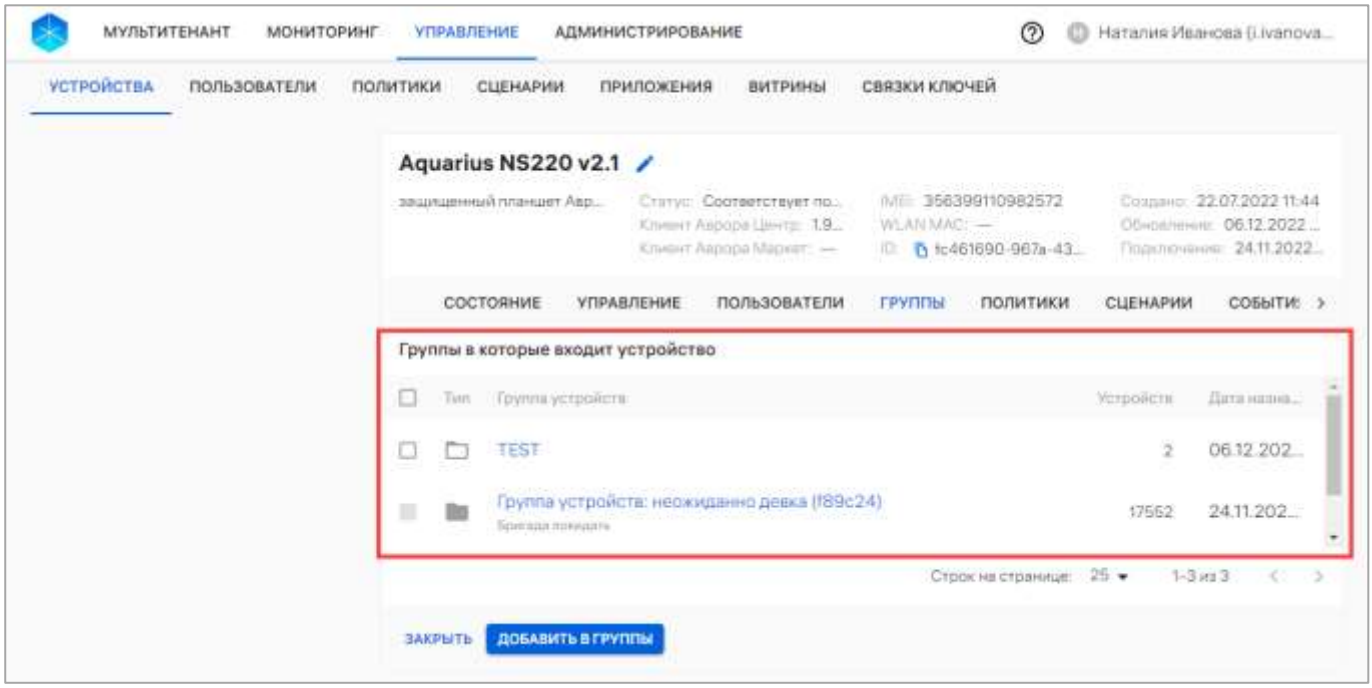

Рисунок 18

Информация о группах пользователей отображается в следующих столбцах:

– «Тип» - Тип группы:

- Динамическая группа – группа, в которую устройства добавляются автоматически согласно выбранному алгоритму добавления;
- Статическая группа - группа, в которую можно добавлять отдельные устройства;

– «Группа устройств» — название группы устройств и комментарий (при наличии);

– «Устройств» — количество устройств в данной группе устройств;

– «Дата назначения» — дата и время добавления устройств в группу устройств.

Устройства можно привязать к группе устройств с помощью кнопки «Добавить в группы», выполнив действия, приведенные в пп. 2.2.6.2.

Название группы устройств представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы устройств (п. 2.1.2).

2.1.1.6. Вкладка «Политики»

Во вкладке «Политики» отображается список назначенных на устройство политик и его правил (Рисунок 19).

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 19 [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 19 [2]), при нажатии на которую осуществляется переход к карточке группы.

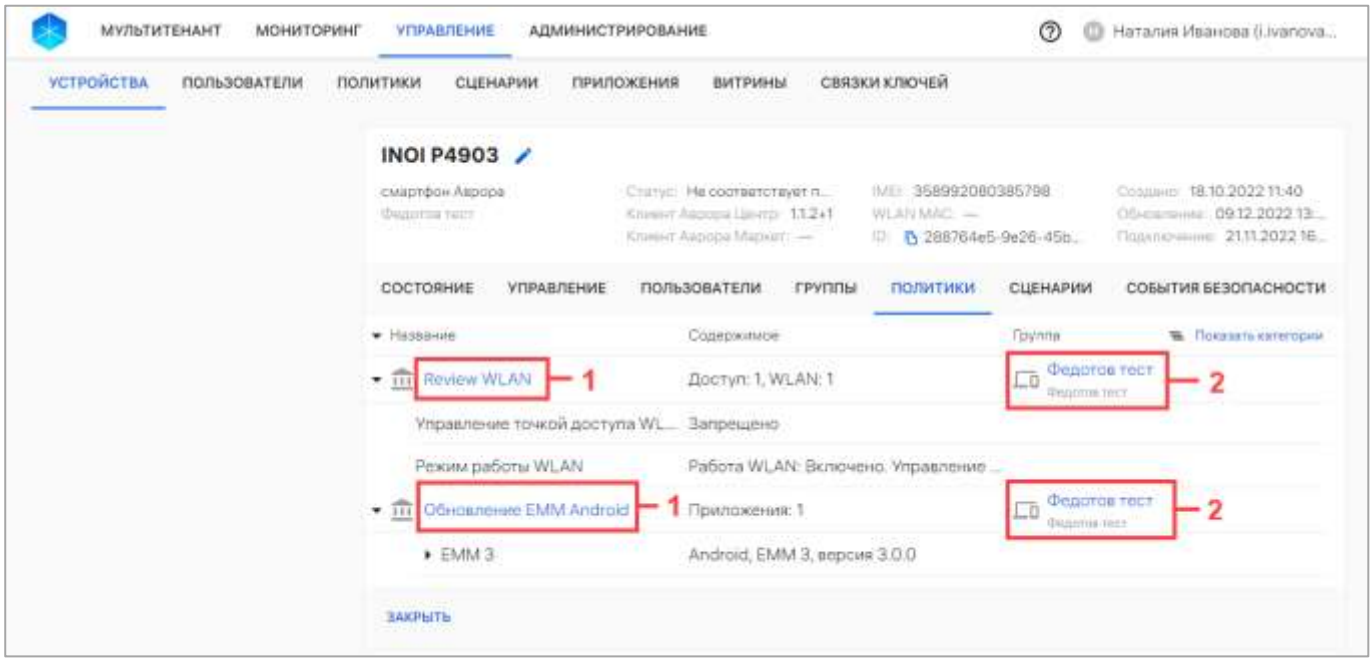

Рисунок 19

При отсутствии политик, назначенных на группу устройств/пользователей, в которую входит данное устройство, отображается сообщение «На устройство не назначено ни одной политики». Подробное описание назначения политики на группу устройств приведено в пп. 2.4.5.2.

2.1.1.7. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается следующий список:

– офлайн-сценарии, назначенные на устройство (Рисунок 20 [1]);

– бизнес-сценарии, выполняющиеся на устройстве (Рисунок 20 [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) и архивируется (пп. 2.2.13).

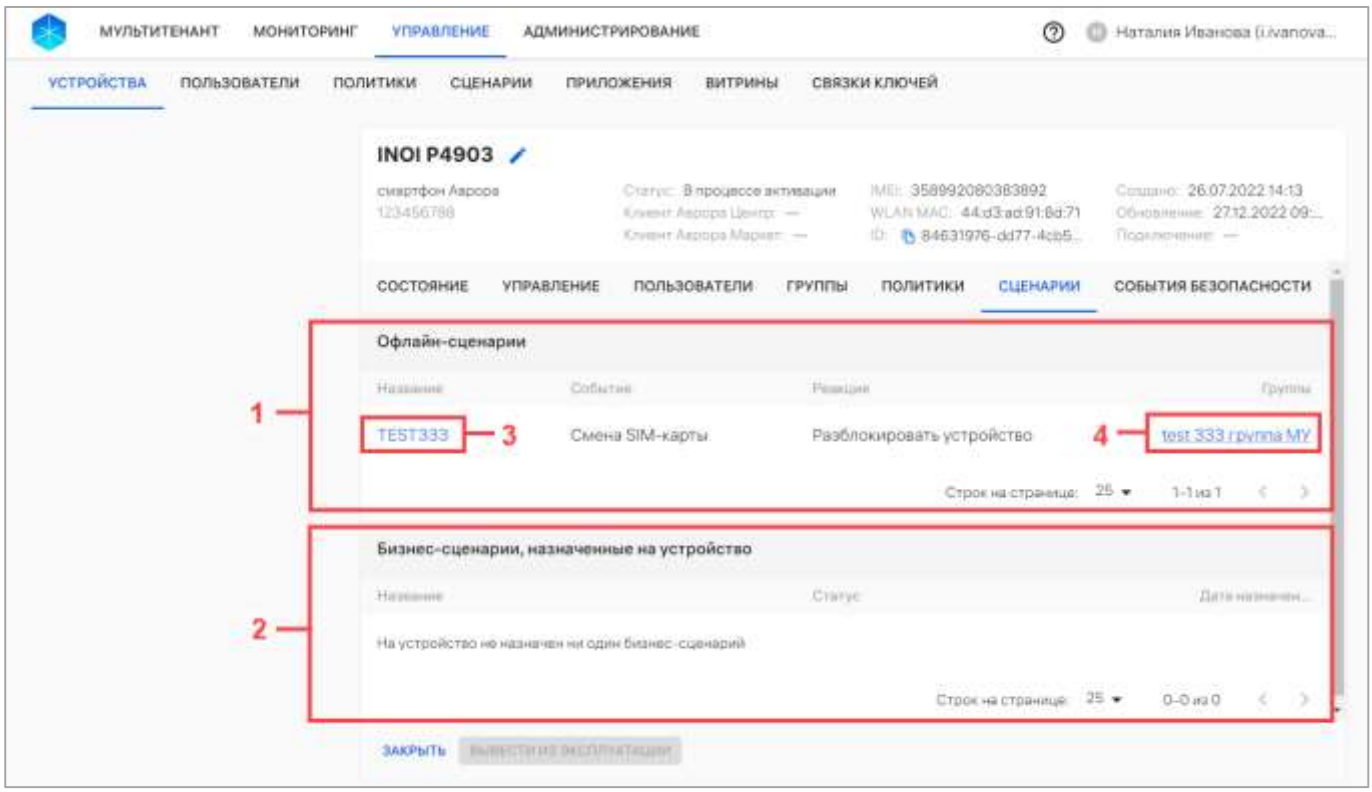

Рисунок 20

Информация об офлайн-сценариях и о бизнес-сценариях отображается в столбцах, приведенных в таблице (Таблица 4).

Таблица 4

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 (Рисунок 20 [3]), при нажатии на которую осуществляется переход к карточке офлайн-сценария (п. 2.1.6)
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 (Рисунок 20 [4]), при нажатии на которую осуществляется переход к карточке группы (п. 2.1.2, п. 2.1.4)
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

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-сценария на группу устройств/пользователей приведено в п. 2.5.2.

При отсутствии на устройстве бизнес-сценариев отображается сообщение «На устройство не назначен ни один бизнес-сценарий».

2.1.1.8. Вкладка «События безопасности»

Во вкладке «События безопасности» отображается список произошедших на устройстве событий безопасности (Рисунок 21), который при разборе инцидентов позволяет определить, что происходило на устройстве.

Для получения события безопасности необходимо воспользоваться оперативной командой «Расписание отправки событий безопасности» (п. 2.2.8) или политикой с правилом «Конфигурация/Расписание отправки событий безопасности» (пп. 2.4.5.2).

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

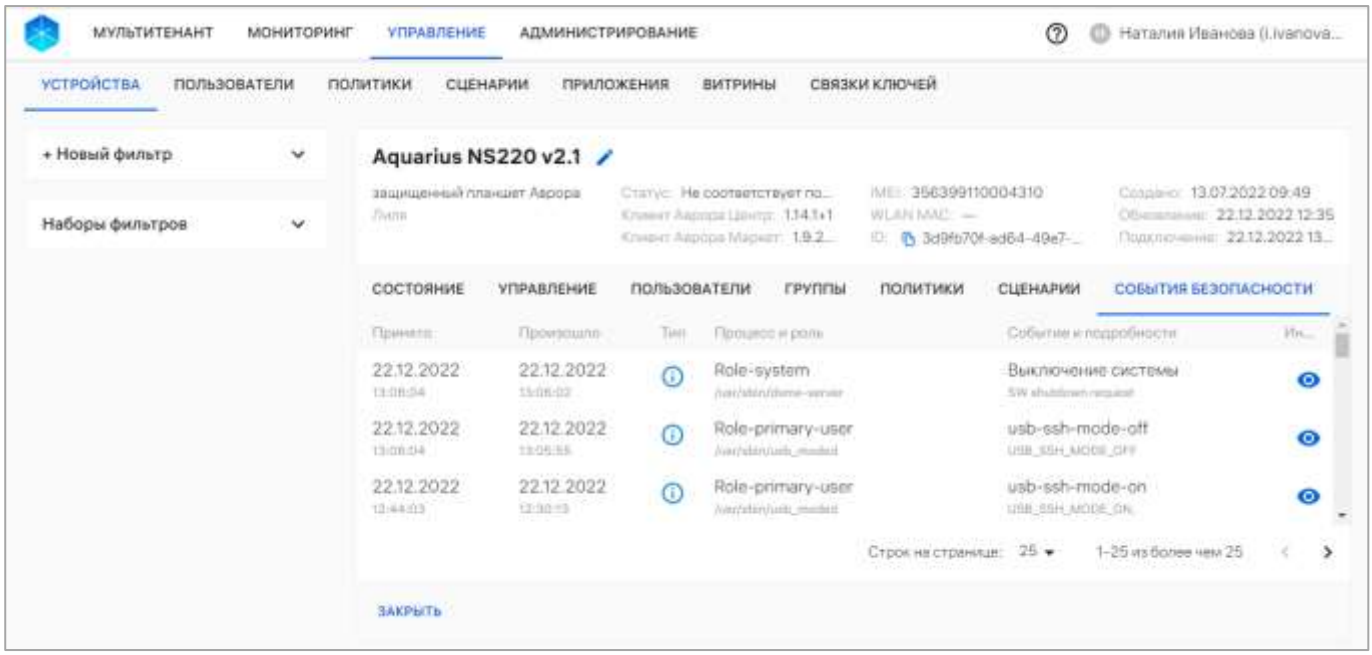

Рисунок 21

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, приведенные в таблице (Таблица 5).

Таблица 5

Параметр	Описание
Принято	Дата и время поступления события на устройства
Произошло	Дата и время выполнения события на устройствах

Параметр	Описание
Тип	Тип сообщения о событии в зависимости от важности: – «Информационное»; – «Предупреждение»; – «Критическое»; – «Отладочное»
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 содержания сообщения о событии необходимо нажать значок «Содержание сообщения» в столбце «Инфо» (Рисунок 22).

Для копирования текста сообщения в буфер обмена необходимо нажать кнопку «Копировать». Для закрытия сообщения необходимо нажать кнопку «Закрыть».

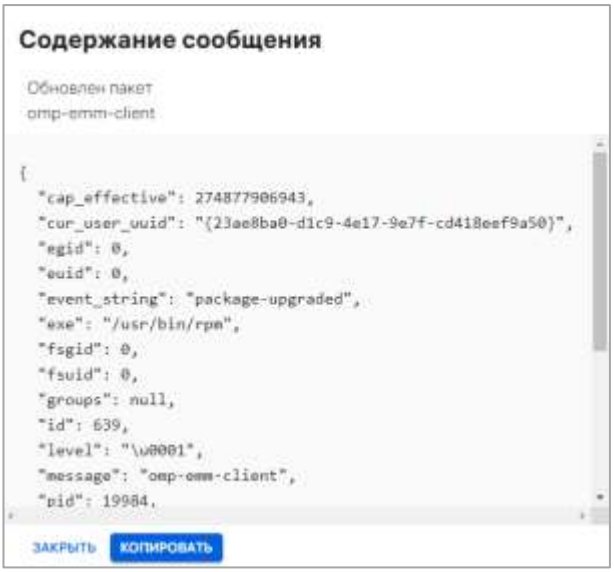

Рисунок 22

При отсутствии событий на устройстве отображается сообщение «Нет данных».

Для завершения просмотра карточки устройства и возврата к списку устройств необходимо нажать копку «Закрыть» (см. Рисунок 21).

2.1.1.9. Вкладка «Приложения»

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

Информация о приложениях отображается в столбцах (Рисунок 23 [1], Таблица 22), приведенных в таблице (Таблица 6).

Таблица 6

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, то ячейка не заполняется
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, то ячейка не заполняется
Политика	Название политики, по правилу которой было установлено приложение. Название политики выделено цветом и представляет собой активную ссылку (Рисунок 23 [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 24) при нажатии значка 👁 «Дополнительная информация» (Рисунок 23 [3])

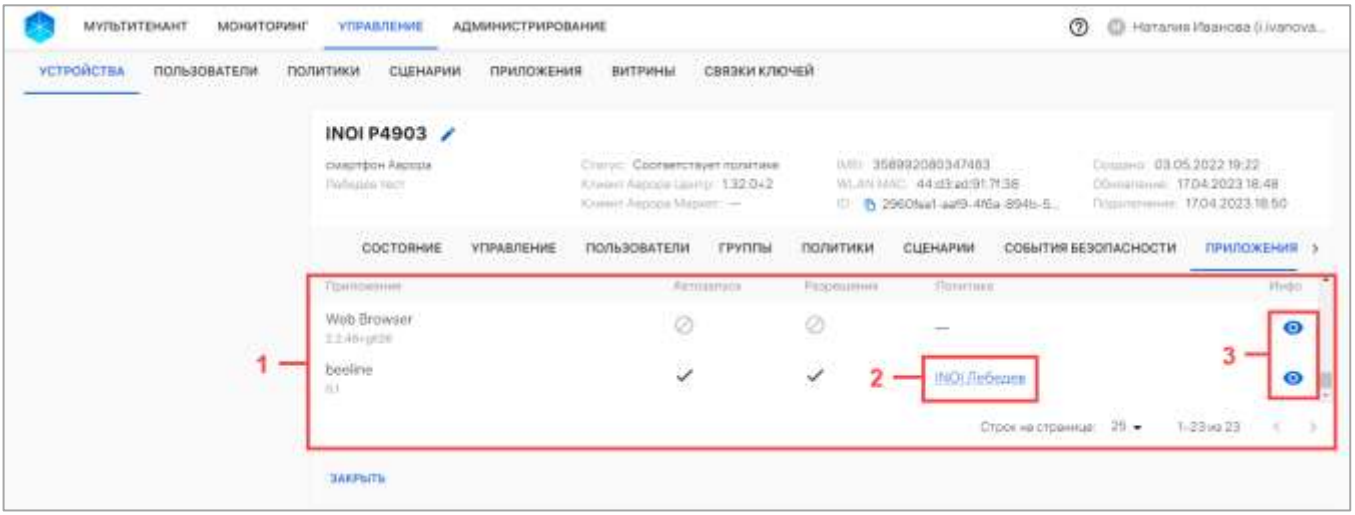

Рисунок 23

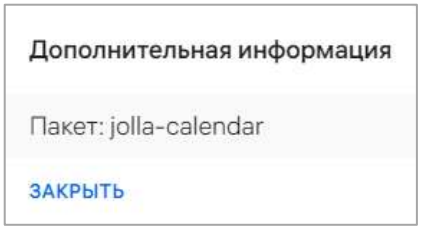

Рисунок 24

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»;

– выбрать группу устройств.

В результате откроется карточка группы устройств, интерфейс которой включает следующие элементы:

– шапка карточки (Рисунок 25 [1]);

– вкладки карточки. В карточке группы устройств доступен переход к следующим вкладкам (Рисунок 25 [2]):

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

- «Сценарии» (пп. 2.1.2.4).

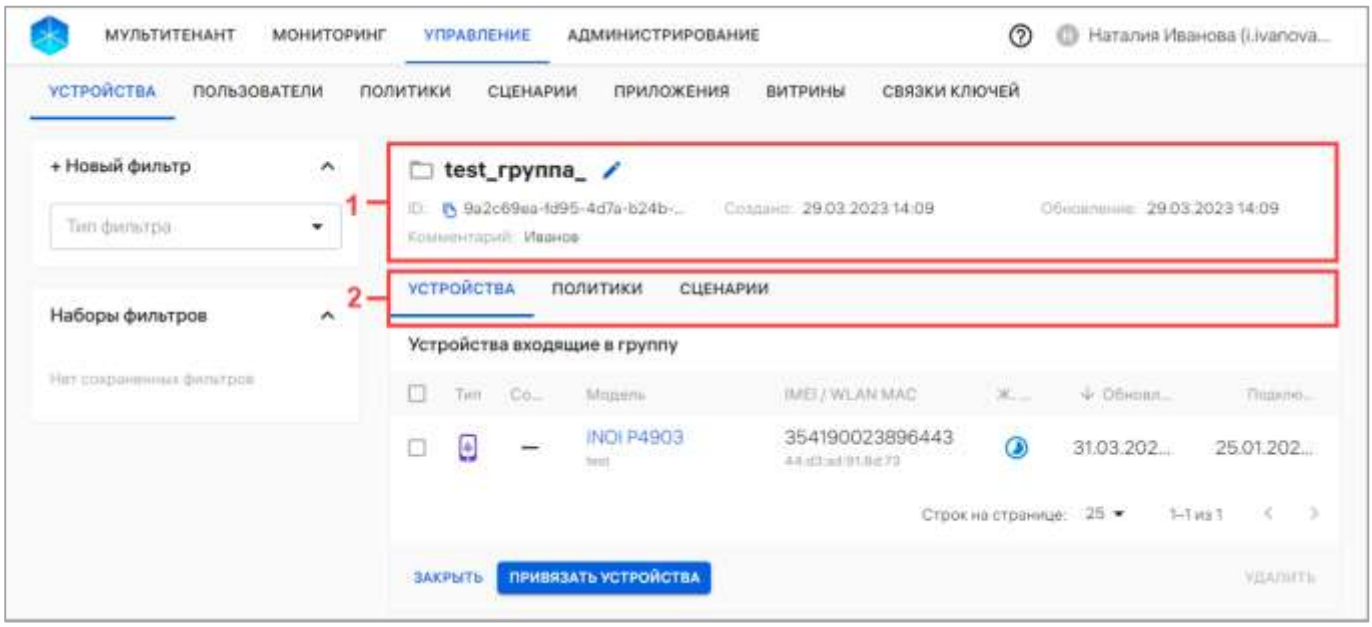

Рисунок 25

2.1.2.1. Шапка карточки

В шапке карточки группы устройств отображается название и тип группы устройств, а также следующая информация (см. Рисунок 25 [1]):

– «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» — комментарий, добавленный при создании группы устройств.

Для редактирования группы устройств необходимо выполнить следующие действия:

– нажать на значок «Редактировать» (см. Рисунок 25 [1]);

– отобразится окно «Редактирование группы устройств» (Рисунок 26);

– отредактировать имя группы устройств и/или комментарий к группе;

– сохранить изменения либо отменить действия.

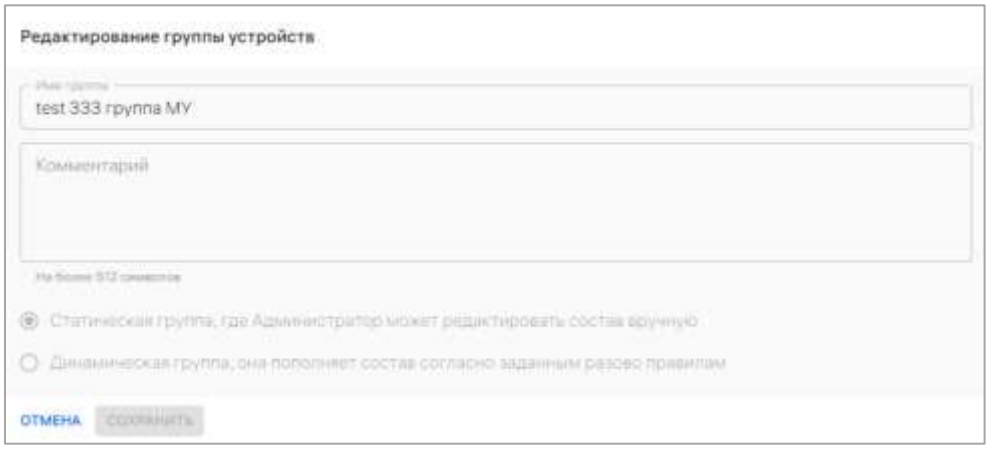

Рисунок 26

В результате успешного сохранения данные в шапке карточки группы устройств обновятся.

2.1.2.2. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к группе устройств (Рисунок 27 [1]), а при его отсутствии отображается сообщение «Группа не содержит устройств». Подробное описание привязки устройств к группе устройств из карточки группы устройств приведено в пп. 2.2.6.3.

При необходимости для поиска устройств возможно применение фильтров. Описание фильтров и процесса поиска приведено в подразделе 1.5.

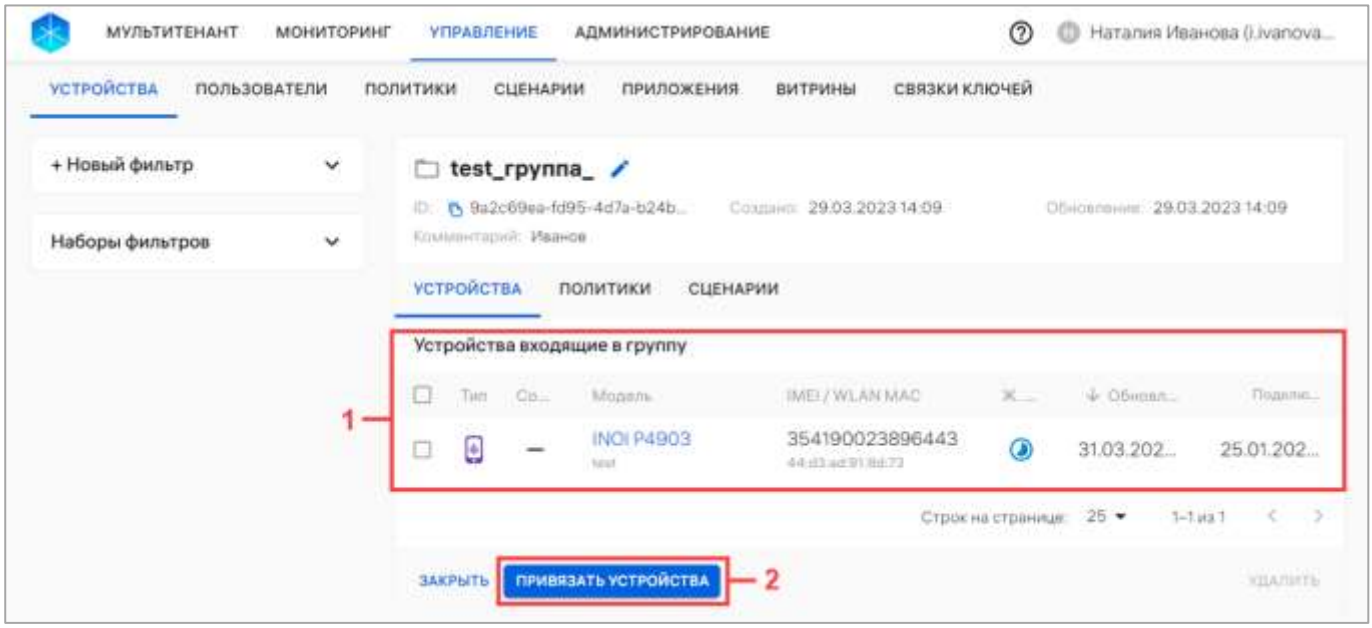

Рисунок 27

Информация по каждому устройству отображается в столбцах, приведенных в таблице (Таблица 7).

Таблица 7

<table>
<tr><th>Параметр</th><th colspan="2">Описание</th></tr>
<tr><td>Тип</td><td colspan="2">Тип устройства может иметь одно из следующих наименований:
– смартфон Аврора/защищенный смартфон Аврора;
– планшет Аврора/защищенный планшет Аврора;
– КПК Аврора;
ВНИМАНИЕ! ОС Android, а также ОС семейства Linux, в комплект поставки не входят</td></tr>
<tr><td>Соответствие</td><td colspan="2">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</td></tr>
<tr><td rowspan="2">Модель</td><td>Модель устройства</td><td>Название модели устройства представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку устройства</td></tr>
<tr><td>Комментарий</td><td>Дополнительная информация. Заполняется при необходимости</td></tr>
<tr><td>IMEI/WLAN MAC</td><td colspan="2">– IMEI устройства;
– MAC-адрес WLAN устройства</td></tr>
<tr><td>Ж. Цикл</td><td colspan="2">Статус жизненного цикла устройства:
– «Зарегистрировано» — устройство добавлено в ПУ;
– «В процессе активации» — сгенерирован QR-код для устройств;
– «Активировано» — устройство активировано;
– «Очищено» — устройство очищено (сброшено к заводским настройкам);
– «Архивное» — устройство архивировано (удалено)</td></tr>
<tr><td>Обновлено</td><td colspan="2">Дата и время обновления данных устройств. Значение столбца отсортировано в направлении стрелки - от старых к новым, от новых к старым</td></tr>
<tr><td>Подключено</td><td colspan="2">Дата и время последнего подключения ПУ к Серверу приложений ПУ</td></tr>
</table>

Название модели устройства представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке устройства (п. 2.1.1).

Для редактирования списка устройств во вкладке «Устройства» необходимо нажать кнопку «Привязать устройства» (см. Рисунок 27 [2]) и выполнить действия, описанные в пп. 2.2.6.3.

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

2.1.2.3. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу устройств (Рисунок 28 [1]), а при его отсутствии отображается сообщение «На группу не назначена ни одна политика».

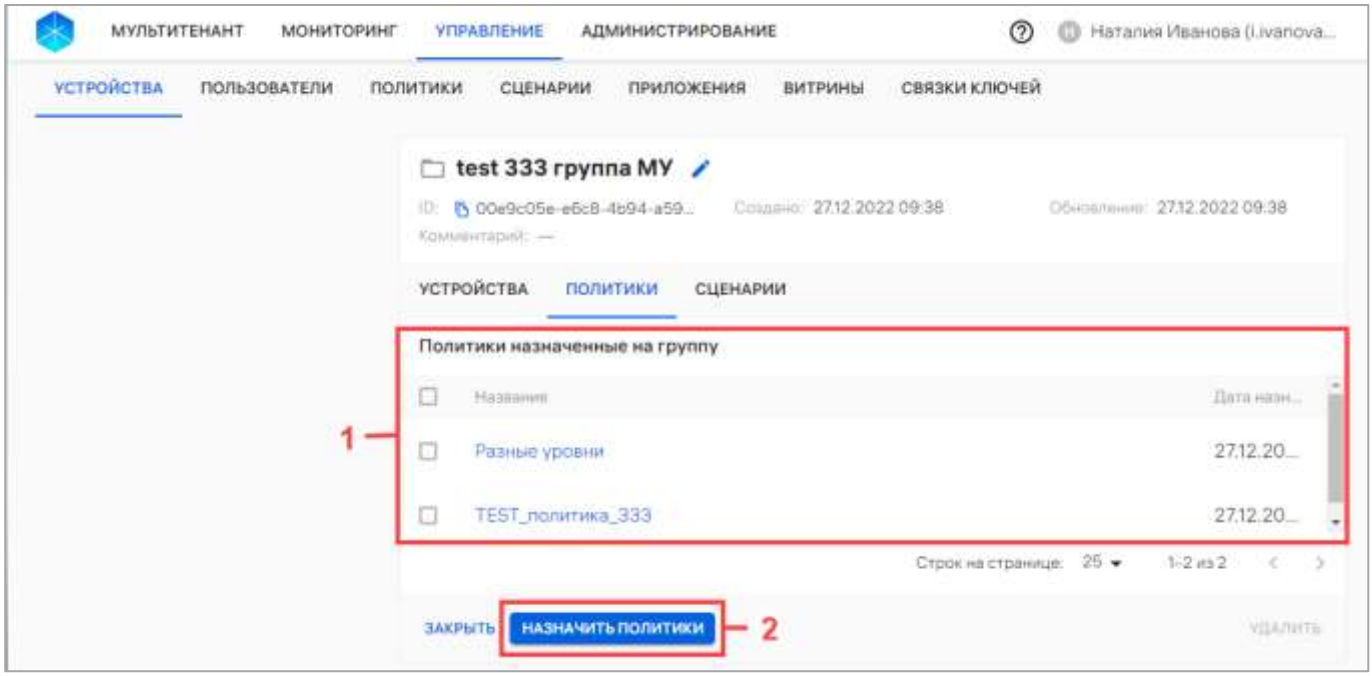

Рисунок 28

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.

Политика может быть назначена на группу устройств нажатием кнопки «Назначить политики» (Рисунок 28 [2]). Процесс назначения политики на группу устройств приведен в п. 2.4.5.2.

2.1.2.4. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу устройств (Рисунок 29), 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.

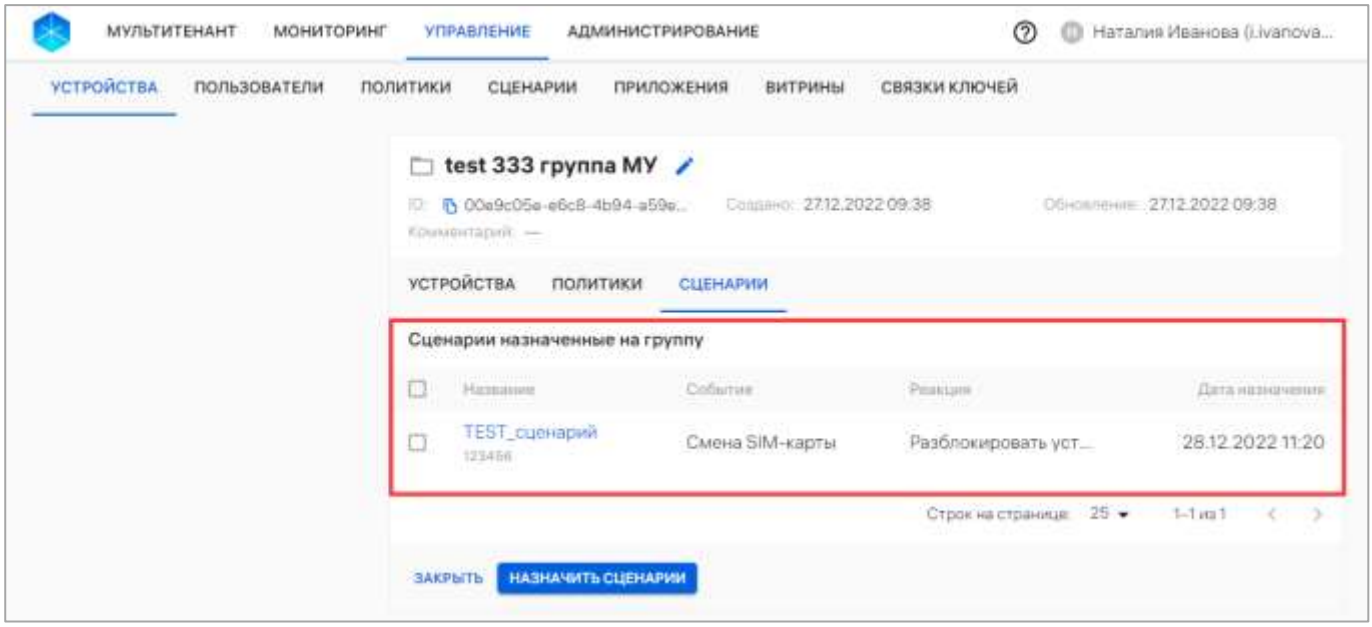

Рисунок 29

В рабочей области информация о назначенных офлайн-сценариях отображается в столбцах, приведенных в таблице (Таблица 8).

Таблица 8

Название столбца	Описание
Название	Название офлайн-сценария
	Комментарий – дополнительная информация к офлайн-сценарию
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 27)
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

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.

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 следующие элементы:

– шапка карточки (2.1.3.1);

– вкладки карточки. В карточке группы устройств доступен переход к следующим вкладкам:

- «Устройства» (пп. 2.1.3.2);
- «Группы» (пп. 2.1.3.3);
- «Политики» (пп. 2.1.3.4).

2.1.3.1. Шапка карточки

В шапке карточке пользователя отображается (Рисунок 30 [1]):

– фамилия, имя и отчество пользователя;

– «Email» - электронная почта пользователя;

– «Должность» - должность, занимаемая пользователем;

– «ID» — идентификатор пользователя, который можно скопировать, нажав кнопку «Копировать id пользователя в буфер обмена»;

– «Тел. рабочий» - рабочий телефон пользователя;

– «Создание» — дата и время добавления группы устройств;

– «Обновление» — дата и время последнего обновления группы устройств.

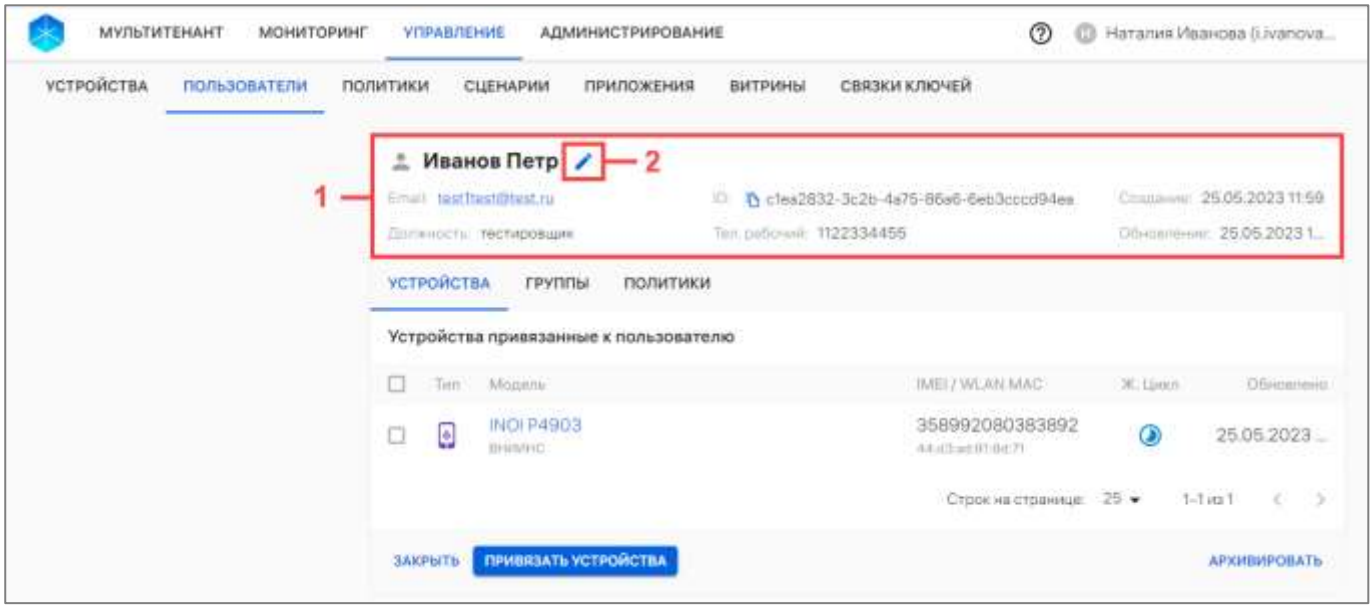

Рисунок 30

Для редактирования данных пользователя необходимо выполнить следующие действия:

– нажать значок «Редактировать» (Рисунок 30 [2]);

– в окне «Редактирование пользователя» внести необходимые изменения (Рисунок 31);

– сохранить изменения либо отменить действия.

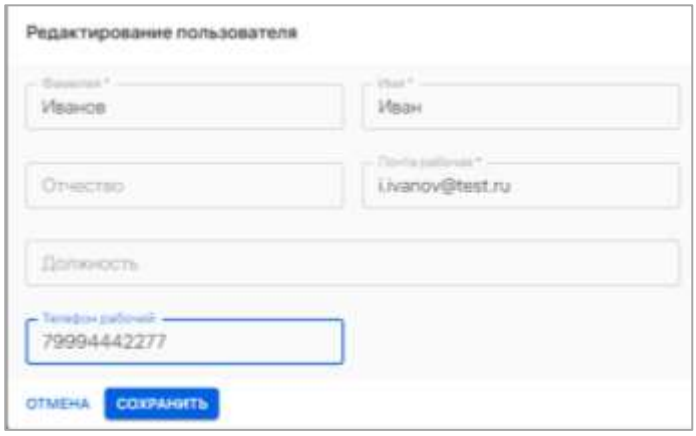

Рисунок 31

В результате успешного сохранения отобразится сообщение «Данные пользователя обновлены».

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).

2.1.3.2. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к пользователю (Рисунок 32 [1]).

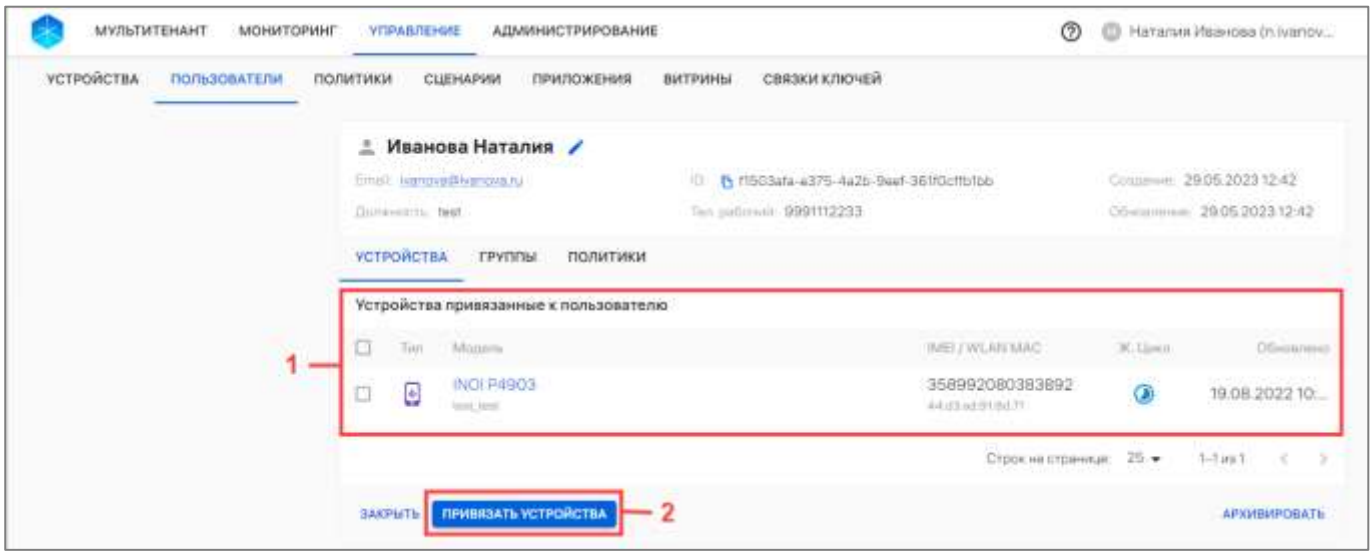

Рисунок 32

Информация об устройствах отображается в столбцах, приведенных в таблице (Таблица 9).

Таблица 9

Параметр	Описание
Тип	Тип устройства может иметь одно из следующих наименований: – смартфон Аврора/защищенный смартфон Аврора; – планшет Аврора/защищенный планшет Аврора; – КПК Аврора. **ВНИМАНИЕ!** ОС Android, а также ОС семейства Linux, в комплект поставки не входят
Модель	Модель устройства — название модели устройства, представляющее собой активную ссылку, при нажатии на которую осуществляется переход к карточке устройства
	Комментарий — дополнительная информация
IMEI/WLAN MAC	– IMEI устройства; – MAC-адрес WLAN устройства
Ж. Цикл	Статус жизненного цикла устройства: – «Зарегистрировано» — устройство добавлено в ПУ; – «В процессе активации» — сгенерирован QR-код для устройства; – «Активировано» — устройство активировано; – «Очищено» — устройств очищено (сброшено к заводским настройкам); – «Архивное» — устройств заархивировано (удалено)
Обновлено	Дата и время обновления данных устройств. Значение столбца отсортировано в направлении стрелки - от старых к новым, от новых к старым

Название модели устройства представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке устройства (п. 2.1.1).

Для редактирования списка устройств во вкладке «Устройства» необходимо нажать кнопку «Привязать устройства» (Рисунок 32 [2]) и выполнить действия, описанные в пп. 2.3.5.2.

При изменении списка устройств пользователя обновится. На все привязанные и отвязанные устройства будут применены новые перекомбинированные политики и офлайн-сценарии.

2.1.3.3. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к пользователю групп пользователей (Рисунок 33 [1]), а при отсутствии групп пользователей отображается сообщение «Пользователь не привязан ни к 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.

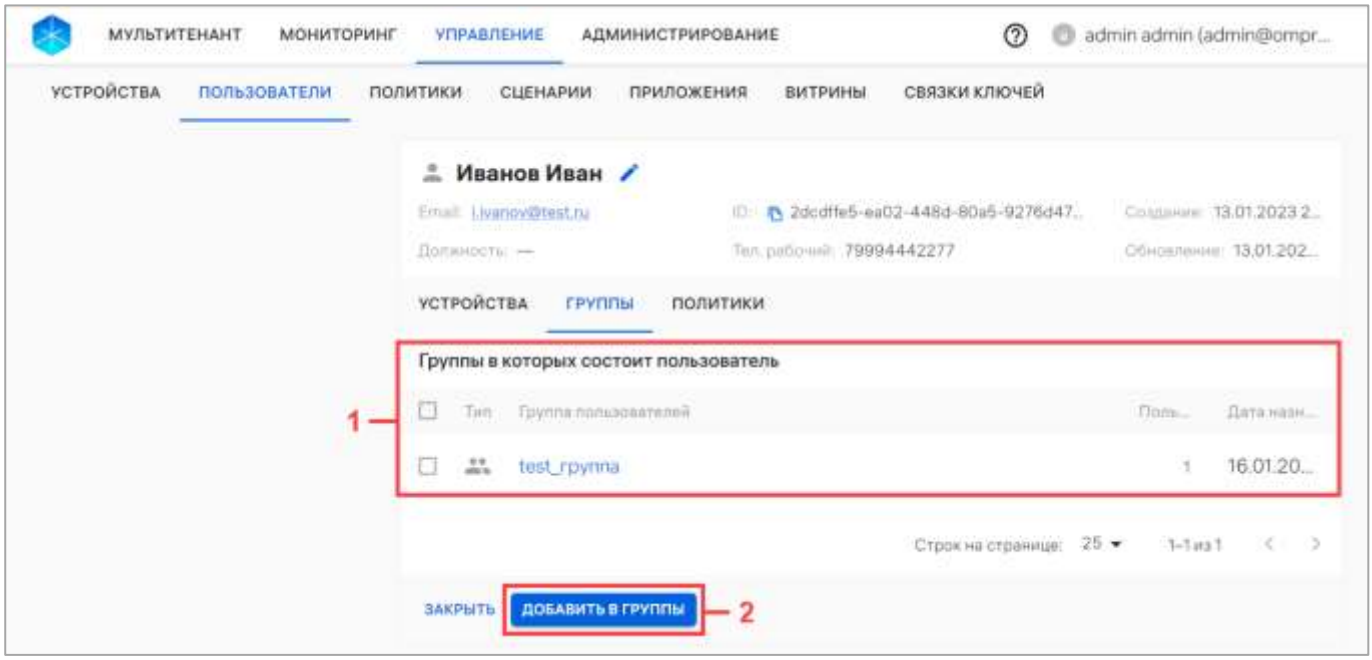

Рисунок 33

Информация о группах пользователей отображается в следующих столбцах:

– «Тип» — тип группы:

- — группа пользователей, созданная вручную или с помощью импорта CSV-файла;
- — организационное подразделение. Группа пользователей, полученная из LDAP;

– «Группа пользователей» — название группы пользователей, к которой привязан данный пользователь, и комментарий к группе (при наличии);

– «Пользователей» — количество участников группы;

– «Дата назначения» — дата и время привязки пользователя к группе. Значение столбца отсортировано в направлении стрелки - от старых к новым  , от новых к старым  .

2.1.3.4. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей, к которой привязан данный пользователь (Рисунок 34 [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 34):

– «Название» — название политики, назначенной на группу пользователей устройства, в которую входит текущий пользователь;

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

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

Название политики/группы пользователей представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке (п. 2.1.5 и 2.1.4).

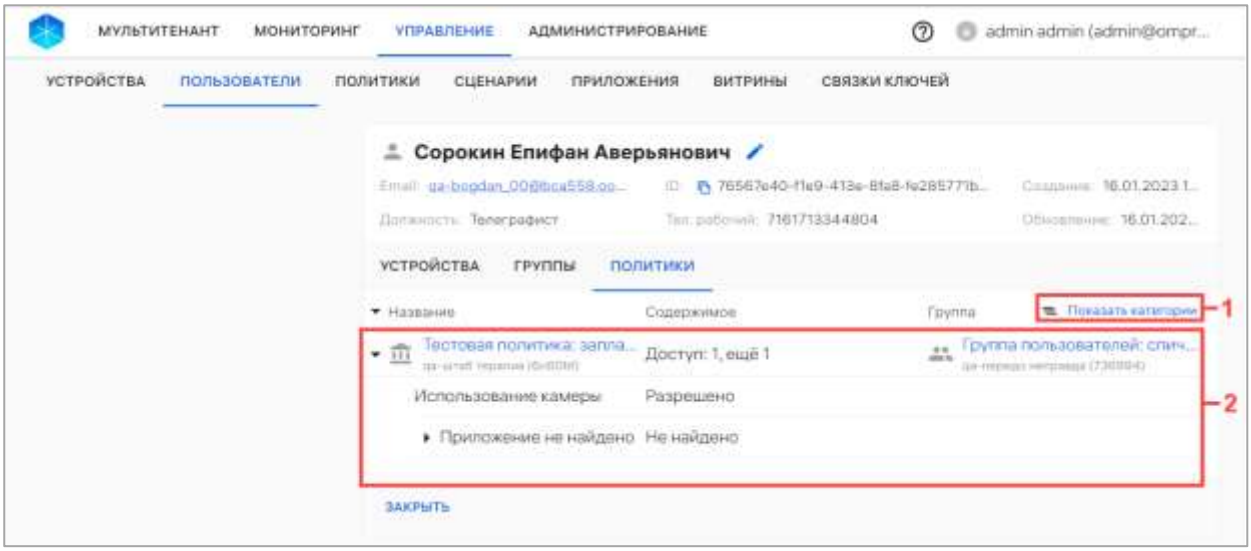

Рисунок 34

Для отображения категорий правил политик, назначенных на группу пользователей, необходимо нажать кнопку «Показать категории» (Рисунок 34 [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»;

– выбрать необходимую группу пользователей.

В результате откроется карточка группы пользователей, интерфейс которой включает следующие элементы (Рисунок 35):

– шапка карточки (пп. 2.1.4.1);

– вкладки карточки. В карточке группы пользователей доступен переход к следующим вкладкам:

- «Пользователи» (пп. 2.1.4.2);
- «Политики» (пп. 2.1.4.3);
- «Сценарии» (пп. 2.1.4.4).

2.1.4.1. Шапка карточки

В шапке карточки группы пользователей отображается название и тип группы пользователей, а также следующая информация (Рисунок 35 [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» — комментарий, добавленный при создании группы пользователей.

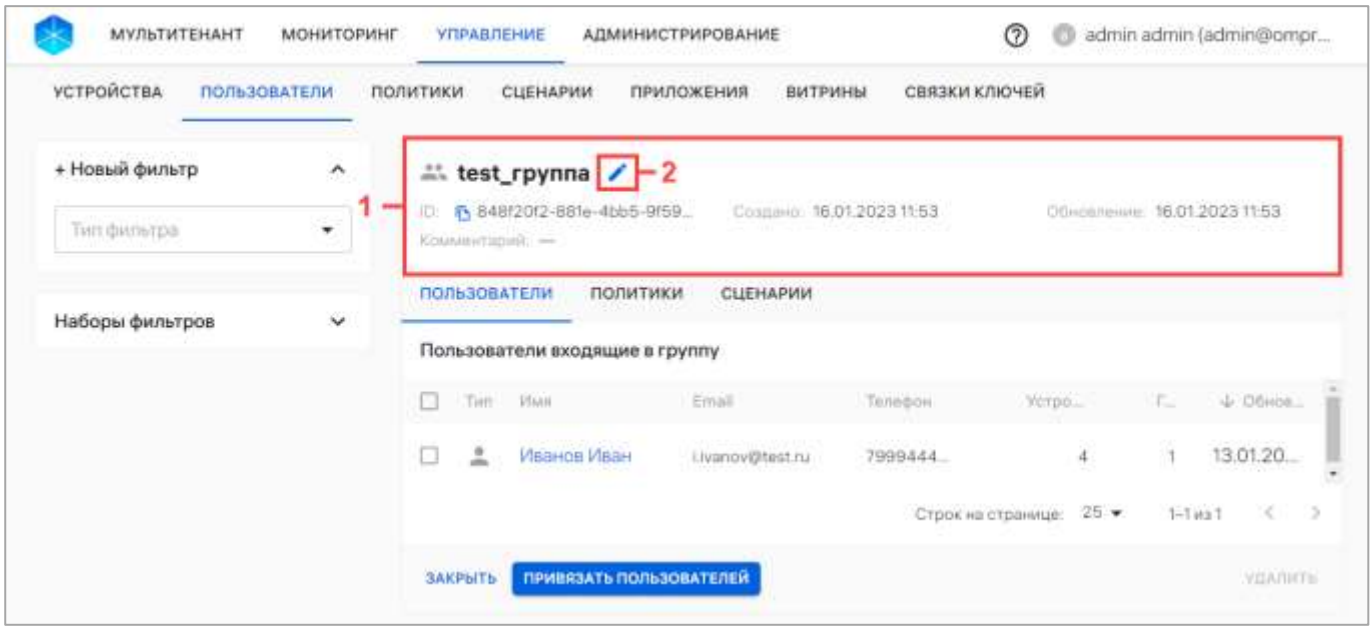

Рисунок 35

Для групп пользователей с типом «Группа пользователей» доступно редактирование названия и комментария.

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

Для редактирования группы пользователей типа «Группа пользователей» необходимо выполнить следующие действия:

– в шапке карточки нажать значок «Редактировать» (см. Рисунок 35 [2]);

– в окне редактирования группы пользователей внести изменения (Рисунок 36);

– сохранить изменения либо отменить действия.

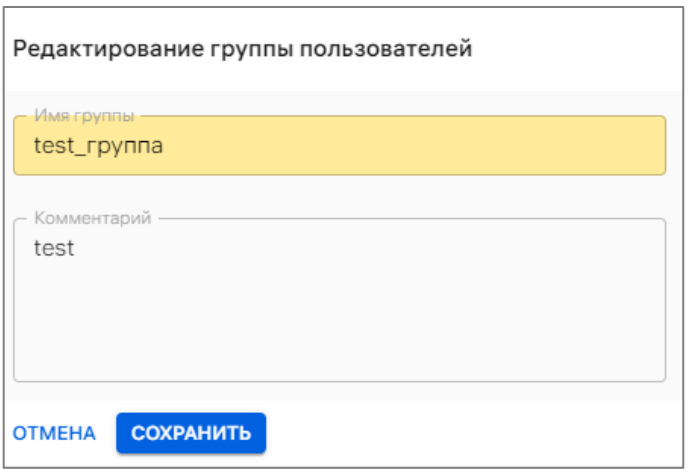

Рисунок 36

В результате сохранения данные в шапке карточки группы пользователей будут обновлены.

2.1.4.2. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список пользователей для данной группы пользователей (Рисунок 37 [1]).

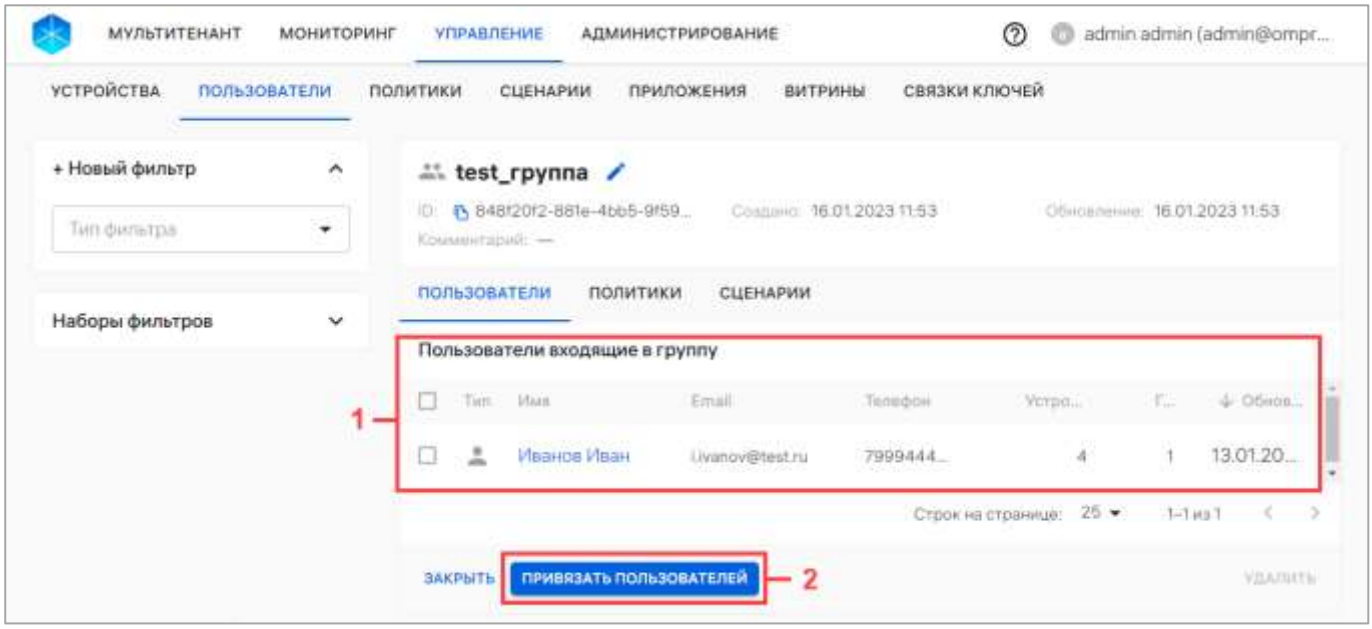

Рисунок 37

Информация о пользователях отображается в следующих столбцах:

– «Тип» — тип пользователей, входящих в группу:

- — пользователь;
- — пользователь из орг.подразделения;

– «Имя» — фамилия, имя и отчество пользователя;

– «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. Значение столбца отсортировано в направлении стрелки - от старых к новым , от новых к старым .

Фамилия, имя и отчество пользователя представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку пользователя (п. 2.1.3).

Для редактирования списка пользователей необходимо нажать кнопку «Привязать пользователей» (см. Рисунок 32 [2]) и выполнить действия, описанные в пп. 2.3.4.3.

2.1.4.3. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей (Рисунок 38 [1]), а при отсутствии списка отображается сообщение «На группу не назначена ни одна политика».

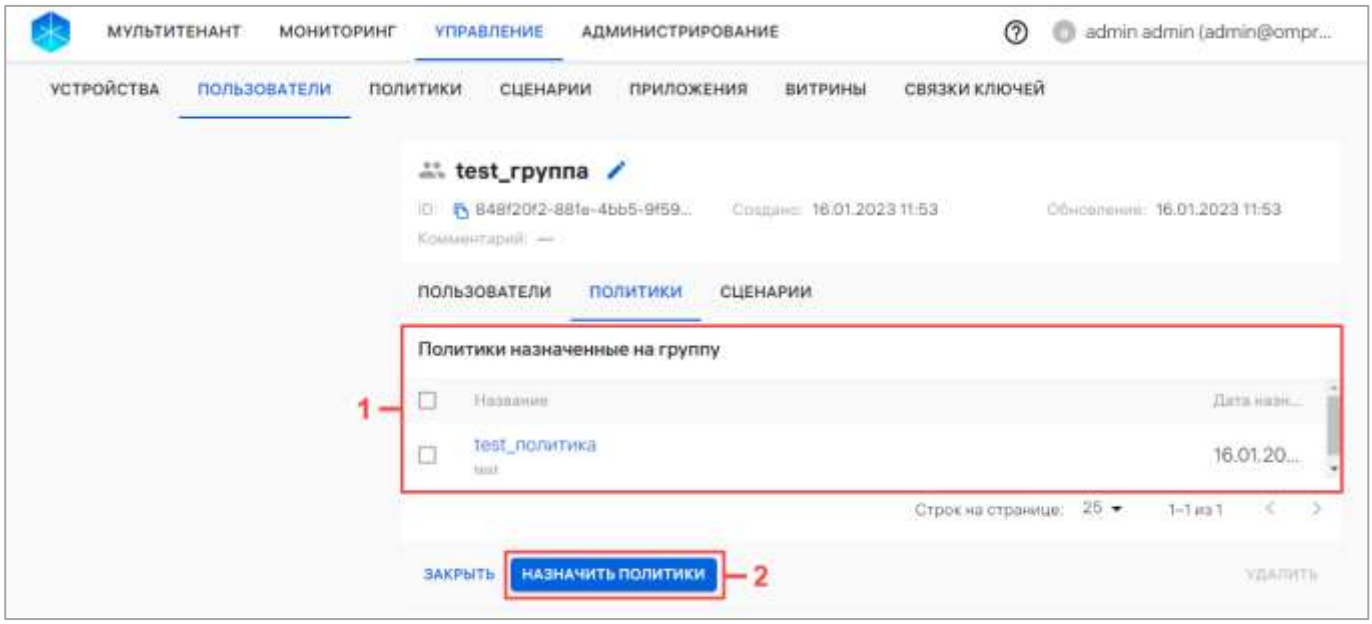

Рисунок 38

Информация о политиках отображается в следующих столбцах:

– «Название» — название политики, назначенной на группу пользователей;

– «Дата назначения» — дата назначение политики.

Название политики представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5).

Для редактирования списка политик необходимо нажать кнопку «Назначить политики» (Рисунок 38 [2]) и далее выполнить действия, описанные в пп. 2.4.5.3.

2.1.4.4. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу пользователей (Рисунок 39), а при его отсутствии отображается сообщение «На группу не назначен ни один офлайн-сценарий».

ПРИМЕЧАНИЕ. 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.

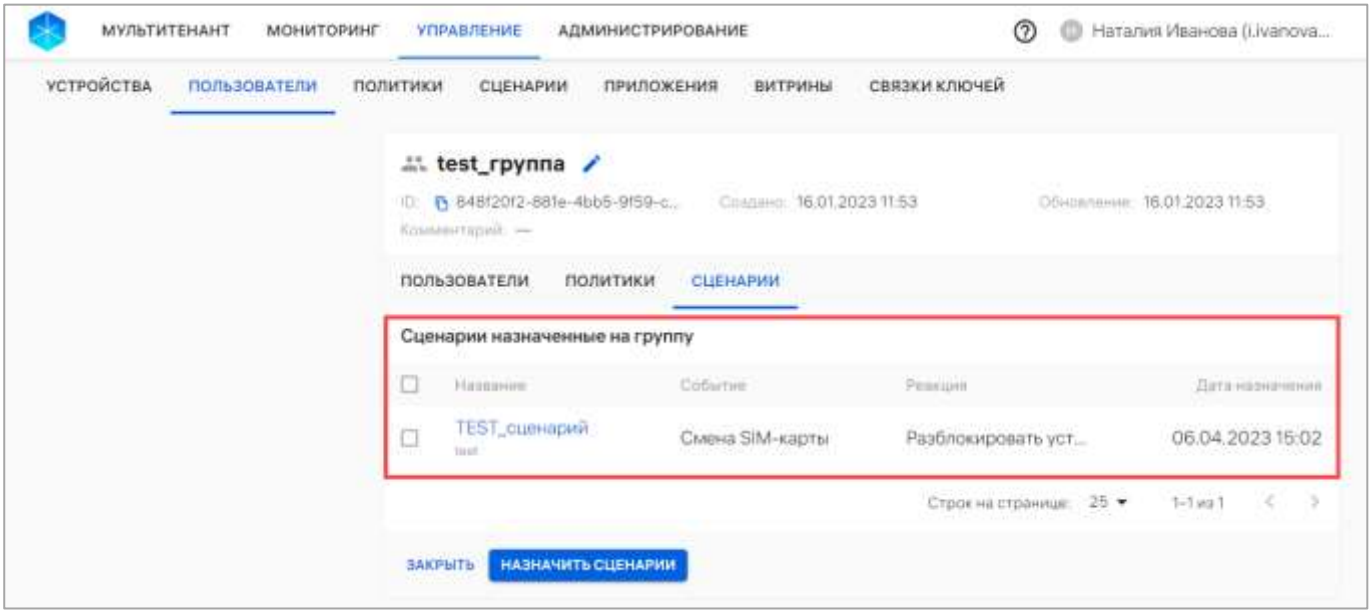

Рисунок 39

В рабочей области информация о назначенных офлайн-сценариях отображается в следующих столбцах (Таблица 10).

Таблица 10

Название столбца	Описание
Название	Название офлайн-сценария
	Комментарий – дополнительная информация к офлайн-сценарию
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 27))
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

ПРИМЕЧАНИЕ. Процесс назначения и отвязки офлайн-сценария на группу пользователей через карточку группы пользователей приведен в п. 2.5.2.4 и п. 2.5.3.3 соответственно.

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»;

– выбрать политику.

В результате откроется карточка политики, интерфейс которой включает следующие элементы:

– шапка карточки (Рисунок 40 [1], пп. 2.1.5.1);

– вкладки карточки (Рисунок 40 [2]). В карточке политики доступен переход к следующим вкладкам:

- «Правила» (пп. 2.1.5.2);
- «Группы» (пп. 2.1.5.3).

2.1.5.1. Шапка карточки

В шапке карточки отображается (Рисунок 40 [1]) следующая информация о политике:

– 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, добавленная при создании политики.

Для редактирования данных политики необходимо выполнить следующие действия:

– нажать значок ✎ «Редактировать» (Рисунок 40 [3]);

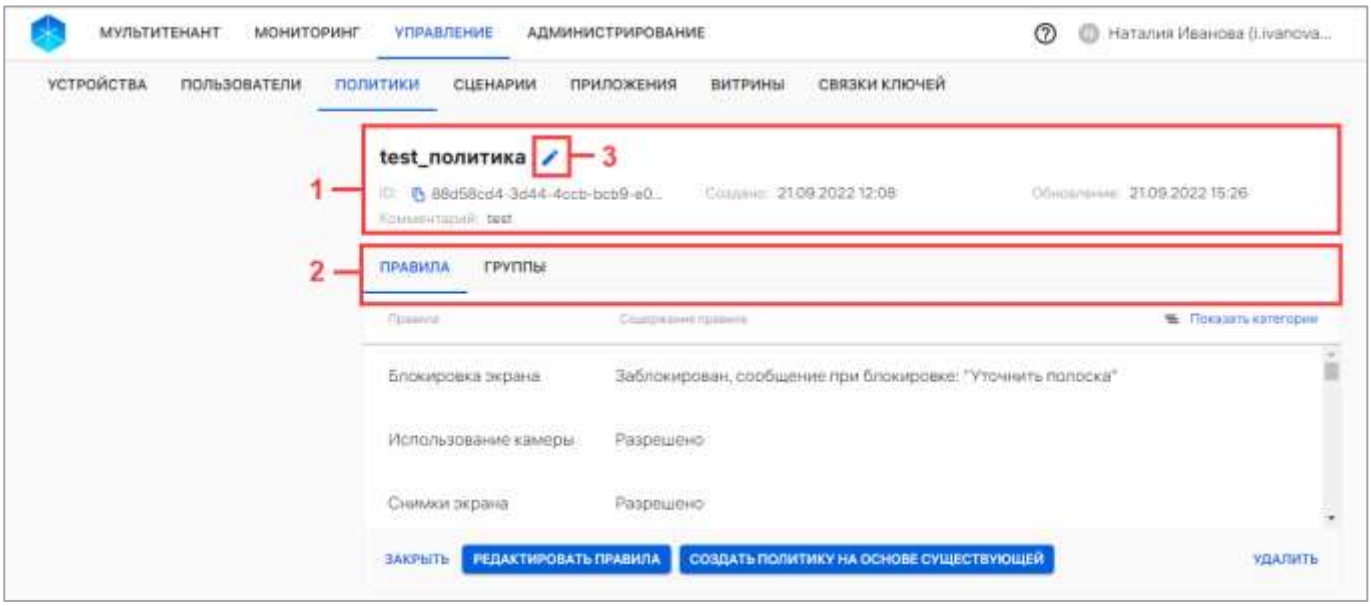

Рисунок 40

– в открывшемся окне «Редактирование политики» внести изменения в необходимые поля;

– сохранить изменения либо отменить действия (Рисунок 41).

Рисунок 41

В результате успешного сохранения данные выбранной политики будут отредактированы, отобразится сообщение «Политика обновлена».

2.1.5.2. Вкладка «Правила»

Во вкладке «Правила» отображается список правил, добавленных в политику, с указанием их категории и содержания. Информация отображается в следующих столбцах (Рисунок 42):

– «Правила» — название правила;

– «Содержание правила» — краткая информация по правилам, добавленным в политику.

Для отображения категории правил необходимо нажать кнопку «Показать категории» (Рисунок 42).

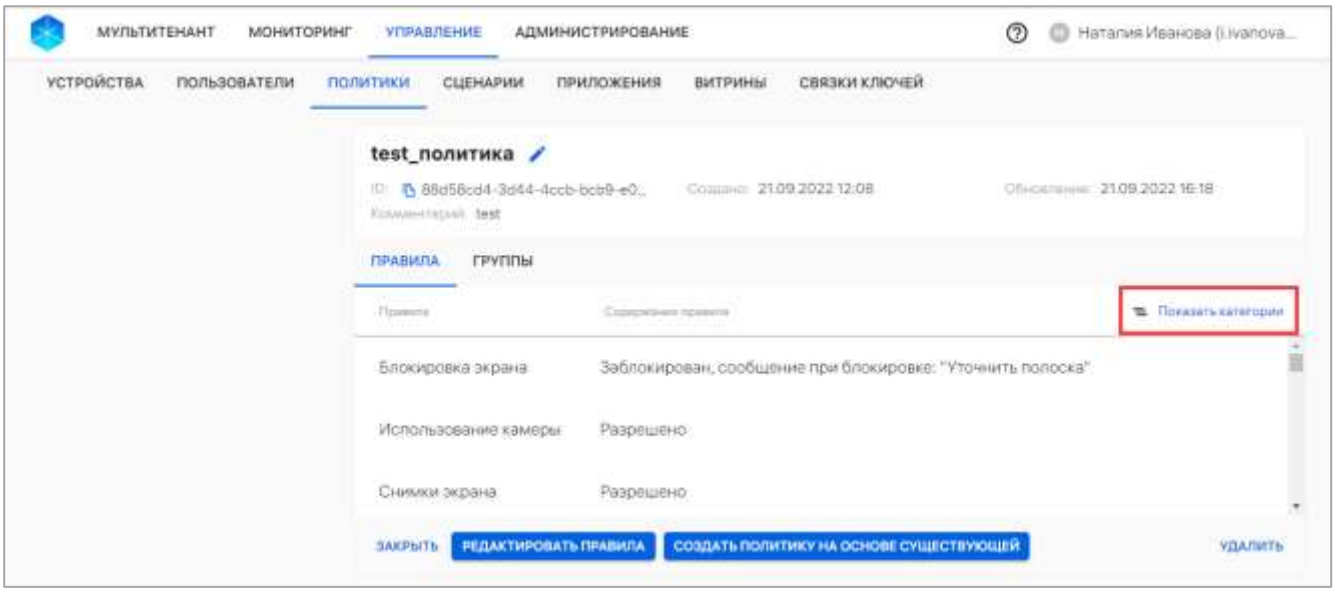

Рисунок 42

Для просмотра информации о каждой категории правил необходимо нажать значок в строке с категорией (Рисунок 43 [1]), в результате чего отобразится перечень правил, входящих в данную категорию.

Для перехода к списку правил необходимо нажать кнопку «Показать список» (Рисунок 43 [2]).

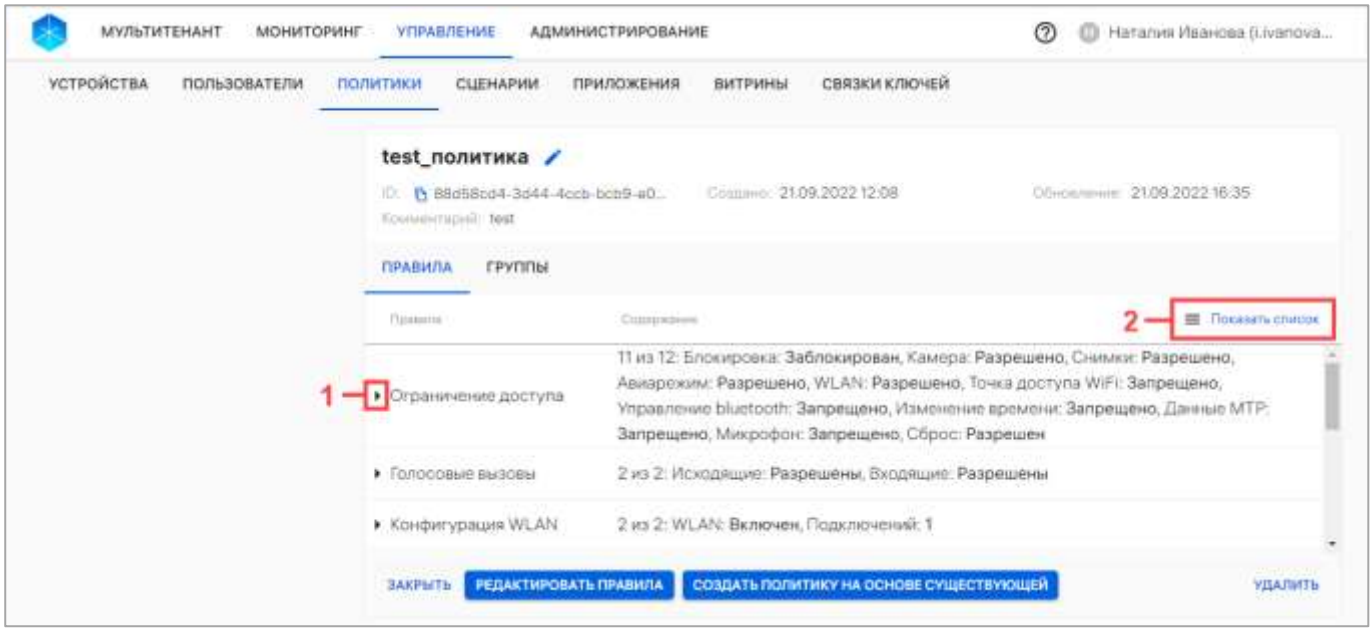

Рисунок 43

Набор правил политики подлежит редактированию. Процесс редактирования приведена в п. 2.4.4.

2.1.5.3. Вкладка «Группы»

Во вкладке «Группы» отображаются группы действия политик (списки групп устройств и групп пользователей), на которые назначена политика (Рисунок 44).

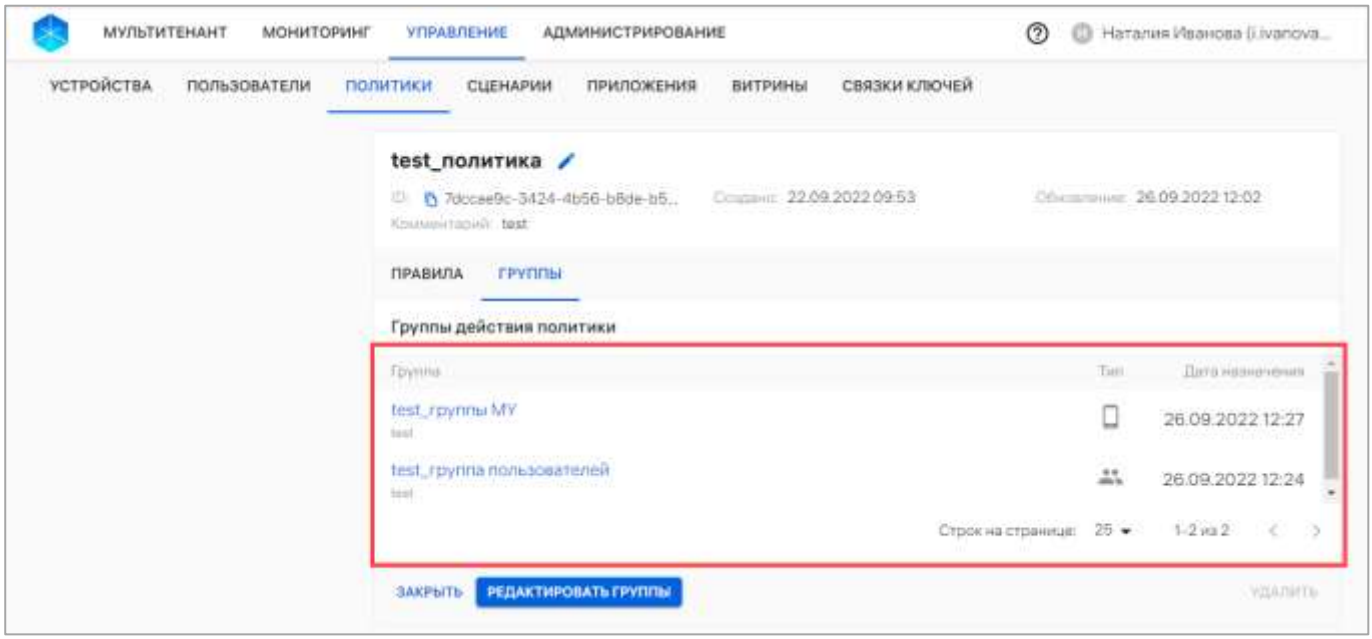

Рисунок 44

Информация отображается в следующих столбцах:

– «Группа» — название группы устройств или группы пользователей, на которые назначена данная политика, и комментарий (при наличии). Представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку группы;

– «Тип» — тип группы:

-  — Группа пользователей;
-  — Группа устройств;

– «Дата назначения» — дата и время назначения политики.

Политика на группы может быть назначена одним из следующих способов:

– через карточку политики (пп. 2.4.5.1);

– чрез карточку группы устройств (пп. 2.4.5.2);

– через карточку группы пользователя (пп. 2.4.5.3).

Отвязать политику от группы возможно одним из следующих способов:

– через карточку политики (пп. 2.4.6.1);

– через карточку группы устройств (пп. 2.4.6.2);

– через карточку группы пользователя (пп. 2.4.6.3).

2.1.6. Работа с карточкой офлайн-сценария

В карточке 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»;

– выбрать офлайн-сценарий.

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

– шапка карточки (Рисунок 45 [1]);

– список групп устройств и групп пользователей, на которые назначен данный офлайн-сценарий (Рисунок 45 [2]).

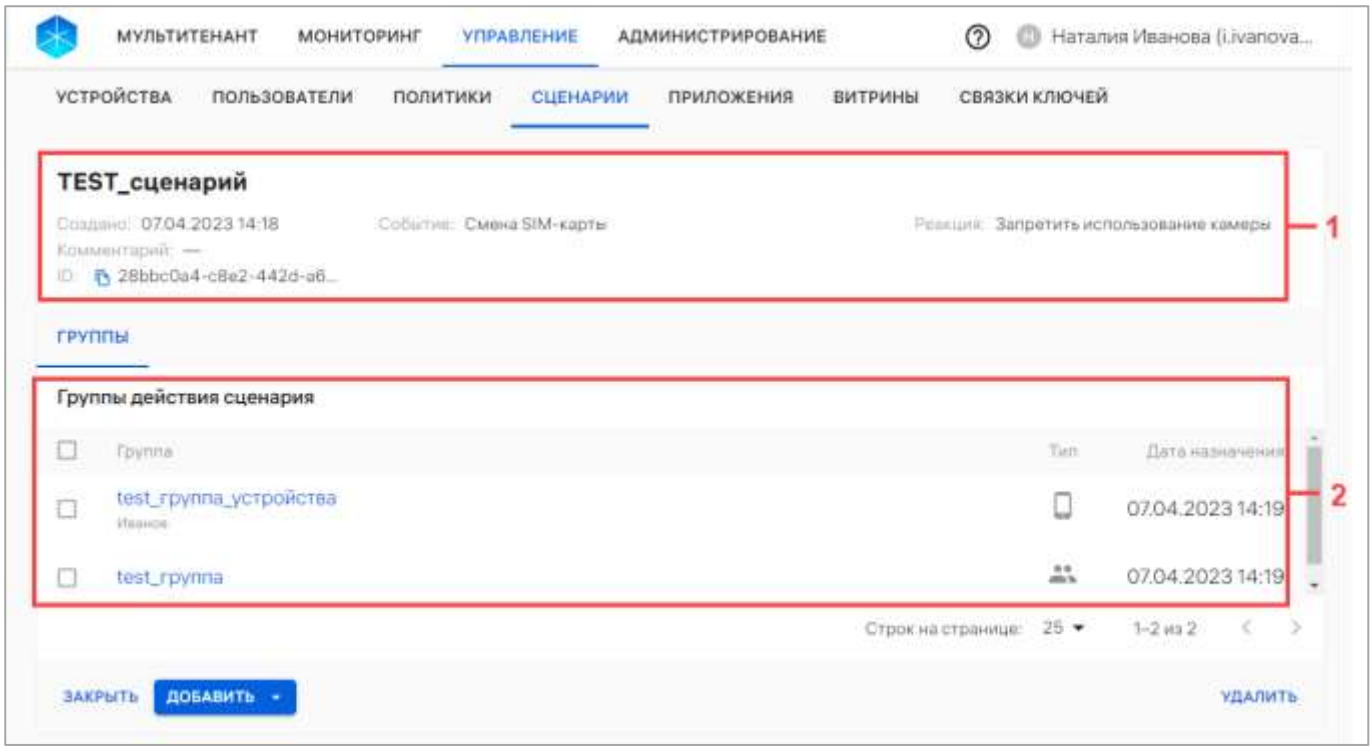

Рисунок 45

В шапке карточки отображается следующая информация:

– название офлайн-сценария;

– «Создано» – дата и время создания офлайн-сценария;

– «Комментарий» – дополнительная информация, добавленная при создании офлайн-сценария;

– «ID» — идентификатор офлайн-сценария, который можно скопировать, нажав кнопку «Копировать id сценария в буфер обмена»;

– «Событие» – доступные значения приведены в таблице (Таблица 27);

– «BSSID» - данное поле отображается, если выбраны события «Нахождение в зоне WLAN»/«Вне зоны действия WLAN»;

– «ID меток входа» - уникальные идентификаторы меток входа. Данное поле отображается, если выбраны события «Нахождение на территории, определяемой NFC-метками»;

– «ID меток выхода» - уникальные идентификаторы меток выхода. Данное поле отображается, если выбраны события «Нахождение на территории, определяемой NFC-метками»;

– «Реакция» – доступные значения приведены в таблице (Таблица 27);

– «Период» - данное поле отображается, если выбрана реакция «Задать период отправки событий безопасности», либо событие «Отсутствие связи с сервером»).

В рабочей области, в списке групп устройств и групп пользователей, на которые назначен данный офлайн-сценарий, информация отображается в столбцах, приведенных в таблице (Таблица 11).

Таблица 11

Название столбца	Значение	Описание
Группа	Название группы устройств или группы пользователей	Название группы представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку групп устройств или групп пользователей
	Комментарий	Отображается при наличии
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 46 [2]).

ПРИМЕЧАНИЕ. Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 46 [1]).

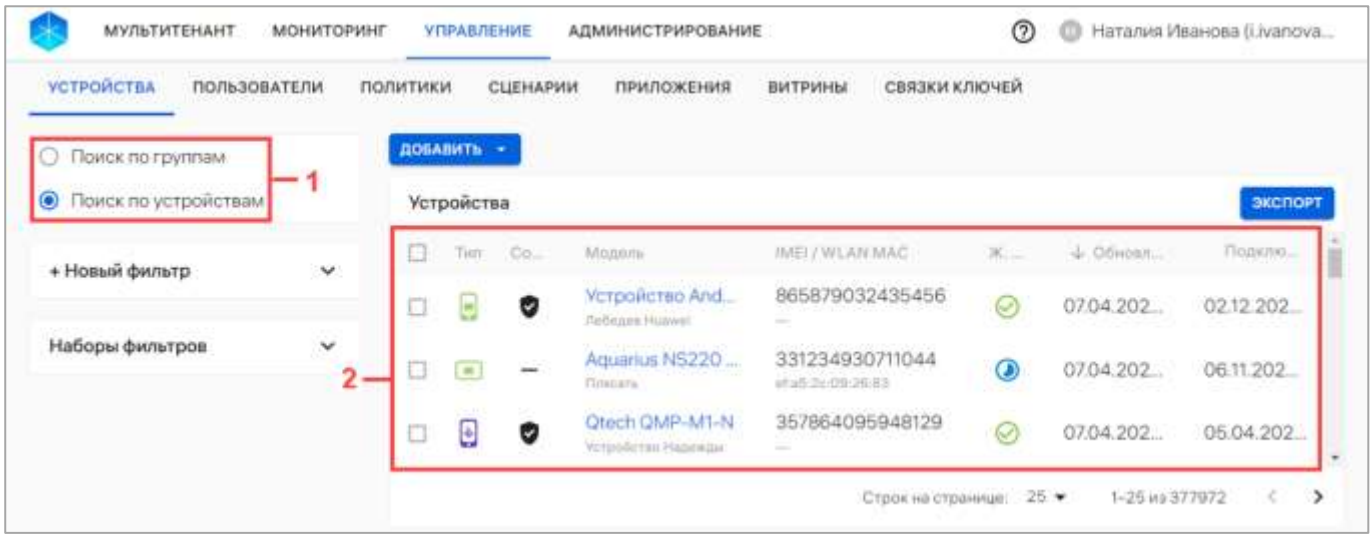

Рисунок 46

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 7), а при отсутствии добавленных об устройствах или групп устройств отображается сообщение «Нет данных».

При выборе в области фильтров «Поиск по группам» (Рисунок 47 [1]) информация о группах устройств в рабочей области отображается в следующих столбцах (Рисунок 47 [2], Таблица 12).

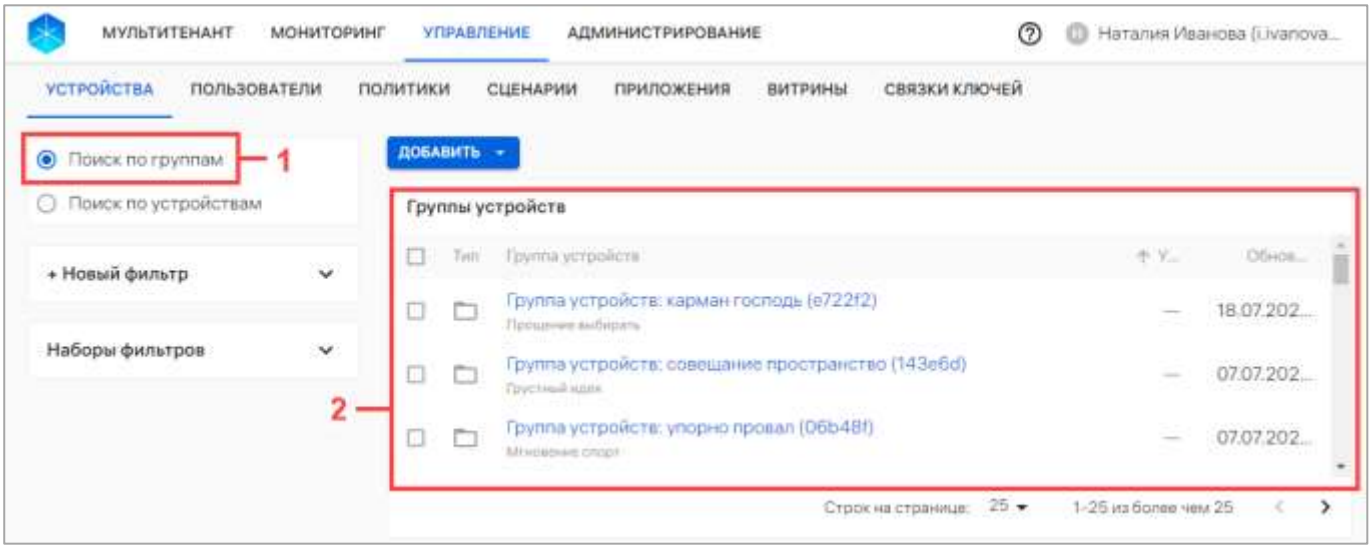

Рисунок 47

Таблица 12

Параметр	Описание	
Тип	Тип группы устройств: – Динамическая группа – группа, в которую устройства добавляются автоматически согласно выбранному алгоритму добавления; – Статическая группа - группа, в которую можно добавлять отдельные устройства	
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
Устройства	Количество устройств, привязанных к группе Значение столбца отсортировано в направлении стрелки: от меньшего к большему, от большего к меньшему	
Обновлено	Параметр сортировки по дате обновления политики. Значение столбца отсортировано в направлении стрелки: от старых к новым, от новых к старым	

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

– вручную в соответствии с п. 2.2.1 и 2.2.2;

– с помощью CSV-файла в соответствии с п. 2.3.3.

2.2.1. 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 48);

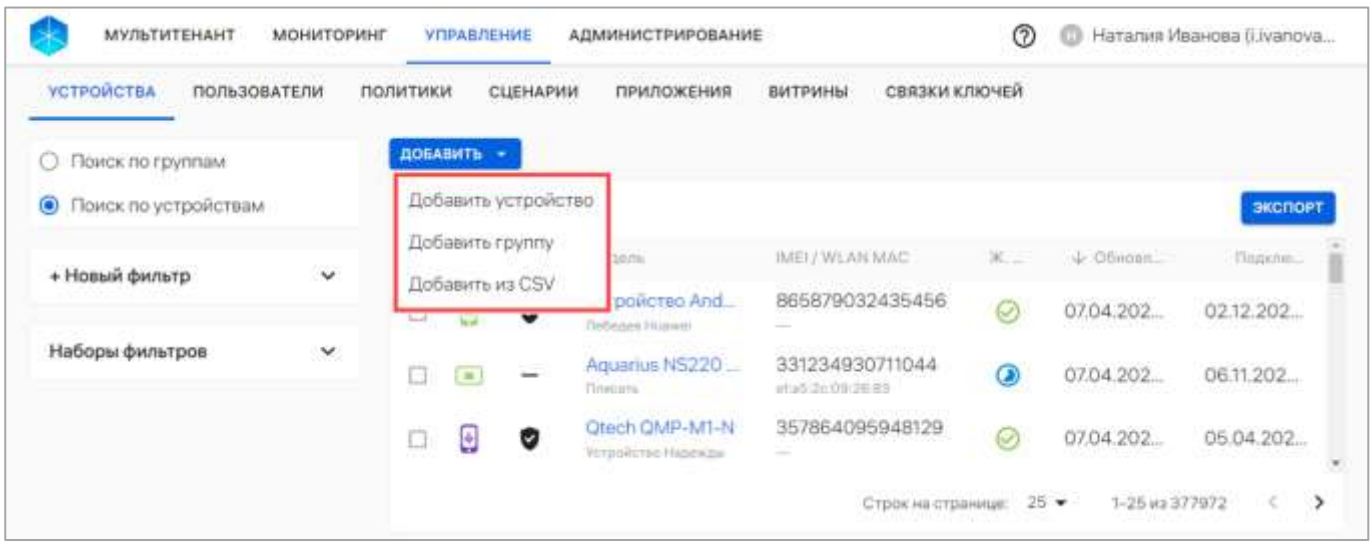

Рисунок 48

– в открывшемся окне «Создание устройства вручную» (Рисунок 49) заполнить поля, приведенные в таблице (Таблица 13);

– подтвердить либо отменить действия.

При успешном добавлении устройства отобразится сообщение «Устройство добавлено» и откроется карточка добавленного устройства (п. 2.1.1).

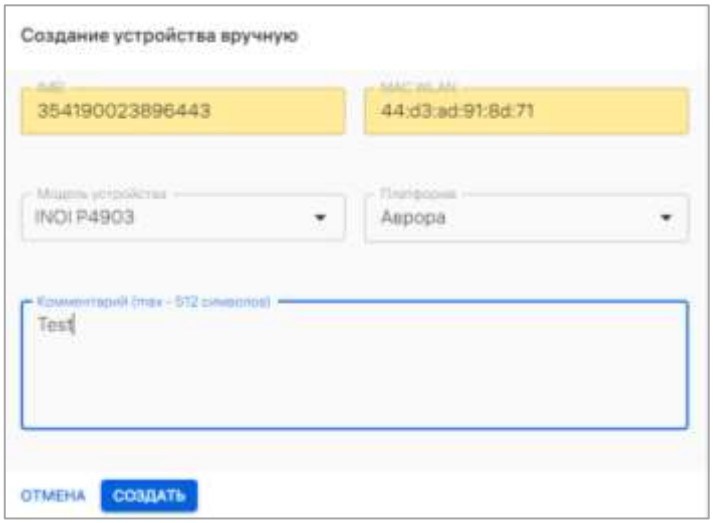

Рисунок 49

Таблица 13

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	Поле обязательно для заполнения, если не заполнено поле MAC WLAN; **ПРИМЕЧАНИЕ.** Если на устройствах под управлением ОС Аврора поле IMEI не заполнено, то после успешной активации значение IMEI отобразится в карточке устройства автоматически
MAC WLAN	Ввести MAC-адрес WLAN устройства. Ввод значения с клавиатуры. Количество символов – 6 пар символов, разделенных двоеточием), например: «00:aa:00:00:a0:00»	Поле обязательно для заполнения для устройств на базе ОС Аврора, если не заполнено поле IMEI. **ПРИМЕЧАНИЕ.** Если на устройстве под управлением ОС Аврора поле MAC WLAN не заполнено, то после успешной активации значение MAC WLAN отобразится в карточке устройства автоматически
Модель устройства	Выбор модели устройства из раскрывающегося списка	Полное название типа устройств зависит от модели устройства

Параметр	Значения	Описание
Платформа	**ВНИМАНИЕ!** При выборе платформы необходимо выбрать «Аврора» т.к. ОС Android, а также ОС семейства Linux, в комплект поставки не входят	Поле обязательно для заполнения
Комментарий	Ввод значения с клавиатуры. Максимальная длина – 512 символов	Поле не является обязательным для заполнения

2.2.2. Добавление группы устройств вручную

Для добавления группы устройств вручную необходимо выполнить следующие действия:

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

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить группу» (см. Рисунок 48);

– в открывшемся окне «Новая группа» (Рисунок 50) заполнить поля и выбрать значение, приведенные в таблице (Таблица 14);

– подтвердить либо отменить действия.

В результате успешного добавления группы устройств отобразится сообщение «Группа успешно создана» и откроется карточка добавленной группы (п. 2.1.2).

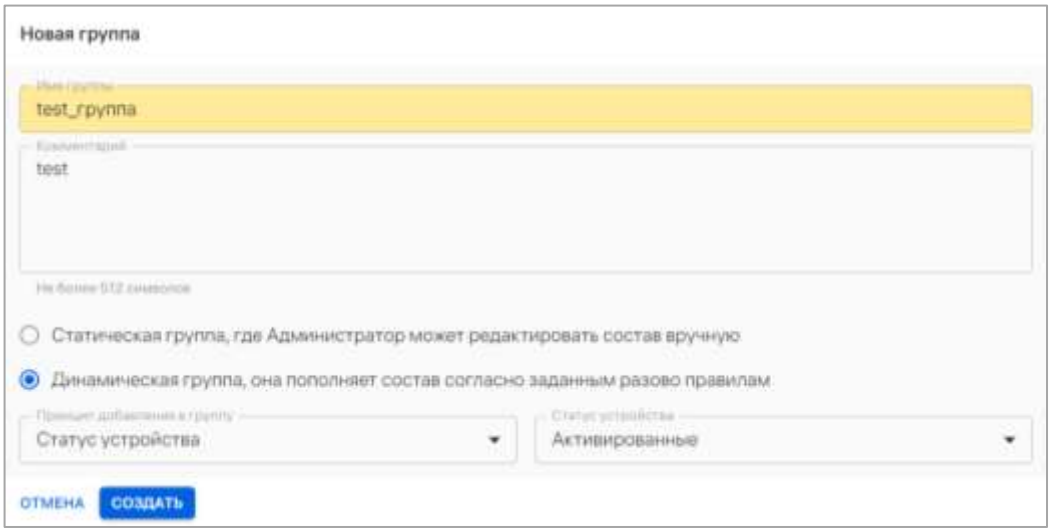

Рисунок 50

Таблица 14

Параметры	Значение	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
Выбор значения	Статическая группа	Состав правил данной группы Администратор может редактировать вручную
	Динамическая группа	Эта группа пополняет состав согласно заданным разово правилам. **ПРИМЕЧАНИЕ.** Нельзя создать несколько динамических групп с одинаковыми условиями. В случае попытки создания еще 1 динамической группы отобразиться сообщение: «Динамическая группа с такими условиями уже существует в системе». Такую группу невозможно удалить (кнопка «Удалить группу» неактивна)
Принцип добавления в группу **ВНИМАНИЕ!** Поле отображается при выборе динамической группы	Выбрать значение «Статус устройства» из раскрывающегося списка	
Статус устройства **ВНИМАНИЕ!** Поле отображается при выборе динамической группы	Выбрать значение из раскрывающегося списка: – Активированные; – Неактивированные	Активированные – в динамическую группу будут автоматически попадать все активированные устройств. Неактивированные – в динамическую группу будут попадать все неактивированные устройства

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 48);

– в открывшемся окне «Импорт устройств из файла CSV» нажать кнопку «Шаблон .CSV ⬇» (Рисунок 51), в результате чего шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 15), пример заполнения CSV-файлов приведен в пп. 2.2.3.2.

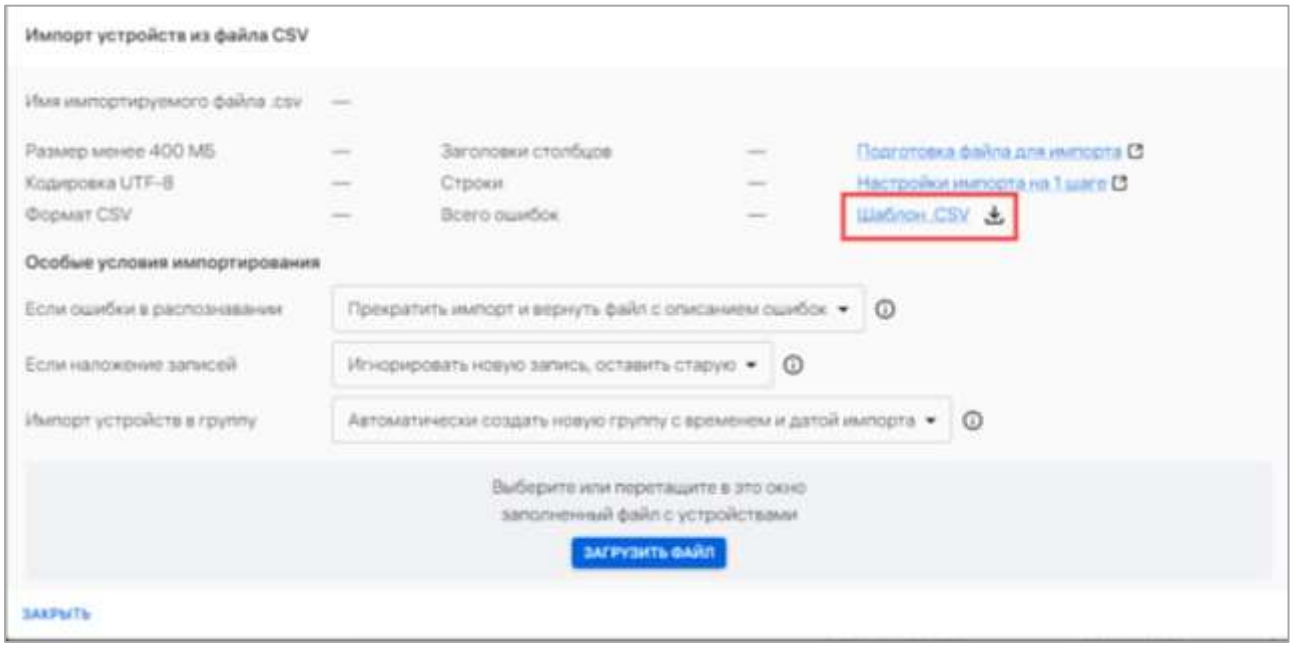

Рисунок 51

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,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT,STRATEGY"). 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";

– строки с пробелами или запятыми должны заключаться в кавычки «"» (если в строке требуется передать кавычку, ее необходимо удвоить).

ПРИМЕЧАНИЕ. После COMMENT может быть добавлен необязательный столбец STRATEGY. Возможные значения: SKIP(S) и REPLACE(R). Он заполняется в случае необходимости указать стратегию для конкретной строки (пп. 2.2.3.3). Стратегия в строке может отличаться от основной выбранной и будет являться приоритетной.

Описание требований к значениям параметров приведены в таблице (Таблица 15).

Таблица 15

Параметр	Описание	Примечание
GROUP	Название группы устройств. Должен содержать от 2 до 64 символов	Параметр обязателен для заполнения, при: – создании группы устройств; – привязке устройств к группе
IMEI	Международный идентификатор мобильного	Параметр обязателен для заполнения:

Параметр	Описание	Примечание
	оборудования. Должен содержать 15 цифр. ПРИМЕЧАНИЕ. Если устройство поддерживает работу 2 SIM-карт, в поле «IMEI» допускается ввод любого из 2 значений IMEI	– если не указан параметр WLAN_MAC при: • добавлении нового устройства на базе ОС Аврора; • привязке устройства к группе. ПРИМЕЧАНИЕ. Если на устройстве под управлением ОС Аврора поле IMEI не заполнено, то после успешной активации значение IMEI отобразится в карточке устройства автоматически
WLAN_MAC	MAC-адрес WLAN устройства. Содержит 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	Параметрт обязателен для заполнения, если не указан параметр IMEI при: • добавлении нового устройства на базе ОС Аврора; • привязке устройства к группе. ПРИМЕЧАНИЕ. Если на устройстве под управлением ОС Аврора 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. Доступные значения: – Aquarius Cmp NS 208; – Aquarius NS208RH; – Aquarius NS208 v4.2; – Aquarius NS220RE – Aquarius NS220 v2.1; – Aquarius NS220 v3.2; – Aquarius NS220 v5.2; – Aquarius NS M11; – Aquarius NS M12; – BlackView 6000S; – Byterg MVK-2020; – F+ LifeTab Plus; – F+ R570;	Параметр не обязателен для заполнения. ПРИМЕЧАНИЕ. Если поле MAC WLAN не заполнено, то после успешной активации значение MAC WLAN отобразится в карточке устройства автоматически

Параметр	Описание	Примечание
	– F+ R570E; – INOI P4903; – INOI T10; – INOI T8; – Mashtab TrustPhone T1; – MIG C55; – Qtech QMP-K8; – Qtech QMP-M1-N; – Qtech QMP-M1-N-IP; – Sony Xperia X **ВНИМАНИЕ!** ОС Android, а также ОС семейства Linux, в комплект поставки не входят	
PLATFORM	Необходимо указать «AURORA», т.к. ОС Android, а также ОС семейства Linux, в комплект поставки не входят	Параметр обязателен для заполнения
COMMENT	Дополнительная информация к устройству или группе устройств. 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, 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	Параметр не обязателен для заполнения. Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта

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

2.2.3.2. Примеры заполненных CSV-файлов

В зависимости от содержимого CSV-файла при загрузке в Консоли администратора ПУ происходит:

– добавление новых устройств или групп устройств;

– привязка устройств к группе устройств.

Для добавления новых устройств необходимо указать значение одного из обязательных параметров «IMEI» или «WLAN_MAC», а также «PLATFORM»:

```
GROUP,IMEI,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT
,352132035783492,, ,AURORA,
,350408012241197,, ,AURORA,
GROUP,IMEI,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT
,,06:C8:67:5B:68:EE, ,ANDROID,
,,03:F7:68:4C:98:EE, ,ANDROID,
```

Для добавления новых групп устройств необходимо указать название группы в параметре «GROUP»:

```
GROUP,IMEI,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT
"Группа устройств 1",,,,,
"Группа устройств 2",,,, ,
```

Для привязки устройства к группе устройства необходимо указать один из обязательных параметров: «IMEI» или «WLAN_MAC», а также указать название группы в параметре «GROUP» и «PLATFORM».

```
GROUP,IMEI,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT
"Группа устройств 1",352132035783492,,,ANDROID,
"Группа устройств 2",,03:F7:68:4C:98:EE,,ANDROID,
```

Пример полностью заполненного CSV-файла:

```
GROUP,IMEI,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT
```

```
"Группа устройств 1",352132035783492,06:C8:67:5B:68:EE,
"MIG C55",AURORA,"Комментарий 1"
"Группа устройств 2",350408012241197,03:F7:68:4C:98:EE,
"MIG C55",AURORA,"Комментарий 2"
```

2.2.3.3. 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 48);

– в открывшемся окне «Импорт устройств из файла CSV» задать особые условия импорта, приведенные в таблице (Таблица 16).

Таблица 16

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 52 [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	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
	некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройства	
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 52 [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	

Наименование полей	Описание	Примечание
Импорт устройств в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 52 [3]): – **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	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ. В результате отобразится текст подсказки следующего содержания: в процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую

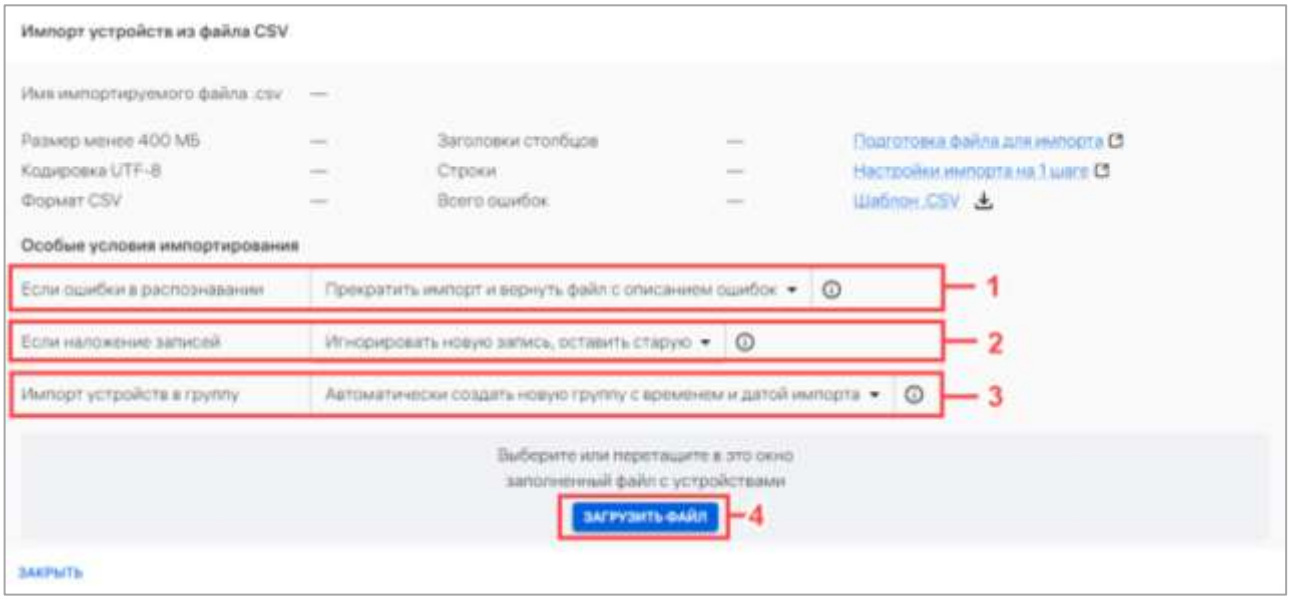

Рисунок 52

– далее необходимо загрузить CSV-файл одним из способов:

- переместить CSV-файл в область загрузки;
- нажать кнопку «Загрузить файл» (см. Рисунок 52 [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 53).

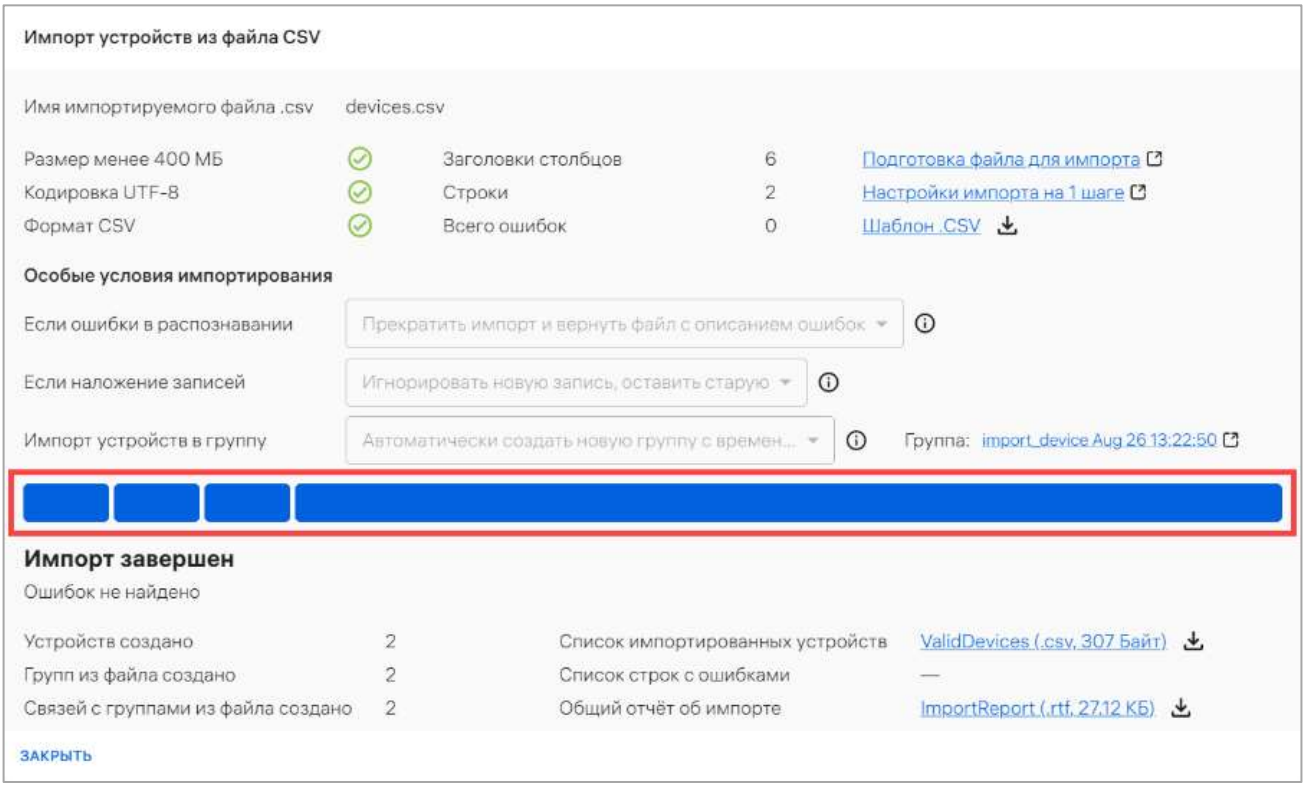

Рисунок 53

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 54 [6]).

Рисунок 54

В окне с результатами импорта устройств отображается следующая информация:

– название импортируемого файла (Рисунок 54 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (Рисунок 54 [2]);

– количество столбцов, всех импортируемых строк и ошибок в файле (Рисунок 54 [3]);

– ссылки (Рисунок 54 [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 (Рисунок 54 [5], см. Таблица 16);

– шкала прогресса импорта (Рисунок 54 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (Рисунок 54 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (Рисунок 54 [8]);

– количество добавленных устройств, групп устройств и их связей (Рисунок 54 [9]);

– ссылки на скачивание отчетов (Рисунок 54 [10]):

- отчет со списком импортированных устройств. Формат отчета — `.csv`;
- отчет со списком строк, содержащих ошибки и с указанием причины ошибки. Формат отчета — `.csv` (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);
- 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. 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»;

– выбрать устройства, при необходимости воспользовавшись фильтром;

– нажать кнопку «Экспорт» (Рисунок 55);

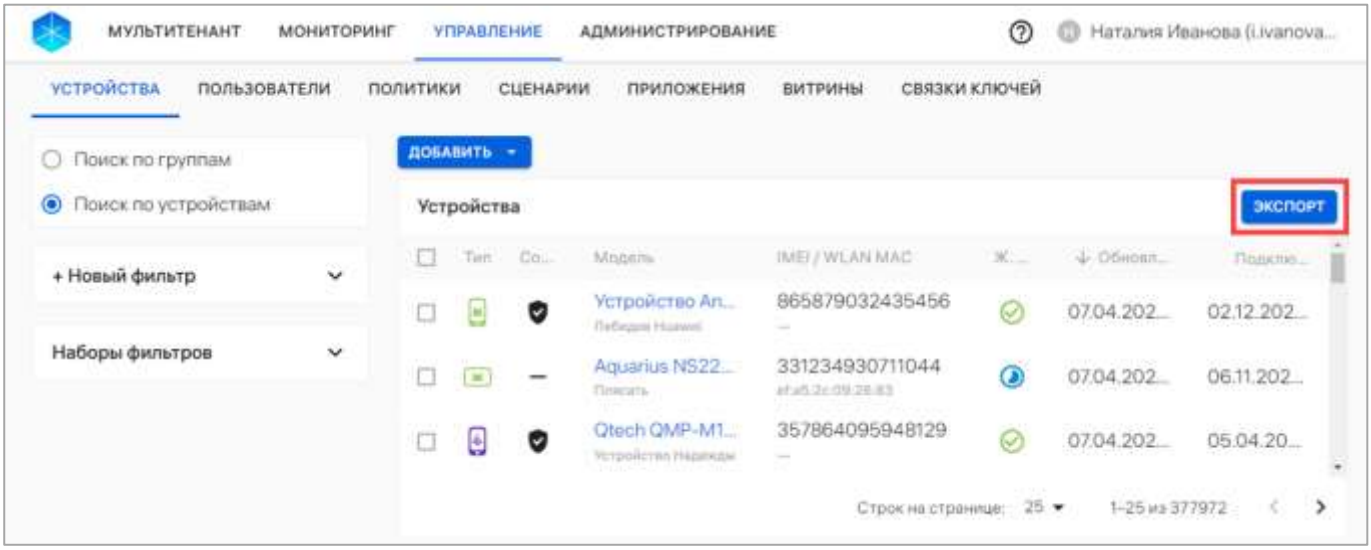

Рисунок 55

– в отобразившемся окне подтверждения экспорта устройств подтвердить либо отменить действия (Рисунок 56).

Рисунок 56

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

ПРИМЕЧАНИЕ. Во время выполнения экспорта кнопка «Экспорт» недоступна для выполнения действий.

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

– imei. Международный идентификатор мобильного оборудования (состоит из 15 цифр);

– macWifi. MAC-адрес WLAN устройства (состоит из 6 пар символов, разделенных двоеточием). Параметр заключен в кавычки;

– **modelName**. Модель устройства. Параметр заключен в кавычки;

– **platform**. ОС устройства. Параметр заключен в кавычки;

– **status**. Статус жизненного цикла устройства. Параметр заключен в кавычки;

– **compliance**. Соответствие устройства назначенной политике. Параметр заключен в кавычки;

– **comment**. Комментарий к устройству. Параметр заключен в кавычки;

– **createdAt.** Дата и время добавления устройства в Аврора Центр. Параметр заключен в кавычки;

– **connectedAt.** Дата и время последнего подключения устройства к Аврора Центр. Параметр заключен в кавычки;

– **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.

2.2.5. 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. 2.2.5.1);

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

– вручную через карточку устройства (пп. 2.2.5.2);

– 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.

2.2.5.1. 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 57 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям» (Рисунок 57 [2]);

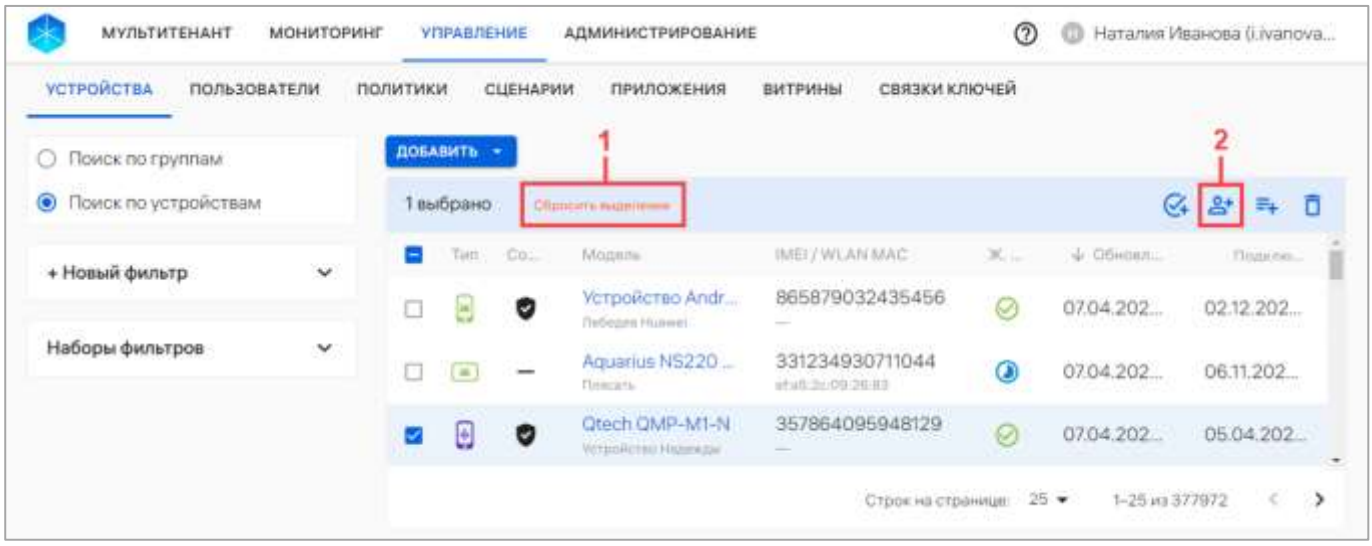

Рисунок 57

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте либо телефону пользователя (Рисунок 58 [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 58 [3]);

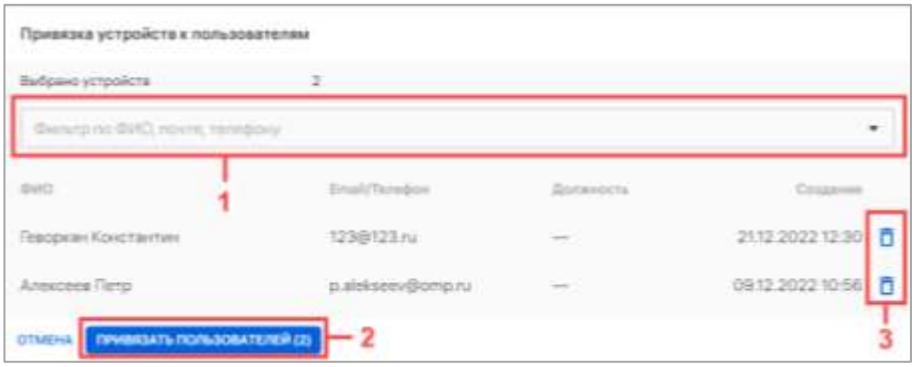

Рисунок 58

– нажать кнопку «Привязать пользователей» (Рисунок 58 [2]).

В результате успешной привязки пользователей отобразится сообщение «Пользователь успешно привязан к [количество устройств] устройству».

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

2.2.5.2. 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»;

– выбрать устройство из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку устройства;

– в открывшейся карточке устройства перейти во вкладку «Пользователи»;

– нажать кнопку «Привязать пользователей» (Рисунок 59);

– в отобразившемся окне (см. Рисунок 58) выполнить действия, описанные в пп. 2.2.5.1.

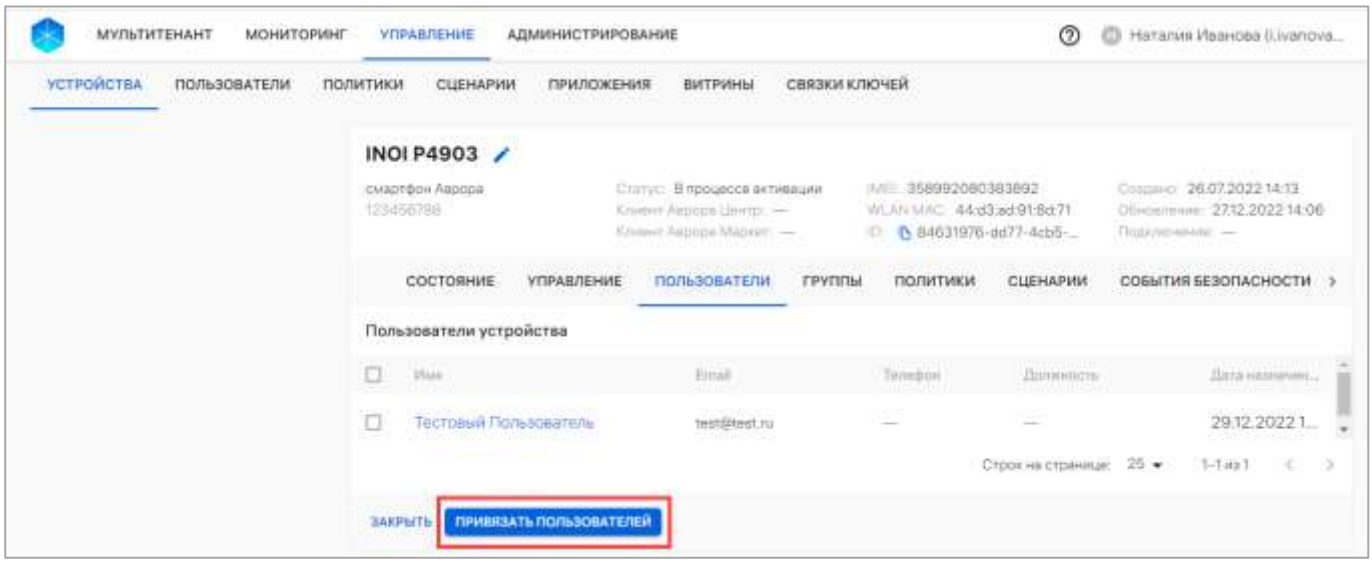

Рисунок 59

2.2.6. 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. 2.2.6.1);

– карточки устройства (пп. 2.2.6.2);

– 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).

2.2.6.1. 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 60 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к группам» (Рисунок 60 [2]);

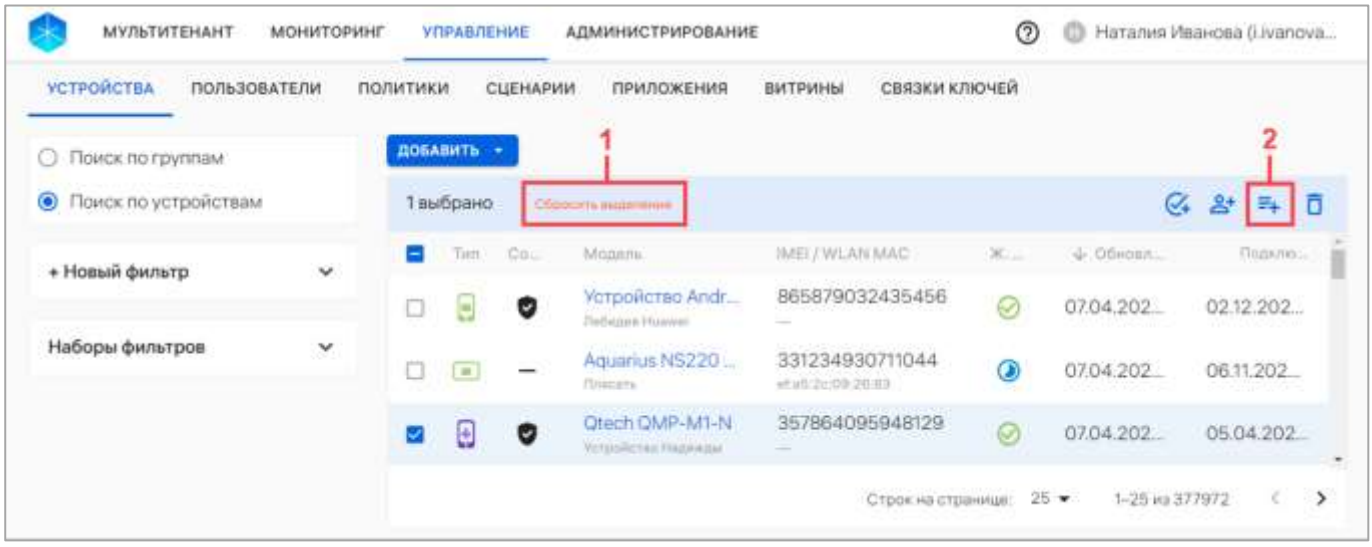

Рисунок 60

– в отобразившемся окне «Добавление устройств в группы» выбрать необходимую группу устройств из раскрывающегося списка (Рисунок 61 [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 61 [3]);

Рисунок 61

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 62 [1]) и нажав кнопку «Создать группу» (Рисунок 62 [2]);

Рисунок 62

– нажать кнопку «Добавить в группы» (Рисунок 61 [2]).

В результате отобразится сообщение «Устройство успешно привязано к [количество групп] группе», и на активированные устройства будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.6.2. 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»;

– выбрать устройства из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку;

– в открывшейся карточке устройства перейти во вкладку «Группы»;

– нажать кнопку «Добавить в группы» (Рисунок 63);

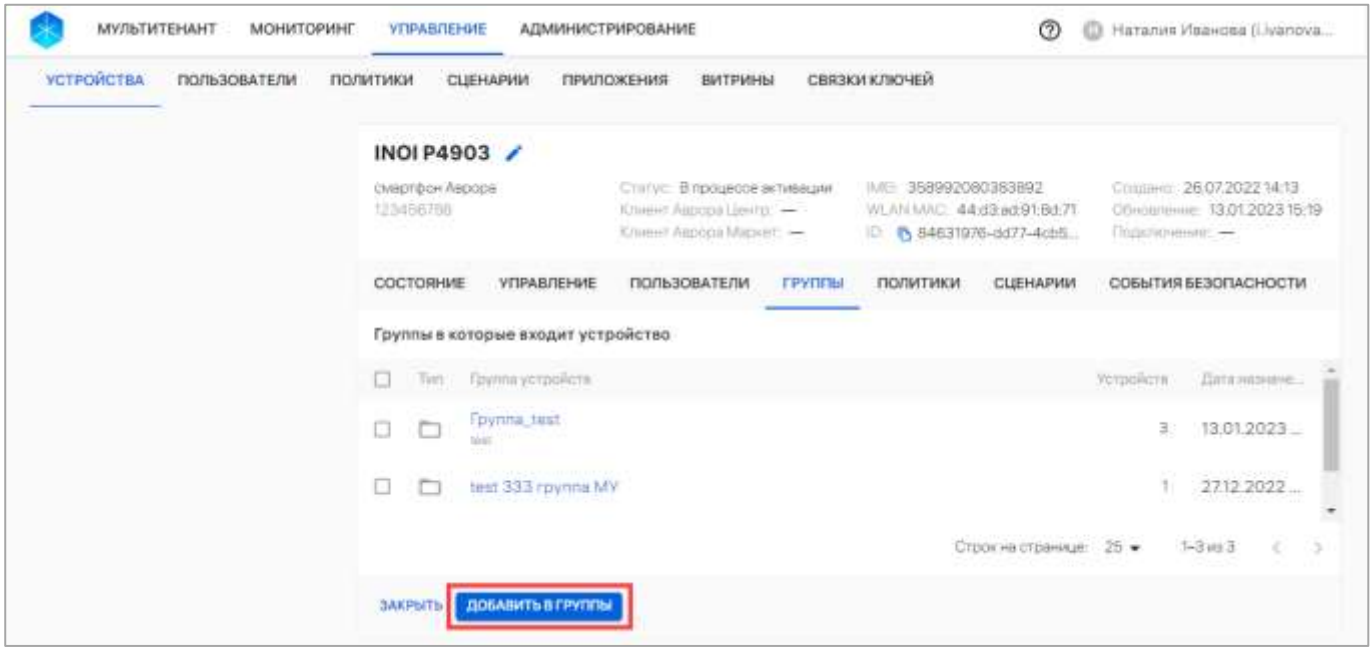

Рисунок 63

– в открывшемся окне «Добавление устройств в группы» необходимо выполнить действия, описанные в пп. 2.2.6.1.

В результате отобразится сообщение «Устройство успешно привязано к [количество групп] группе».

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

2.2.6.3. 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»;

– выбрать группу устройств из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку;

– в открывшейся карточке группы устройств перейти во вкладку «Устройства»;

– нажать кнопку «Привязать устройства» (Рисунок 64);

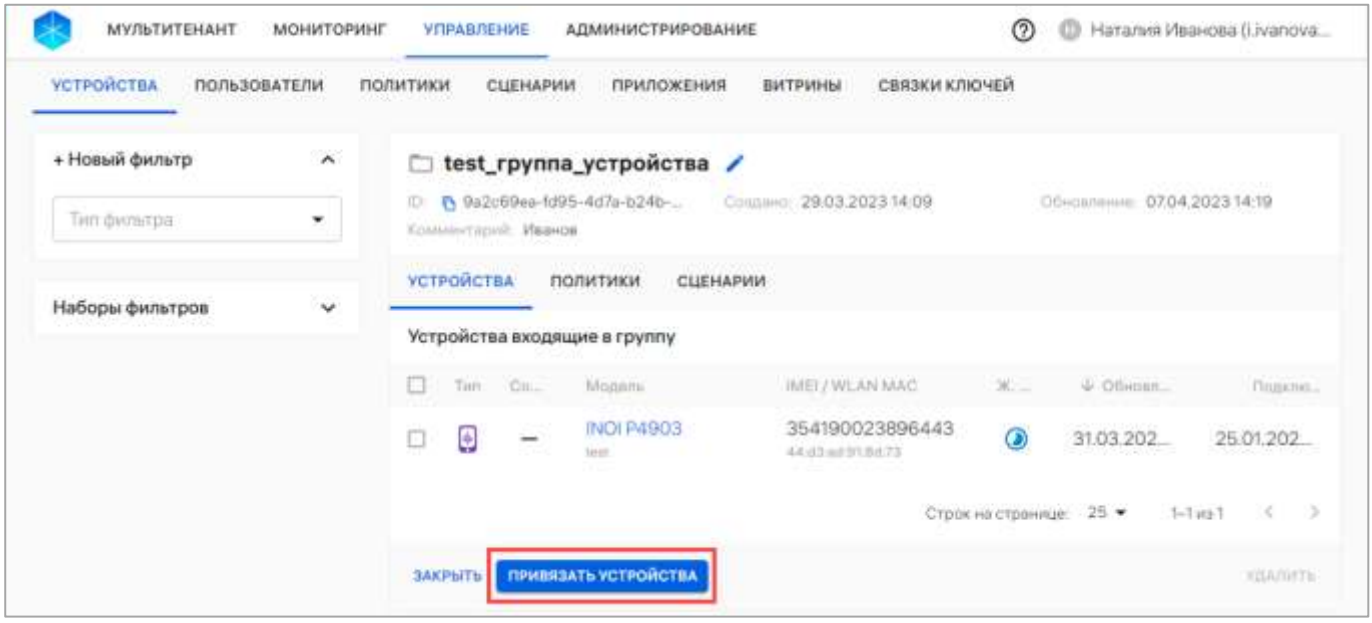

Рисунок 64

– в отобразившемся окне «Добавление устройств в группы» выполнить действия, описанные в пп. 2.2.6.1.

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

2.2.7. 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 документе АДМГ.20134-01 90 01-6.

Активация устройств возможна следующими способами:

– вручную (пп. 2.2.7.1), если необходимо самостоятельно активировать 1 устройство;

– с помощью списка быстрых действий (пп. 2.2.7.2), если необходимо активировать несколько устройств;

– с помощью отправки QR-кода на Email (пп. 2.2.7.3), если необходимо, чтобы пользователи активировали свои устройства самостоятельно;

– с помощью загрузки JSON-файла (пп. 2.2.7.4), если необходимо активировать все устройства группы одним QR-кодом;

– при первом включении устройства (ускоренная активация), если для устройства были выполнены все условия ускоренной активации. Подробное описание процесса ускоренной активации на устройстве приведен в документе АДМГ.20134-01 90 01-6.

2.2.7.1. 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»;

– выбрать устройство из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку устройства;

– в карточке устройства нажать кнопку «Активировать» (Рисунок 65).

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

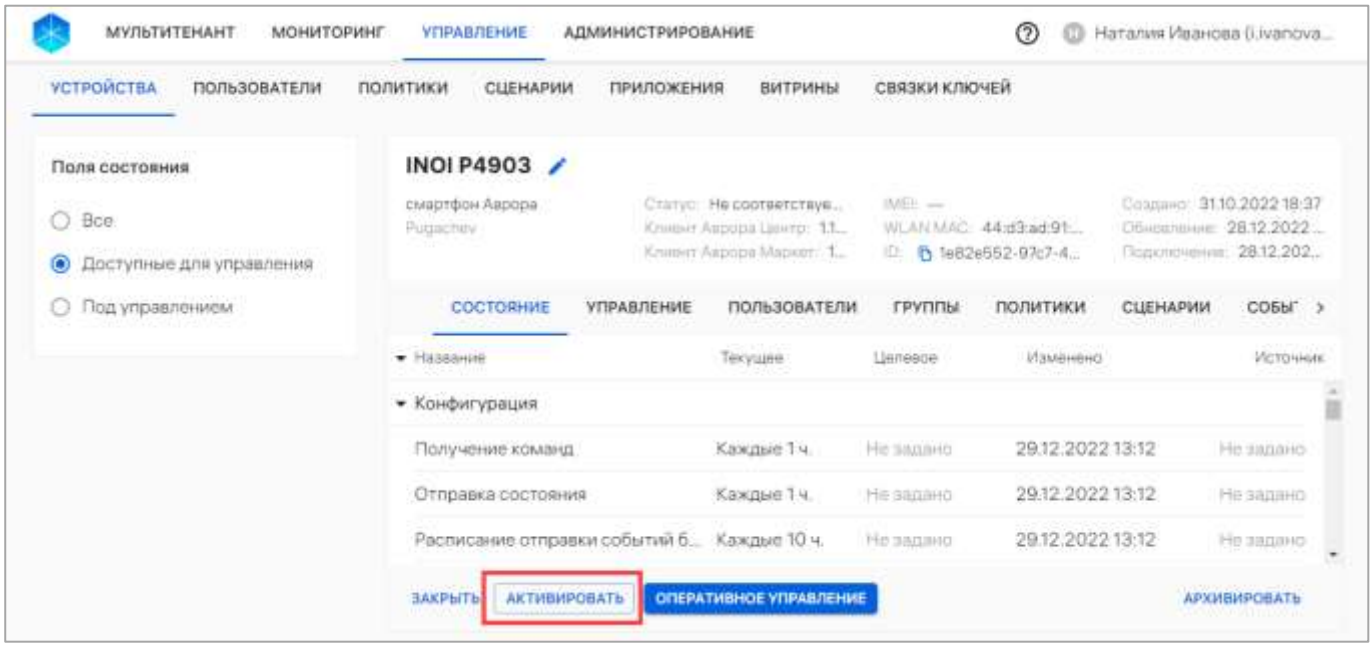

Рисунок 65

– отобразится окно активации устройств (Рисунок 66);

– 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 66 [1]) и нажать кнопку «Дальше» (Рисунок 66 [2]);

Рисунок 66

– откроется окно, где необходимо нажать кнопку «Активация вручную» (Рисунок 67);

Рисунок 67

– в результате отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (Рисунок 68).

Рисунок 68

В результате успешной генерации QR-код будет отображен для активации устройств в клиентском приложении «Аврора Центр» (Рисунок 69).

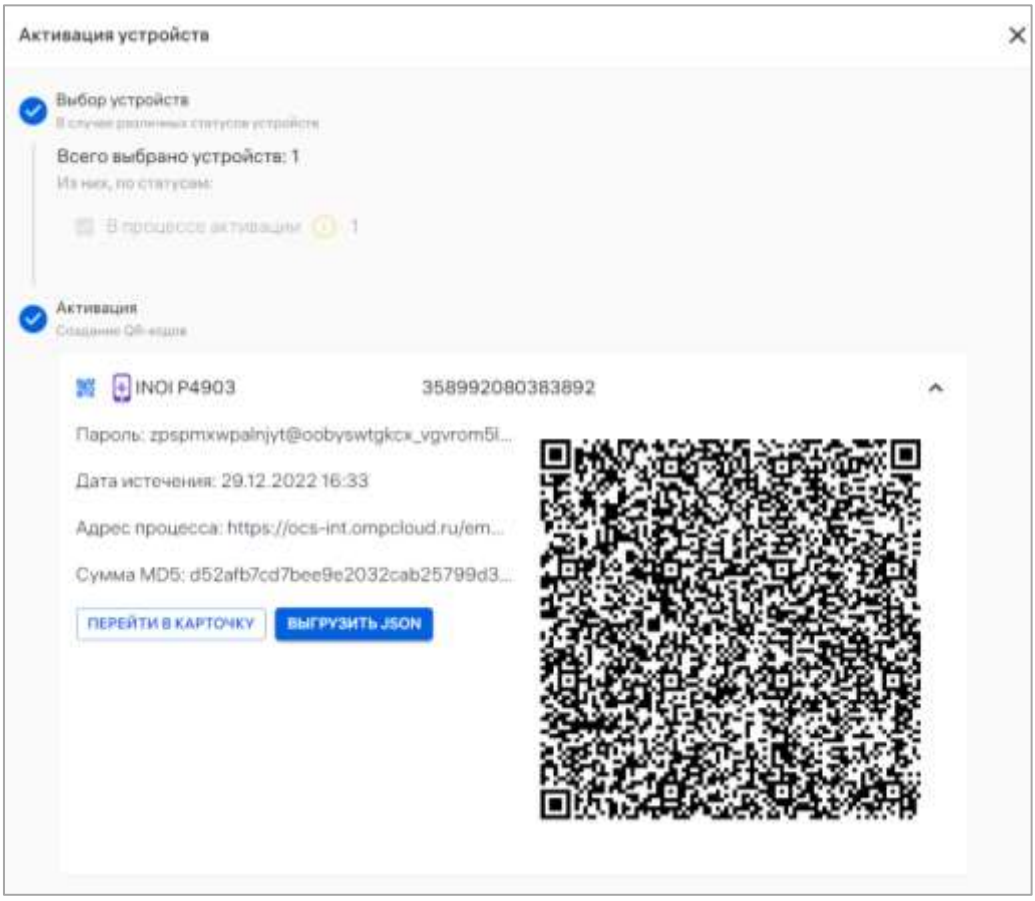

Рисунок 69

Далее пользователю необходимо отсканировать QR-код и выполнить активацию устройств. Подробное описание активации устройств приведено в документе АДМГ.20134-01 90 01-6.

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.

2.2.7.2. 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 70 [1]);

– в списке быстрых действий выбрать значок «Активация устройств» (Рисунок 70 [2]);

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

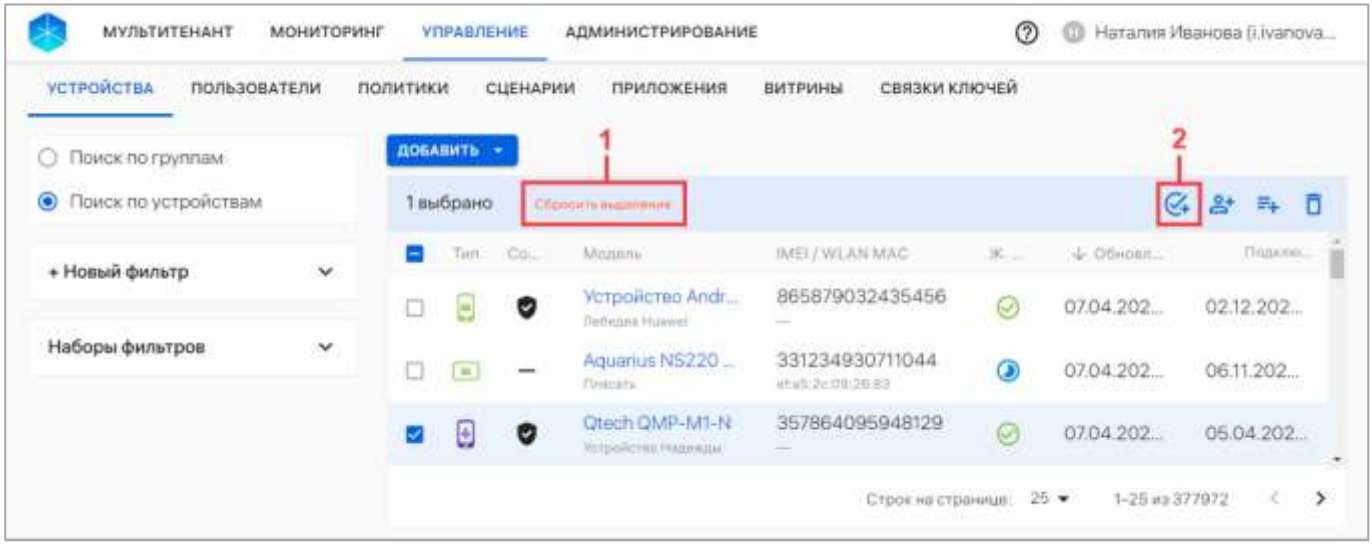

Рисунок 70

– отобразится окно активации устройств (см. Рисунок 66);

– 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 66 [1]) и нажать кнопку «Дальше» (см. Рисунок 66 [2]);

– в открывшемся необходимо нажать кнопку «Активация вручную» (см. Рисунок 67);

– отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия (Рисунок 68).

В результате успешной генерации QR-код будет отображен для каждого из выбранных устройств (Рисунок 71 [1], [2]), который необходимо отсканировать в клиентском приложении «Аврора Центр» на каждом устройстве.

При успешной активации на устройство назначаются все политики и офлайн-сценарии, которые 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.

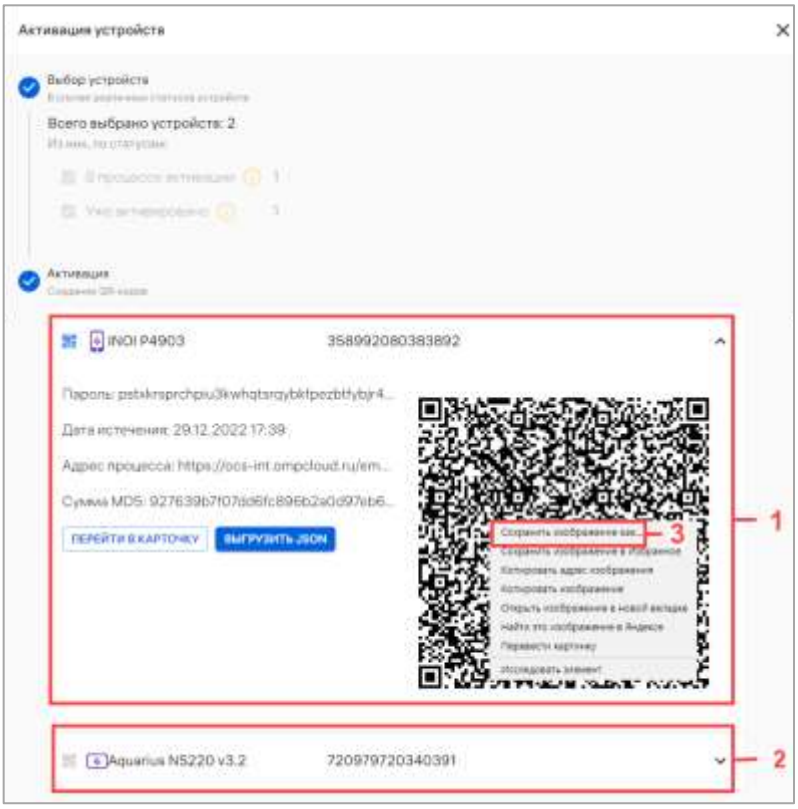

Рисунок 71

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 АДМГ.20134-01 91 01.

QR-код можно скопировать, нажав на него правой кнопкой мыши, и выбрать из списка пункт «Сохранить картинку как...» (Рисунок 71 [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 документе АДМГ.20134-01 90 01-6.

2.2.7.3. 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 70 [1]);

– в списке быстрых действий выбрать значок «Активация устройств» (см. Рисунок 70 [2]);

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

– отобразится окно активации устройств (см. Рисунок 66);

– 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 66 [1]) и нажать кнопку «Дальше» (см. Рисунок 66 [2]);

– откроется окно, где необходимо нажать кнопку «Отправить на Email» (Рисунок 72);

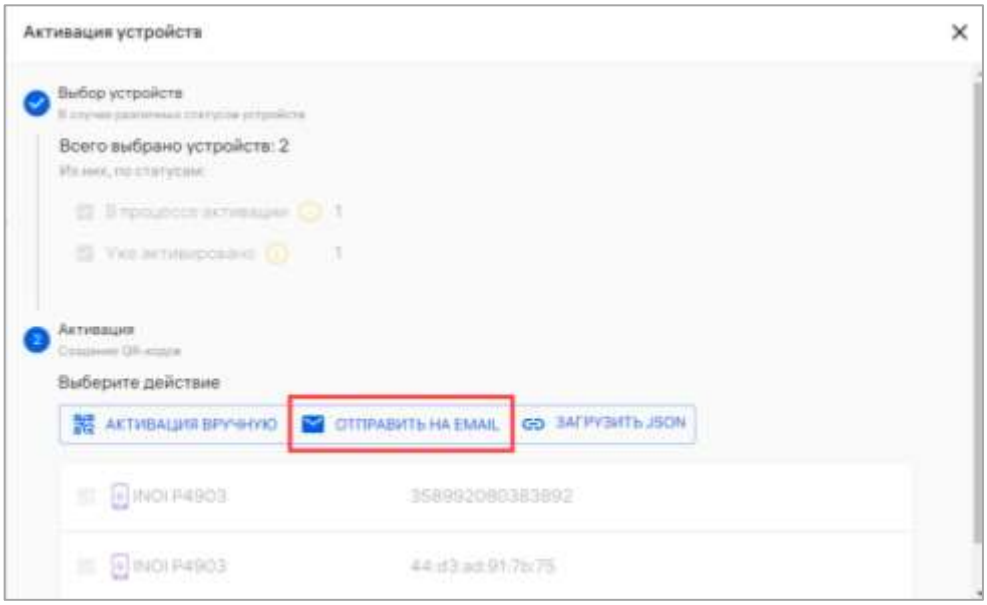

Рисунок 72

– в результате отобразится окно отправки QR-кода на Email, где необходимо ввести Email для писем с активацией (Рисунок 73 [1]);

– нажать кнопку «Отправить» (Рисунок 73 [2]).

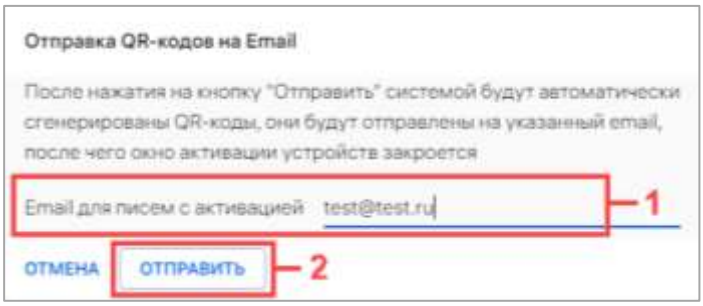

Рисунок 73

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

Подробное описание активации устройств приведено в документе АДМГ.20134-01 90 01-6.

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.

2.2.7.4. Активация группы устройств с помощью JSON-файла

Для активации устройств с помощью JSON-файла необходимо подготовить и загрузить JSON-файл.

Если первоначальная настройка устройств не осуществлялась, необходимо выполнить ускоренную активацию. Подробное описание приведено в документе АДМГ.20134-01 90 01-6.

Если первоначальная настройка устройств была выполнена, необходимо отсканировать QR-код, сгенерированный для группы устройств, в которую входят устройства. Подробное описание приведено в документе АДМГ.20134-01 90 01-6.

2.2.7.4.1. Подготовка JSON-файла

Активация группы устройств единым QR-кодом осуществляется с помощью JSON-файла, который можно сгенерировать в ПУ или подготовить самостоятельно. Пример содержания JSON-файла:

```
{"createdAt":"2020-02-10T11:27:45.897075114+03:00",
"enrollmentID":"beefbeef-0000-4000-8000-000000000000",
"expiredAt":"2020-02-10T11:32:45.780728184+03:00",
"gatewayURI":"https://cloud.ru/mobile",
"password":"QwErt*p$3i2y5"}
```

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

Описание требований к значениям параметров приведено в таблице (Таблица 17).

Таблица 17

Параметр	Описание	Примечание
`createdAt`	Дата генерации QR-кода (дата создания активации)	
`enrollmentID`	Идентификатор созданной активации	При создании QR-кода посредством загрузки 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`	Адрес сервера активации устройств	
`password`	Пароль, присваиваемый 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	При генерации JSON-файла создаются учетные записи устройств. Требования к паролю задаются администратором и могут отличаться от приведенных

2.2.7.4.2. Выгрузка JSON-файла

Для выгрузки JSON-файла необходимо выполнить действия, описанные в пп. 2.2.7.2, до этапа отображения окна активации устройств.

Далее на этапе отображения QR-кода необходимо нажать кнопку «Загрузить JSON» (Рисунок 74).

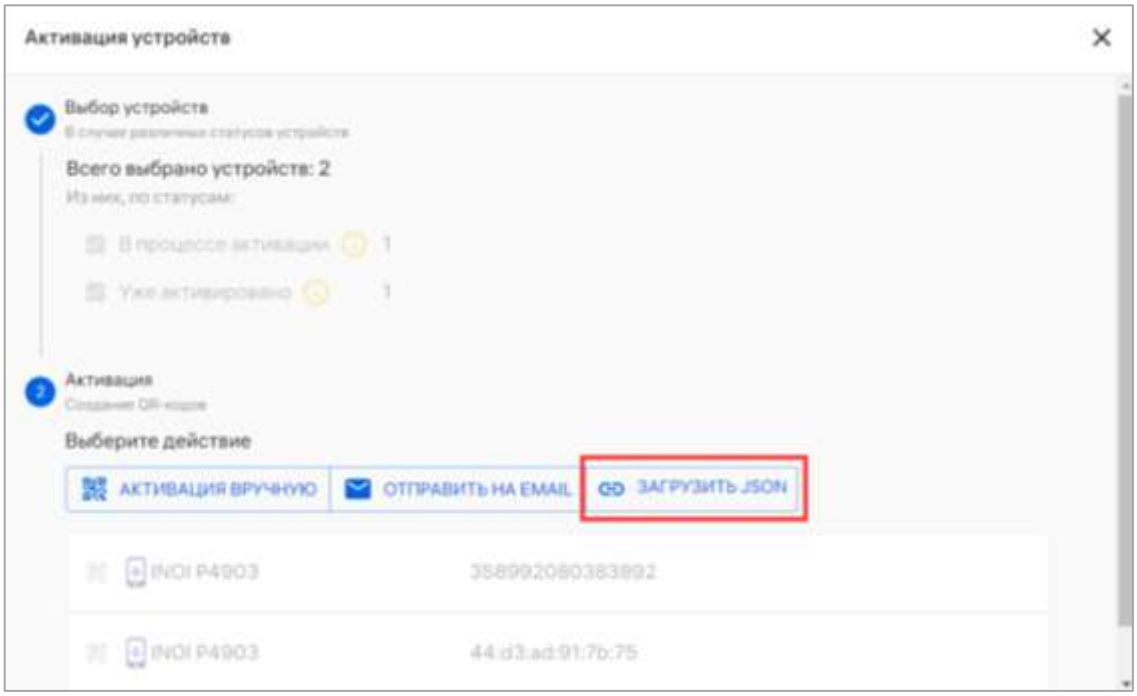

Рисунок 74

В результате на ЭВМ будет выгружен заполненный JSON-файл, при этом статус выбранных устройств в параметре «Жизненный цикл» поменяется на «В процессе активации».

2.2.7.4.3. 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 из списка, при необходимости воспользовавшись фильтром (подраздел 1.5);

– выбрать группу устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения следует нажать кнопку «Сбросить выделение» (Рисунок 75 [1]);

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

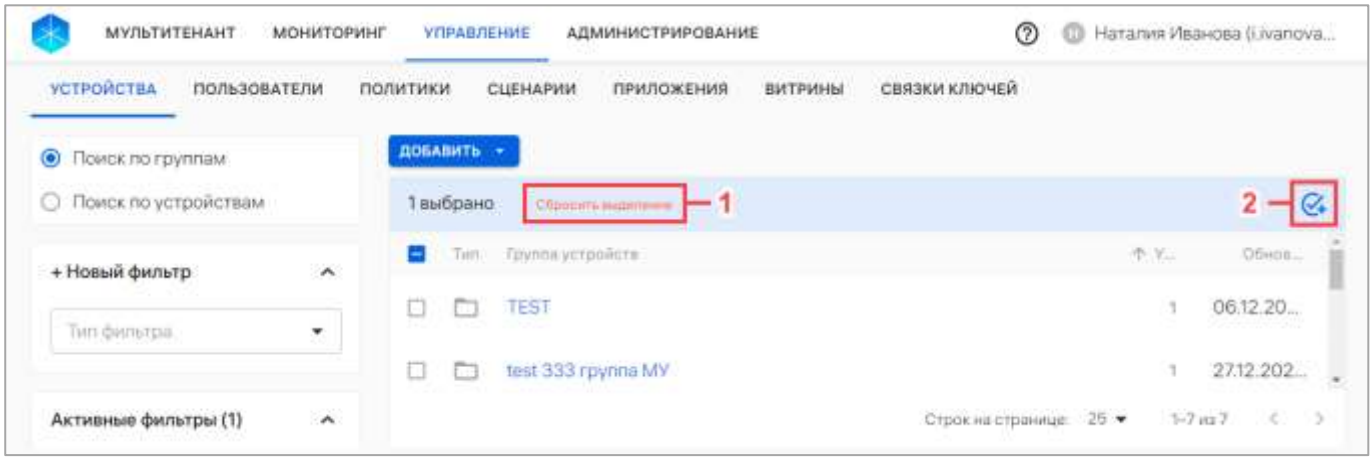

Рисунок 75

– перенести сгенерированный или подготовленный самостоятельно JSON-файл из файлового менеджера в поле загрузки (Рисунок 76);

Рисунок 76

– отобразится информация о загруженном JSON-файле, где необходимо нажать кнопку «Активация вручную» (Рисунок 77 [1]). Для удаления загруженного JSON-файла необходимо нажать кнопку «Удалить JSON» (Рисунок 77 [2]);

Рисунок 77

– в отобразившемся окне активация устройств необходимо нажать кнопку «Продолжить» (Рисунок 78);

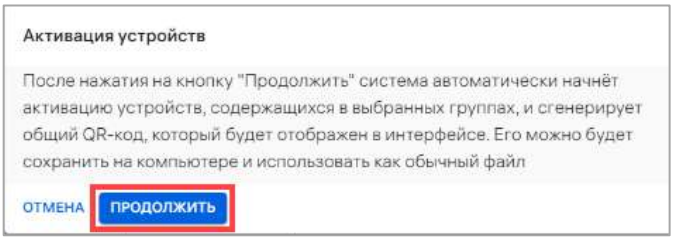

Рисунок 78

– если были выбраны группы, содержащие активированные устройства или в статусе «В процессе активации», отобразится окно подтверждения операции (Рисунок 79), 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.

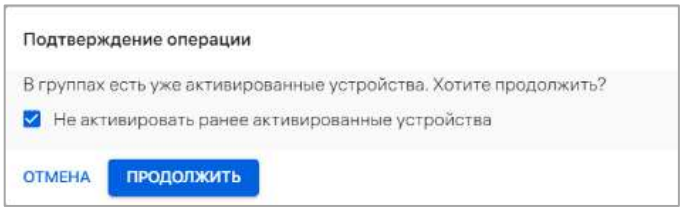

Рисунок 79

В результате JSON-файл будет загружен, и отобразится QR-код для активации группы устройств (Рисунок 80).

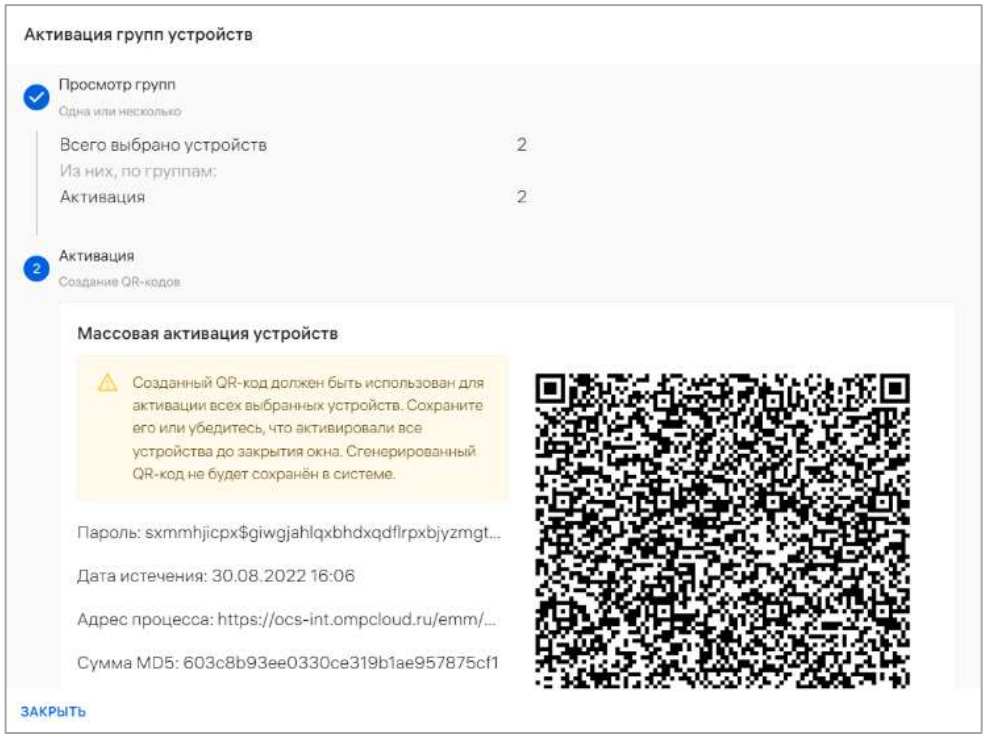

Рисунок 80

Для завершения активации необходимо выполнить следующие действия:

– выполнить ускоренную активацию устройств, если их первоначальная настройка не осуществлялась. Описание процедуры ускоренной активации приведено в документе АДМГ.20134-01 90 01-6;

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

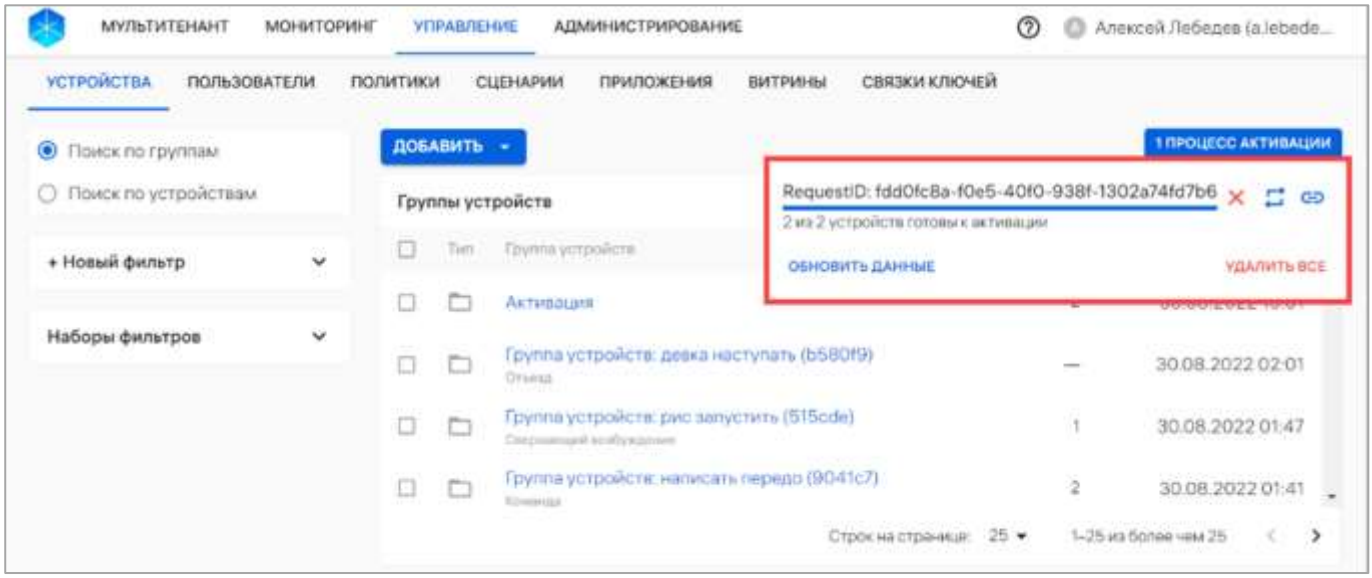

Рисунок 81

Для копирования ссылки процесса необходимо нажать значок «Скопировать ссылку процесса» (Рисунок 81). 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».

2.2.8. Применение оперативных команд

Для применения команд оперативного управления необходимо выполнить следующие действия:

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

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку устройства;

– в открывшейся карточке устройства перейти во вкладку «Состояние»;

– нажать кнопку «Оперативное управление» (Рисунок 82);

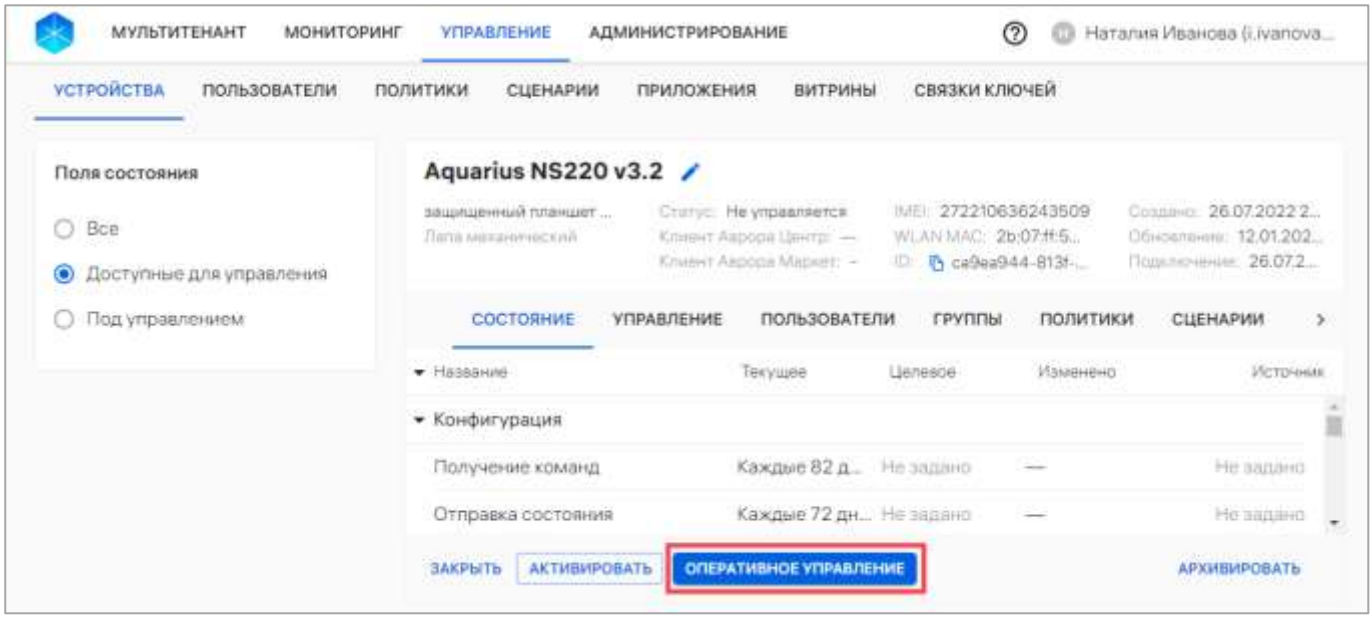

Рисунок 82

– в открывшемся окне выбрать доступные команды (Рисунок 83 [1]), задать необходимые значения согласно таблице (Таблица 18) и нажать кнопку «Активировать изменения» (Рисунок 83 [2]).

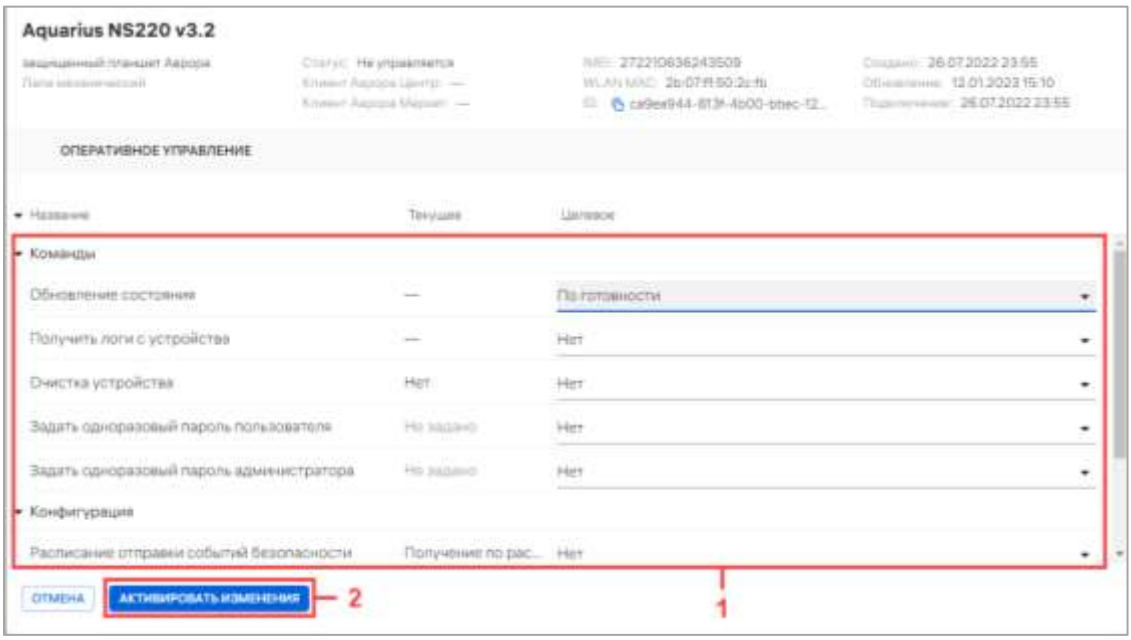

Рисунок 83

В результате отобразится сообщение «Оперативная команда успешно отправлена».

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 15).

Таблица 18

Оперативная команда	Описание	Доступные значения
Команды		
Обновление состояния	Установка расписания обновления состояния устройства	Выбор значения из списка: – «Нет»; – «По готовности» — состояние обновляется в любой момент времени, в который устройство должно прислать состояние; – «По расписанию» — состояние обновляется в момент времени до заданного периода. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]»
Получить логи с устройства	Получение на электронную почту файла со списком системных сообщений об ошибках устройства (Рисунок 85). Название файла – `Reports.tar.bz2`	Выбор значения из списка: – «Нет»; – «По готовности» – письмо будет отправлено на электронную почту текущего оператора (Рисунок 84). При необходимости данное значение можно отредактировать в поле ввода. Если Email оператора не заполнен или не является действительным (например, в

Оперативная команда	Описание	Доступные значения
		созданном тенанте), необходимо ввести его вручную
Очистка устройства	Очистка всех данных пользователя, включая данные с внешнего носителя (карты памяти microSD) для сохранения конфиденциальности данных в случае утери или кражи устройства. 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	Выбор значения из списка: – «Нет»; – «Очистка устройства»
Задать одноразовый пароль пользователя	Установка одноразового пароля пользователя для разблокировки устройства в случае, если пользователь не знает или не помнит пароль. Пароль должен содержать от 7 до 12 символов и должен соответствовать требованиям парольной политики. После установки пароля пользователь должен выполнить входа под своей учетной записью (в режиме пользователя), ввести одноразовый пароль, затем выбрать предлагаемый устройством новый пароль или самостоятельно задать новый пароль.	Выбор значения из списка: – «Задать пароль» - ввод значения с клавиатуры; – «Нет»

Оперативная команда	Описание	Доступные значения
	ВНИМАНИЕ! Оперативная команда «Задать одноразовый пароль пользователя» недоступна для корпоративной версии ОС Аврора релиз 3.x.x	
Задать одноразовый пароль администратора	Установка одноразового пароля администратора для разблокировки устройства в случае, если пользователь не знает или не помнит пароль. Пароль должен содержать от 7 до 12 символов и соответствовать требованиям парольной политики. После установки пароля администратор должен загрузить устройство в режиме администратора, ввести одноразовый пароль на устройстве, затем выбрать предлагаемый устройством новый пароль. Если учетная запись администратора была заблокирована на устройстве, после установки одноразового пароля учетная запись администратора будет разблокирована. ВНИМАНИЕ! Оперативная команда «Задать одноразовый пароль администратора» недоступна для корпоративной версии ОС Аврора релиз 3.x.x	Выбор значения из списка: – «Задать пароль» — ввод значения с клавиатуры; – «Нет»

Оперативная команда	Описание	Доступные значения
Конфигурация		
Расписание отправки событий безопасности	Установка расписания отправки сообщений о произошедших на устройствах событиях безопасности	Выбор значения из списка: – «Нет»; – «Временная установка» — сообщения доставляются по заданному расписанию и в заданный интервал времени. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»; – «Отменить отправку» — на устройствах применяются назначенные политики или настройки по умолчанию, если политик не назначено
Система		
Блокировка экрана	Блокировка экрана устройства для предотвращения его использования посторонними лицами в случае утери или кражи. В результате блокировки устройства на экране блокировки отображается сообщение: «Заблокировано при помощи Aurora Device Manager. Заблокировано администратором». Использование устройства до разблокировки невозможно, кроме совершения экстренного вызова	Выбор значения из списка: – «Временная блокировка» — указание периода блокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]». Также доступна возможность ввода сообщения, которое будет отображаться на экране заблокированного устройства. Для этого необходимо ввести текст сообщения в поле «Сообщение при блокировке»;

Оперативная команда	Описание	Доступные значения
		– «Временная разблокировка» — период разблокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]»
Использование камеры	Установка запрета/разрешения использовать камеру на устройствах	Выбор значения из списка: – «Временно запретить»; – «Временно разрешить»
Использование микрофона	Установка запрета/разрешения использование микрофона на устройствах	Выбор значения из списка: – «Временно запретить»; – «Временно разрешить»

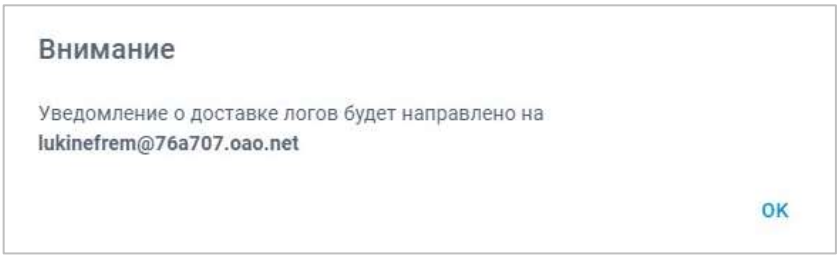

Рисунок 84

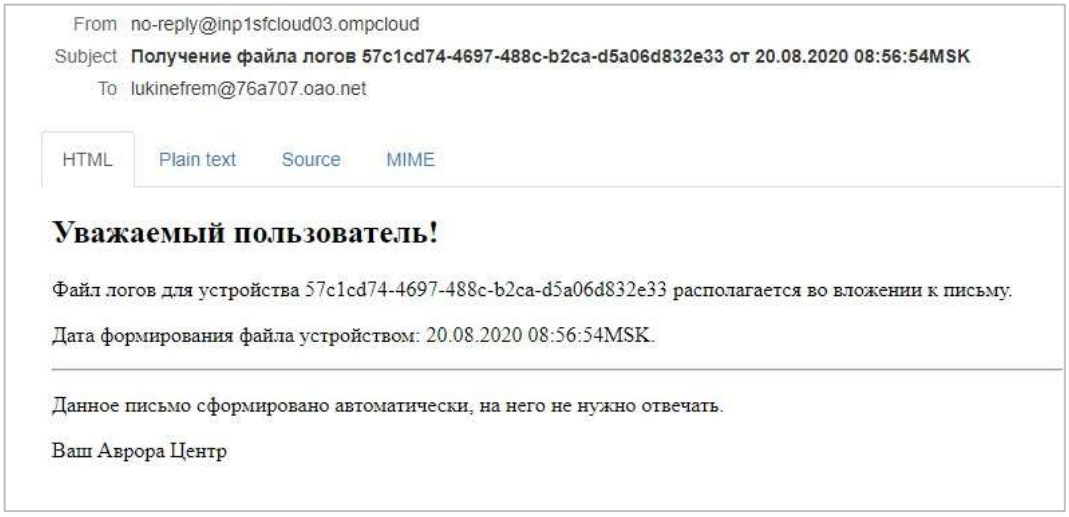

Рисунок 85

2.2.9. Отвязка (удаление) 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. 2.2.9.1);

– каточку группы устройств (пп. 2.2.9.2).

2.2.9.1. Отвязка (удаление) 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»;

– в рабочей области выбрать устройство, при необходимости воспользовавшись фильтром и перейти в карточку 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 86 [1]);

– в списке быстрых действий нажать значок «Исключить устройство из группы» (Рисунок 86 [2]);

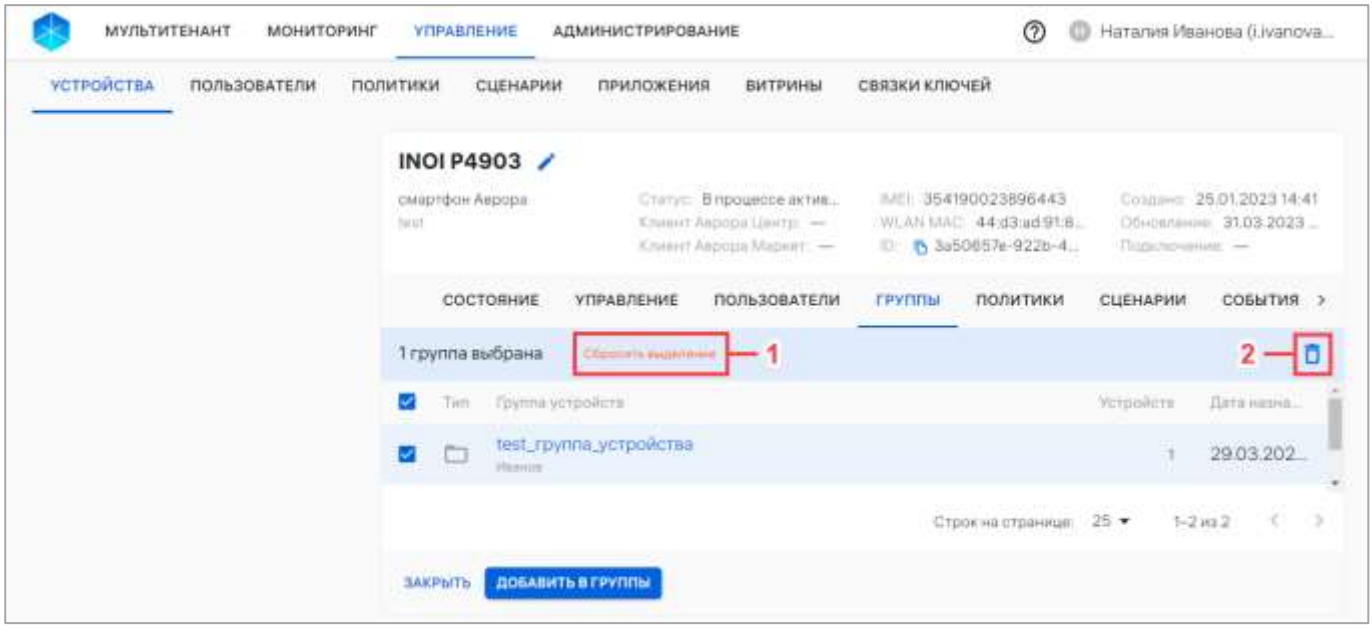

Рисунок 86

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия (Рисунок 87).

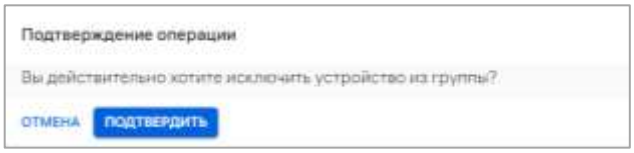

Рисунок 87

В результате подтверждения отобразится сообщение «Устройство исключено из группы». Политики будут перекомбинированы таким образом, что для устройства будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.9.2. Отвязать (удаление) устройства из 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»;

– в рабочей области выбрать группу устройств, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы устройств;

– 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 88 [1]);

– в списке быстрых действий нажать значок «Отвязать устройства от группы» (Рисунок 88 [2]);

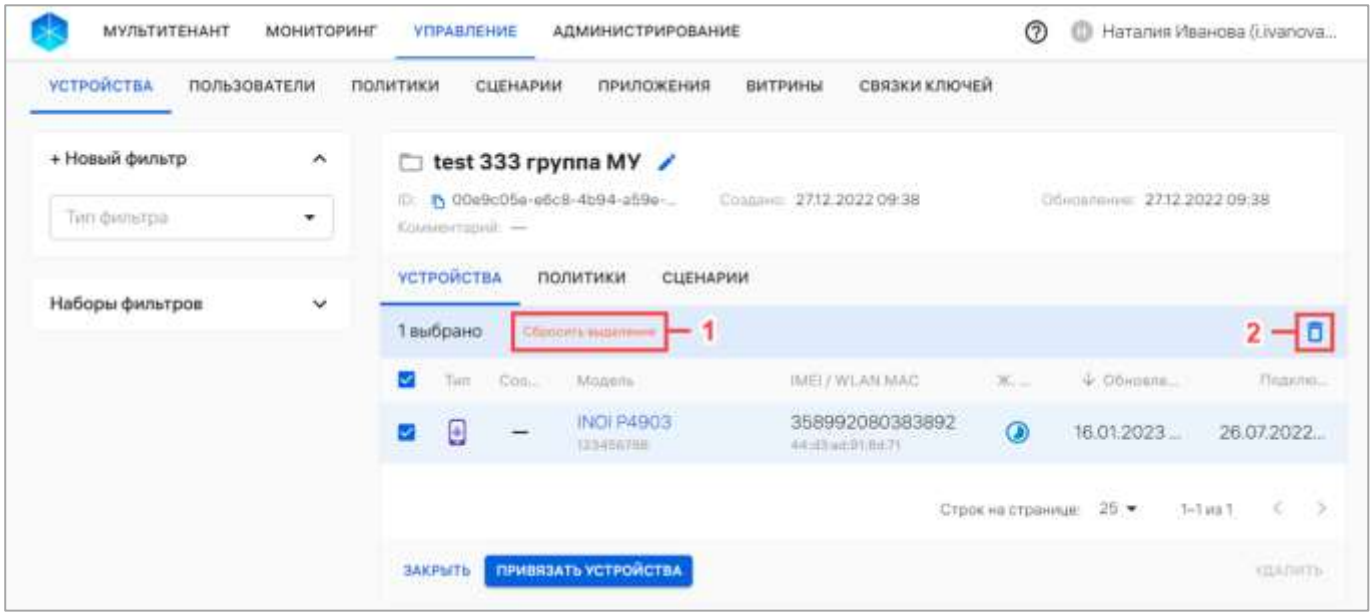

Рисунок 88

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

Рисунок 89

В результате подтверждения отобразится сообщение «[количество устройств] устройство успешно отвязано от группы». Политики будут перекомбинированы таким образом, что для устройств будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.10. 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. 2.2.11.

Перед архивированием активированного устройства необходимо очистить его с помощью оперативных команд (п. 2.2.8).

Архивирование устройства может быть выполнено:

– в подразделе «Устройства» с помощью списка быстрых действий (пп. 2.2.10.1);

– с помощью карточки устройства (пп. 2.2.10.2).

2.2.10.1.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 90 [1]);

– в списке быстрых действий выбрать значок «Архивировать» (Рисунок 90 [2]);

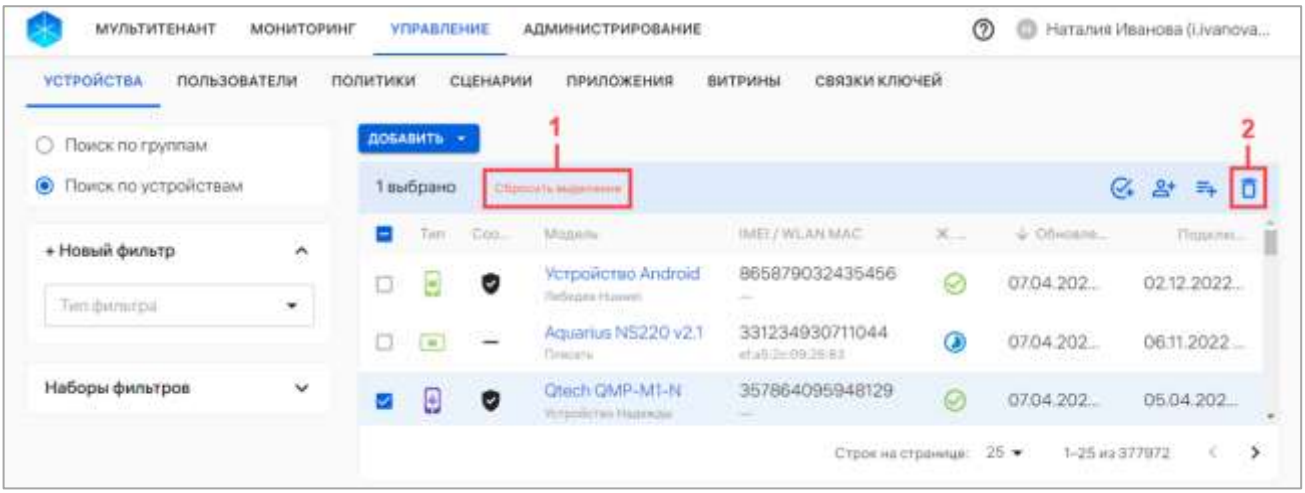

Рисунок 90

– если выбранные устройства были очищены, то отобразится окно подтверждения операции, где необходимо нажать кнопку «Архивировать» (Рисунок 91).

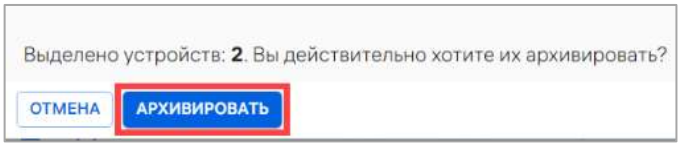

Рисунок 91

Если одно или несколько устройств не очищены, отображается сообщение (Рисунок 92), в котором необходимо выбрать соответствующую кнопку:

– для архивирования только очищенных устройств нажать кнопку «Архивировать только очищенные» (Рисунок 92);

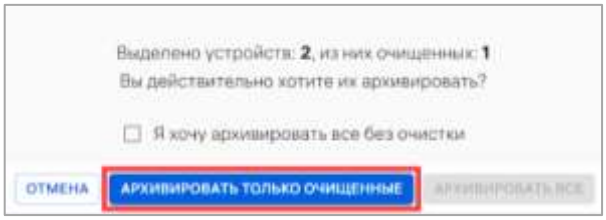

Рисунок 92

– для архивирования без очистки необходимо:

1) подтвердить архивирование без очистки, установив галочки в чекбоксе (Рисунок 93 [1]);

2) нажать кнопку «Архивировать все» (Рисунок 93 [2]).

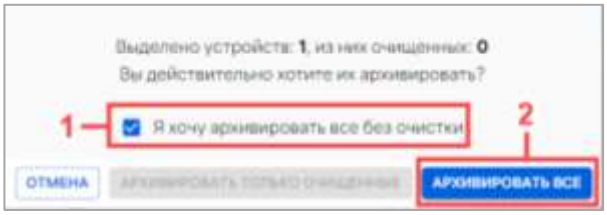

Рисунок 93

В результате отобразится сообщение «Устройство архивировано». Учетные записи устройства будут заблокированы.

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

2.2.10.2.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»;

– выбрать устройство из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку устройства;

– в открывшейся карточке устройства перейти во вкладку «Состояние»;

– нажать кнопку «Архивировать» (Рисунок 94);

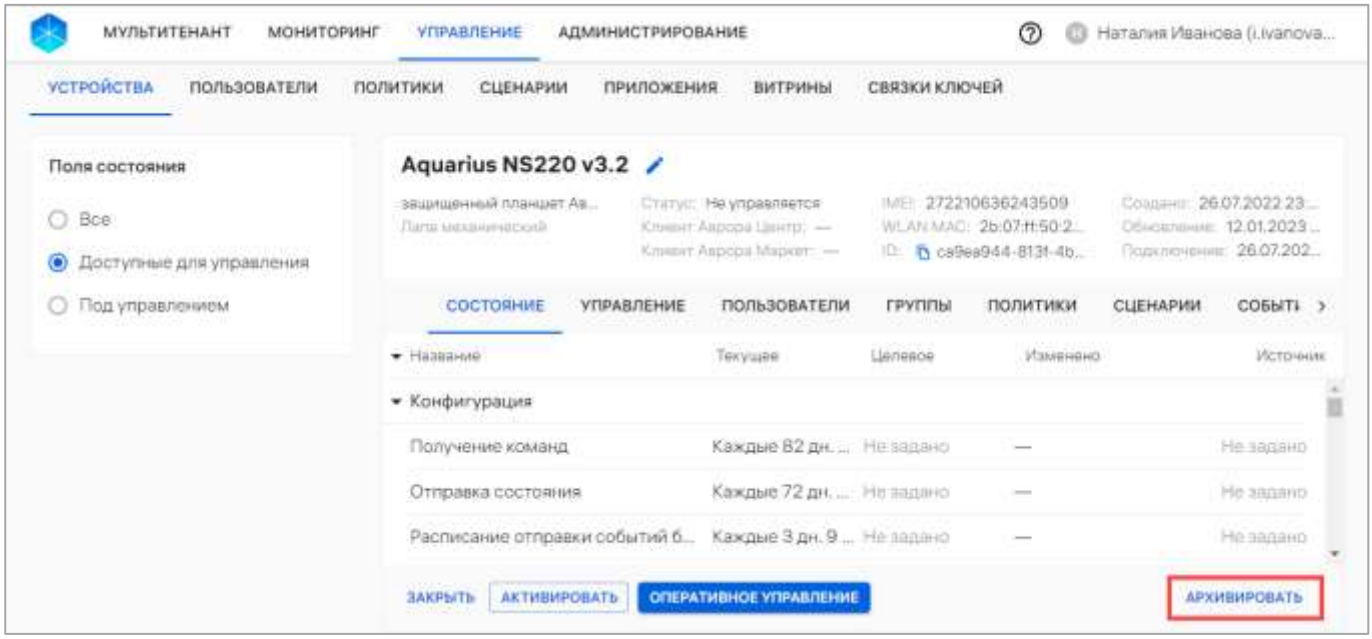

Рисунок 94

– если устройство не очищено, отобразится соответствующее сообщение. Для подтверждения архивирования необходимо нажать кнопку «Архивировать» (Рисунок 95).

Рисунок 95

В результате отобразится сообщение «Устройство архивировано». Учетные записи устройства будут заблокированы.

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

2.2.11. 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 96 [1]);

– выбрать значок «Активация устройств» (Рисунок 96 [2]);

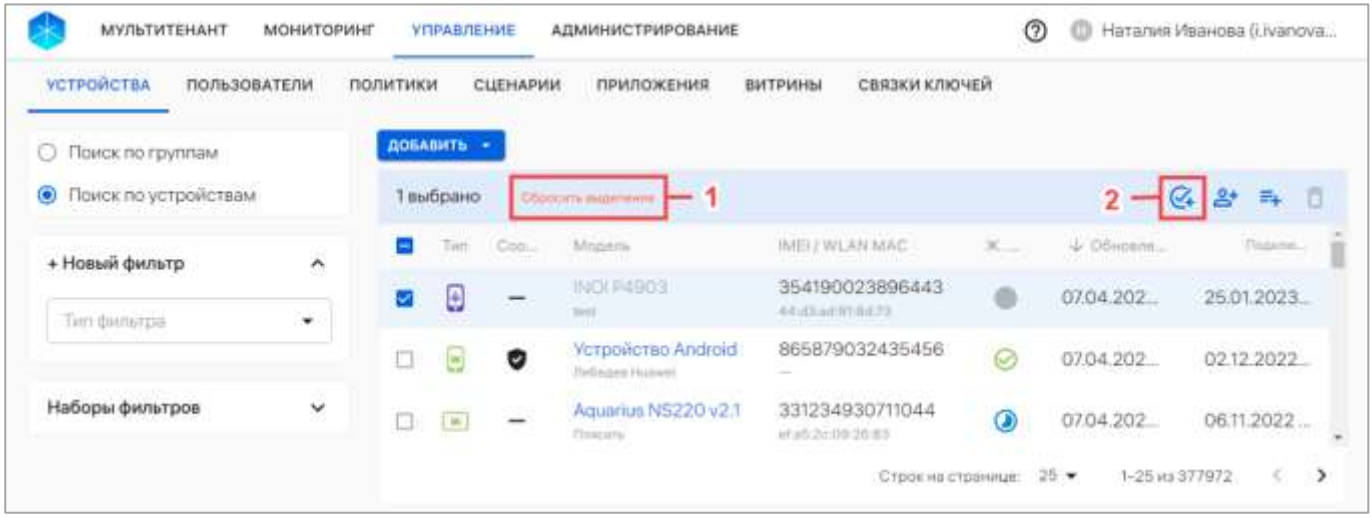

Рисунок 96

– в отобразившемся окне активации устройств установить галочку в чекбоксе «Перенесено в архив» (Рисунок 97 [1]) и нажать кнопку «Дальше»(Рисунок 97 [2]).

Рисунок 97

При наличии у устройств связей со статистическими группами и/или пользователями на шаге «Восстановление связей» необходимо подтвердить восстановление связей, установив галочку в чекбоксе (Рисунок 98 [1]), и нажать кнопку «Дальше» (Рисунок 98 [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 98

Далее активировать устройства возможно одним из способов:

1) нажать кнопку «Отправить на Email» (Рисунок 99 [1]), в открывшемся окне ввести адрес электронной почты и далее нажать кнопку «Отправить»;

2) нажать кнопку «Активация вручную» (Рисунок 99 [2]) и далее нажать кнопку «Продолжить».

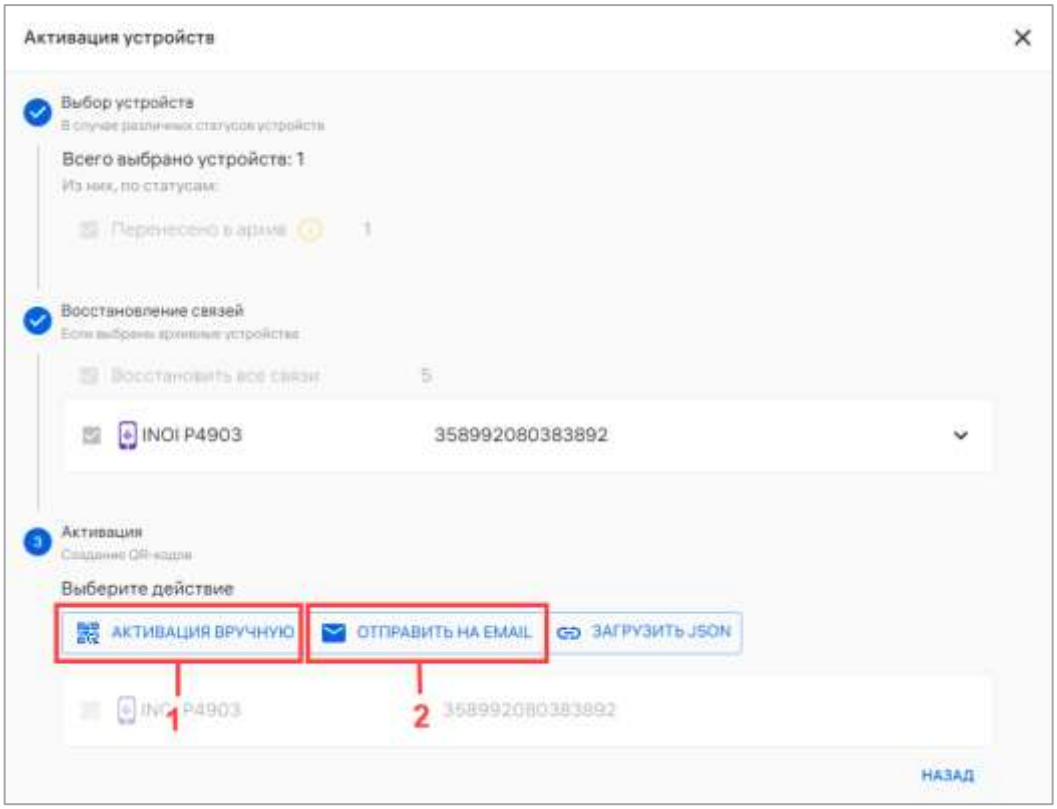

Рисунок 99

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

Для завершения активации необходимо отсканировать QR-код на устройстве. Описание процесса активации устройств приведено в документе АДМГ.20134-01 90 01-6.

2.2.12. Удаление группы устройств

ПРИМЕЧАНИЕ. Перед удалением группы устройств необходимо предварительно исключить все устройства из группы в соответствии с п. 2.2.9.

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»;

– выбрать группу устройств из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке перейти во вкладку «Устройства» и удалить все устройства из группы (пп. 2.2.9.2);

– в карточке группы устройств нажать кнопку «Удалить» (Рисунок 100);

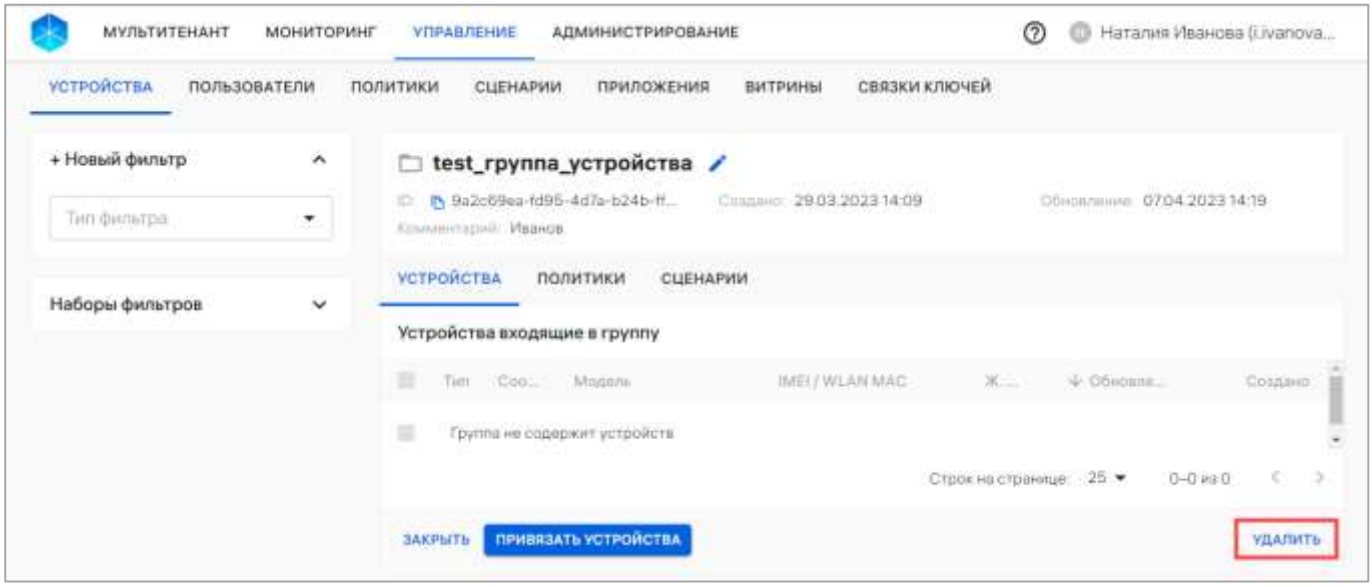

Рисунок 100

– в отобразившемся окне (Рисунок 101) подтвердить либо отменить действия.

Рисунок 101

В результате успешного удаления отобразится сообщение «Группа удалена».

2.2.13. Очистка устройств до заводских настроек

Для сброса устройства до заводских настроек необходимо назначить оперативную команду «Очистка устройства» (см. Таблица 18) в соответствии с п. 2.2.8,

в результате чего отобразится окно подтверждения операции, где необходимо нажать кнопку «Очистить» (Рисунок 102).

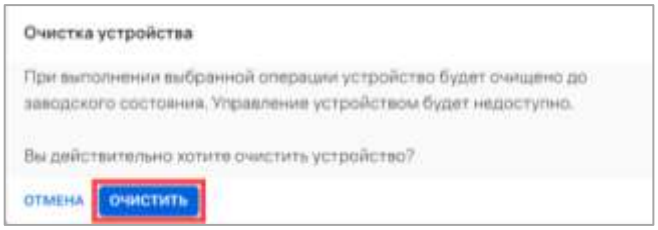

Рисунок 102

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

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. 2.2.7).

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

2.2.14. Вывод устройства из эксплуатации

ПРИМЕЧАНИЕ. 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»;

– выбрать устройство из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку устройства;

– в открывшейся карточке устройств перейти во вкладку «Сценарии»;

– нажать кнопку «Вывести из эксплуатации» (Рисунок 103);

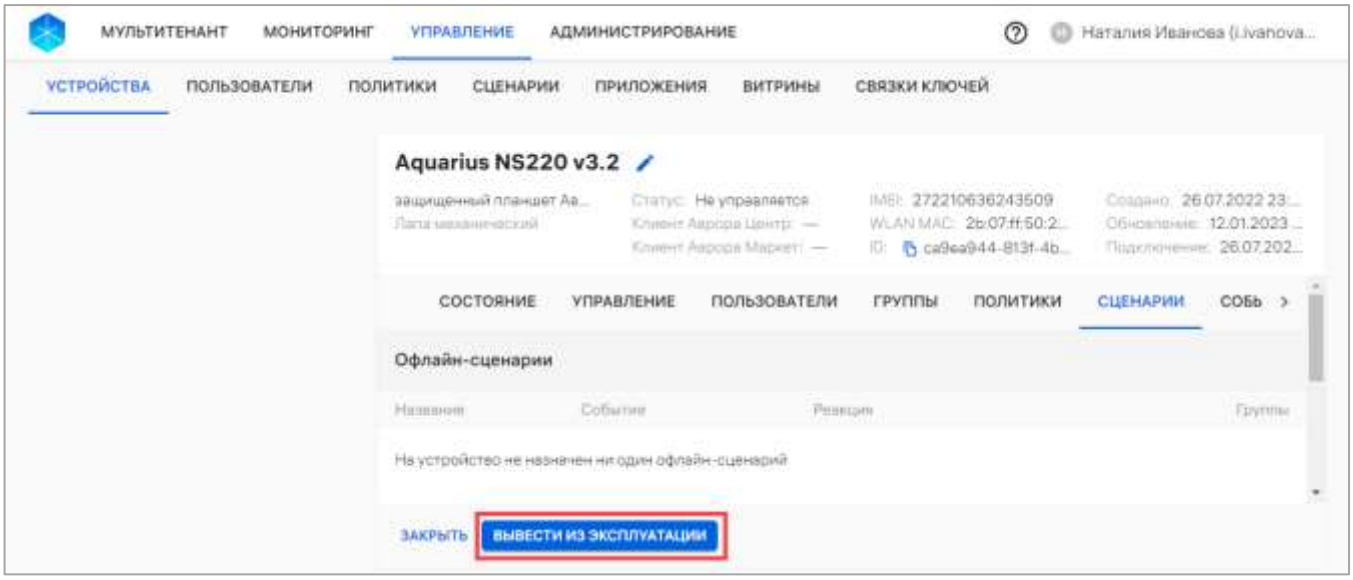

Рисунок 103

– в отобразившемся окне подтверждения операции (Рисунок 104) подтвердить либо отменить действия.

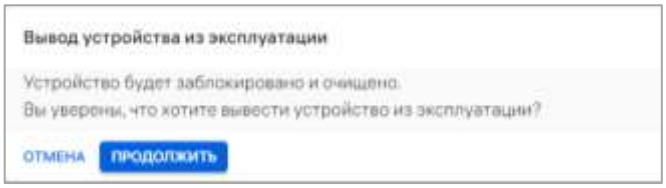

Рисунок 104

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 105 [2]).

ПРИМЕЧАНИЕ. Для отображения группы пользователей необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 105 [1]).

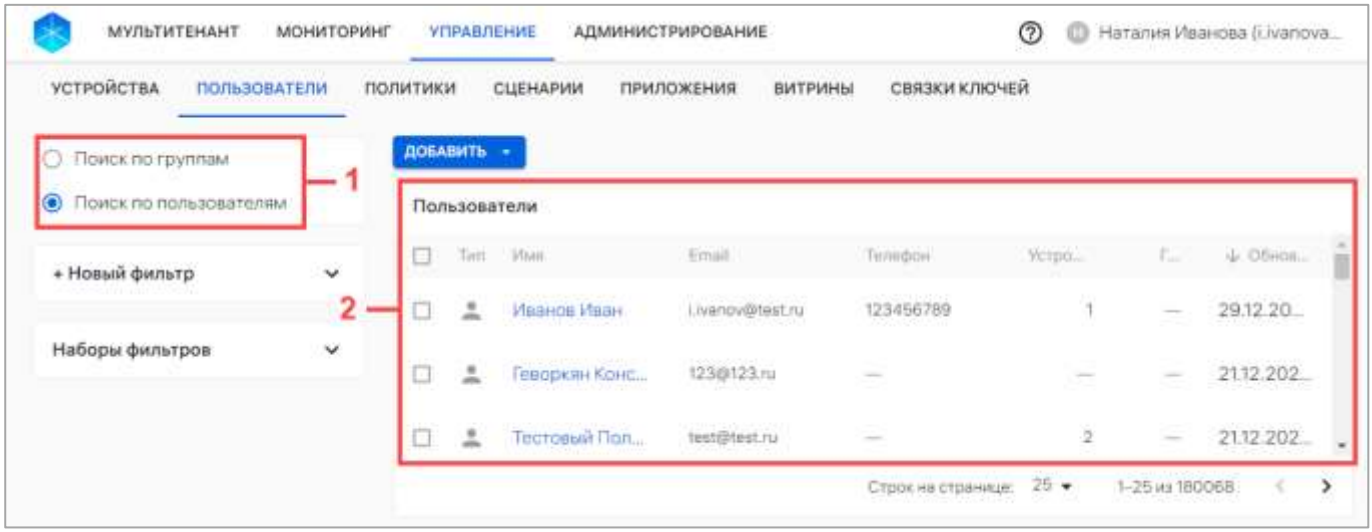

Рисунок 105

В рабочей области информация о пользователях и группах пользователей отображается в столбцах, приведенных в таблице (Таблица 19), а при отсутствии добавленных пользователей или групп пользователей отображается сообщение «Нет данных».

Таблица 19

Название столбца	Значение		Описание
Пользователи			
Тип		Пользователь	Пользователь, добавленный в ПУ вручную или с помощью импорта CSV-файла
		Пользователь из орг. Подразделения	Пользователь, полученный из LDAP)
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		Значение столбца отсортировано в направлении стрелки: от старых к новым, от новых к старым
Группы	Количество групп, к которым привязан пользователь		
Обновлено	Дата обновления		
Группа пользователей			
Тип		Группа пользователей	Группа пользователей, созданная вручную или с помощью импорта CSV-файла
		Организационное подразделение	Группа пользователей, полученная из LDAP
Группа пользователей	Название группы пользователей		Представляет собой активную ссылку, при нажатии на которую происходит переход к карточке группы пользователей
	Комментарий		Заполняется при необходимости
Пользователей	Количество пользователей, привязанных к группе		Значение столбца отсортировано в направлении стрелки: от старых к новым, от новых к старым
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 2.3.2);

– с помощью импорта CSV-файла (п. 2.3.3).

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 106);

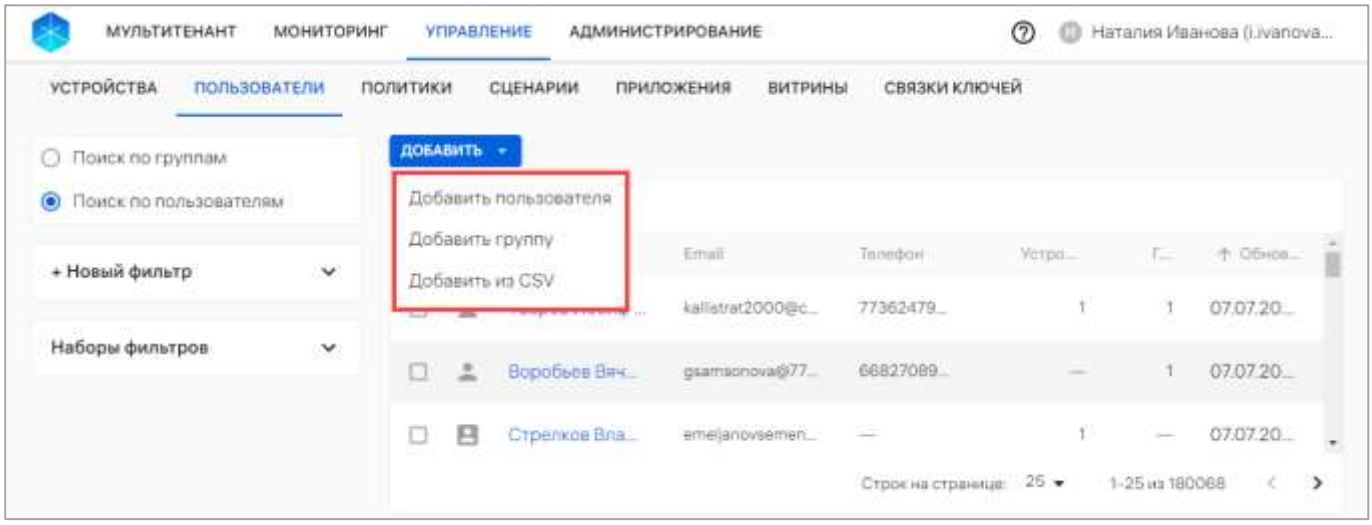

Рисунок 106

– в открывшемся окне «Новый пользователь» (Рисунок 107) ввести данные о пользователе (Таблица 20);

Таблица 20

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
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 107).

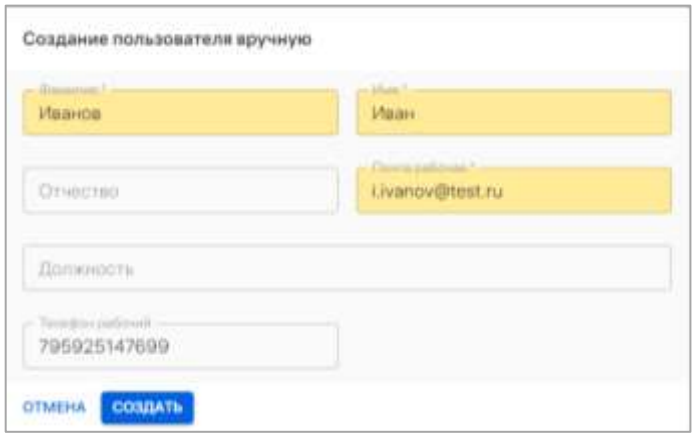

Рисунок 107

В результате успешного добавления пользователя отобразится сообщение «Пользователь успешно создан» и откроется его карточка. Описание процесса работы с карточкой пользователя приведено в п. 2.1.3.

2.3.2. Добавление группы пользователей вручную

Для добавления группы пользователей вручную необходимо выполнить следующие действия:

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

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить группу» (см. Рисунок 106);

– в открывшемся окне «Создание группы пользователей» (Рисунок 108) заполнить поля (Таблица 21).

Таблица 21

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 108).

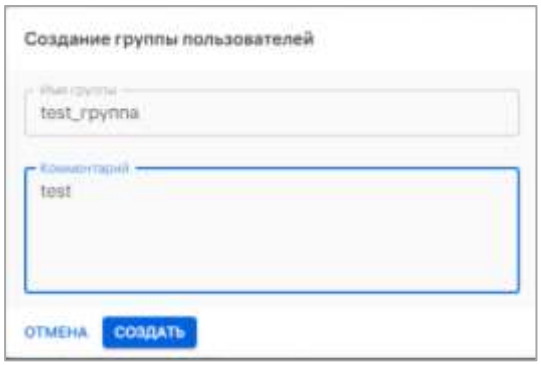

Рисунок 108

В результате отобразится сообщение «Группа успешно создана» и откроется карточка добавленной группы пользователей. Подробное описание работы с карточкой группы пользователей приведено в п. 2.1.4.

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 106);

– в открывшемся окне «Импорт пользователей из CSV» нажать «Шаблон .CSV» (Рисунок 109). В результате шаблон файла для импорта будет выгружен. Требования к заполнению CSV-файлов приведены в таблице (Таблица 22), пример заполнения CSV-файлов приведен в пп. 2.3.3.2.

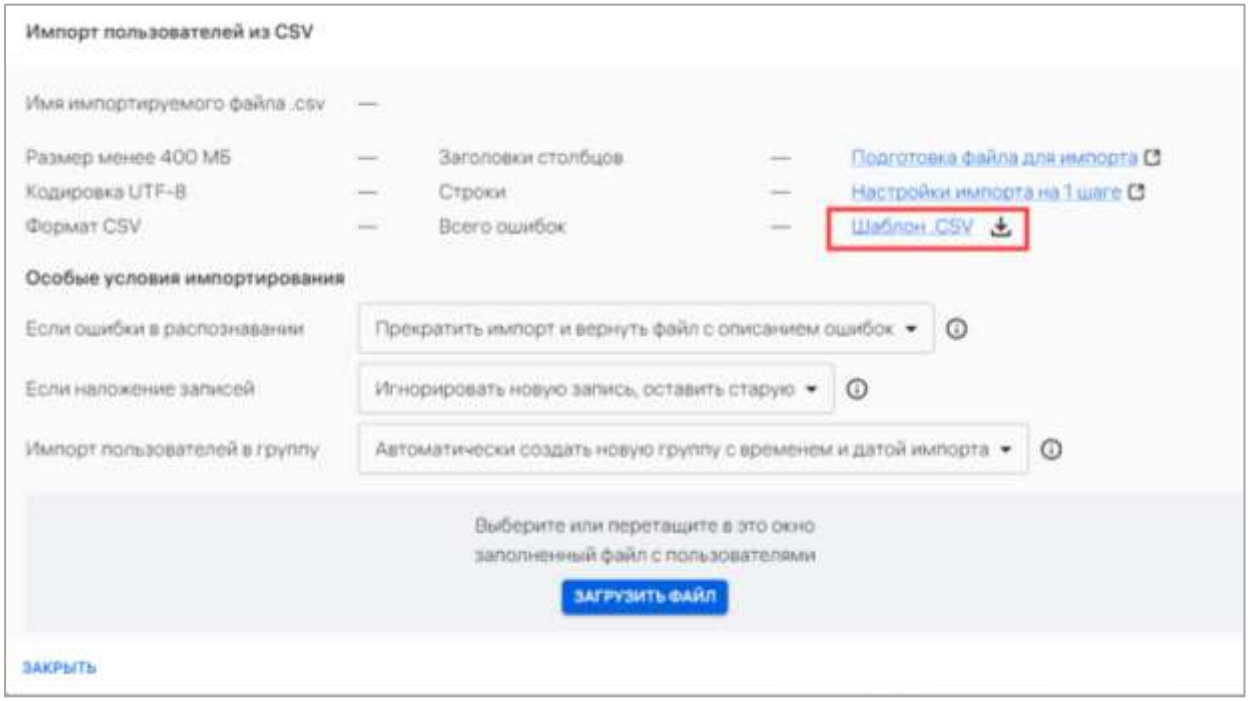

Рисунок 109

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,WLAN_MAC,STRATEGY»). 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»;

– строки с пробелами или запятыми должны заключаться в кавычки «"» (если в строке требуется передать кавычку, ее необходимо удвоить).

Описание требований к значениям параметров приведено в таблице (Таблица 22).

Таблица 22

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. 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

Параметр	Описание	Примечание
EMAIL	Рабочая почта пользователя. Содержит 1 до 256 символов	Рабочая почта пользователя должна быть уникальной для каждого пользователя. 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 обязателен для заполнения при: – добавлении нового пользователя; – привязке пользователя к группе
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	Параметр обязателен для заполнения при: – добавлении нового пользователя; – привязке пользователя к группе
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 и имеет длину от 2 до 64 символов	Параметр не обязателен для заполнения

Параметр	Описание	Примечание
IMEI	Международный идентификатор мобильного оборудования. Содержит 15 цифр. **ПРИМЕЧАНИЕ.** Если устройство поддерживает работу 2 SIM-карт, в поле «IMEI» допускается ввод любого из 2 значений IMEI	Параметр обязателен для заполнения, если устройство, которое зарегистрировано в ПУ по IMEI, привязывается 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, которое зарегистрировано в ПУ по MAC-адресу WLAN, привязывается к пользователю
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. Примеры заполненных CSV-файлов

В зависимости от содержимого CSV-файла при загрузке в Консоли администратора ПУ происходит:

– добавление новых пользователей;

– добавление новых устройств;

– добавление новых групп пользователей;

– привязка/отвязка пользователей к/от устройств.

Для добавления новых пользователей необходимо указать значение обязательных параметров «EMAIL», «FIRST_NAME» и «LAST_NAME»:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMB
ER,IMEI,WLAN_MAC
,i.ivanov@doc.ru,Игорь,Иванов,,,,,
,d.dolin@doc.ru,Дмитрий,Долин,,,,,
```

Для добавления новых групп пользователей необходимо указать название группы в параметре «GROUP»:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMB
ER,IMEI,WLAN_MAC
"Пользователи INOI T10",,,,,,,,
"Пользователи MIG C55",,,,,,,,
```

Для привязки пользователей к устройству необходимо указать значение одного из обязательных параметров «IMEI» или «WLAN_MAC», а также заполнить обязательные параметры «EMAIL», «FIRST_NAME» и «LAST_NAME»:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMB
ER,IMEI,WLAN_MAC
,i.ivanov@doc.ru,Игорь,Иванов,,,,350081328638495,
,d.dolin@doc.ru,Дмитрий,Долин,,,,350422453760656,
```

Пример полностью заполненного CSV-файла:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMB
ER,IMEI,WLAN_MAC
"Пользователи INOI T10",i.ivanov@doc.ru,Игорь,Иванов,Иванович,
"Дежурный СТО",9000900000,350081328638495,20:B9:58:5B:48:DF
"Пользователи MIG C55",d.dolin@doc.ru,Дмитрий,Долин,Петрович,
"Руководитель СТО",9000100000,350422453760656,03:E7:97:7B:78:DF
```

2.3.3.3. 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 106);

– в открывшемся окне «Импорт пользователя из CSV» задать особые условия импортирования, приведенные в таблице (Таблица 23).

Таблица 23

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 110 [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 110 [1],[2]). В результате отобразится текст подсказки следующего содержания: при завершении импорта система предоставит 2 файла: список системных сообщений ошибок

Наименование полей	Описание	Примечание
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 110 [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. **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	распознавания и Журнал успешно импортированных устройств
Импорт пользователей в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 110 [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;	В поле содержится подсказка, доступная для просмотра нажатием значка (Рисунок 110 [3]). В результате отобразится текст подсказки следующего содержания: в процессе импорта система может помещать все

Наименование полей	Описание	Примечание
	– **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	устройства в одну из имеющихся групп или создать новую

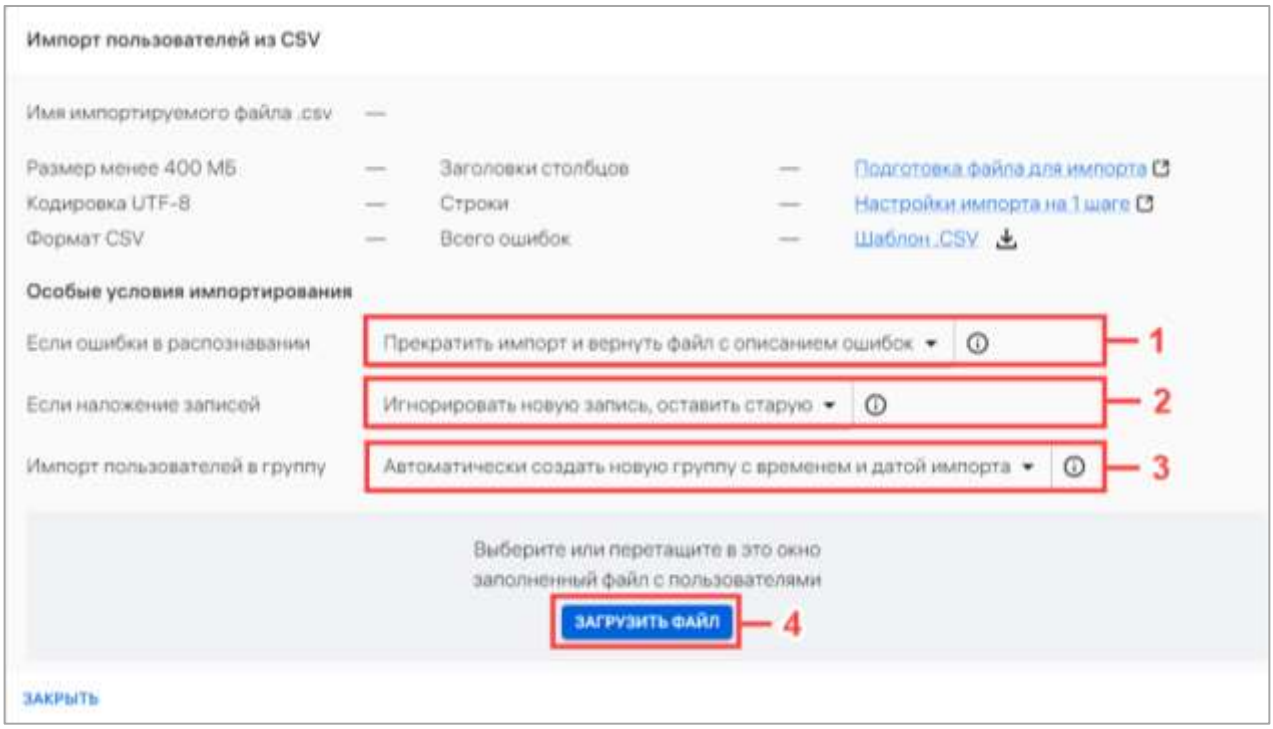

Рисунок 110

– далее необходимо загрузить CSV-файл одним из способов:

- переместить CSV-файл в область загрузки;
- нажать кнопку «Загрузить файл» (см. Рисунок 110 [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 111).

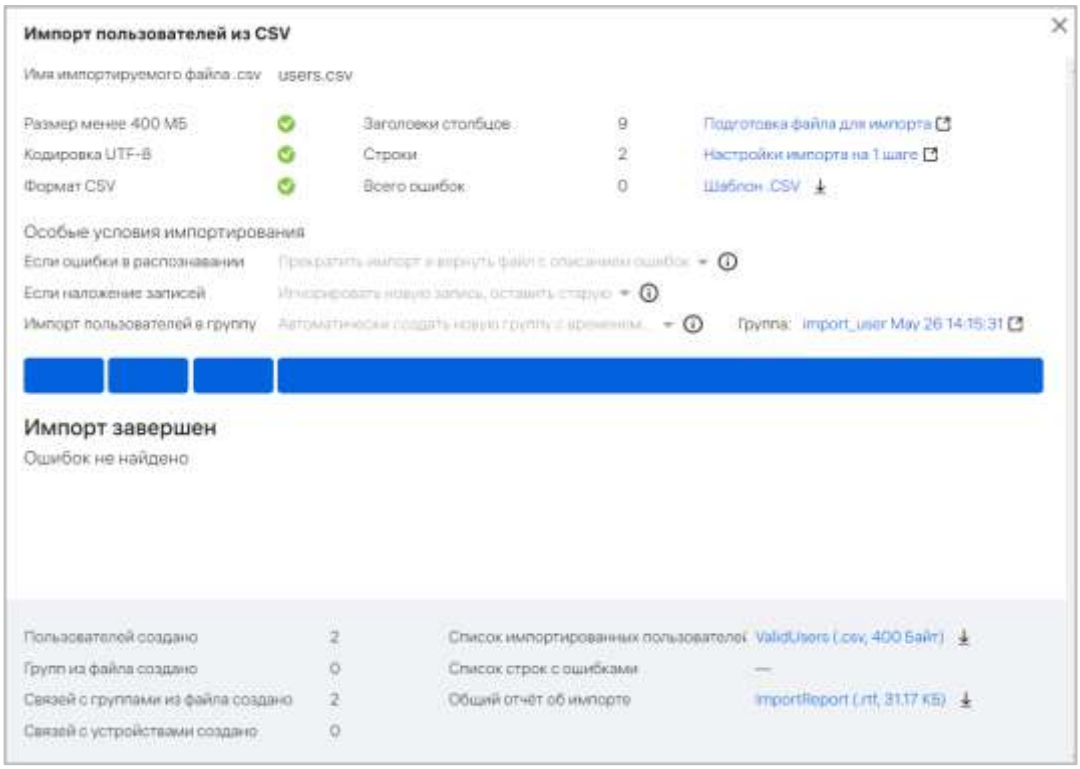

Рисунок 111

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 112 [6]).

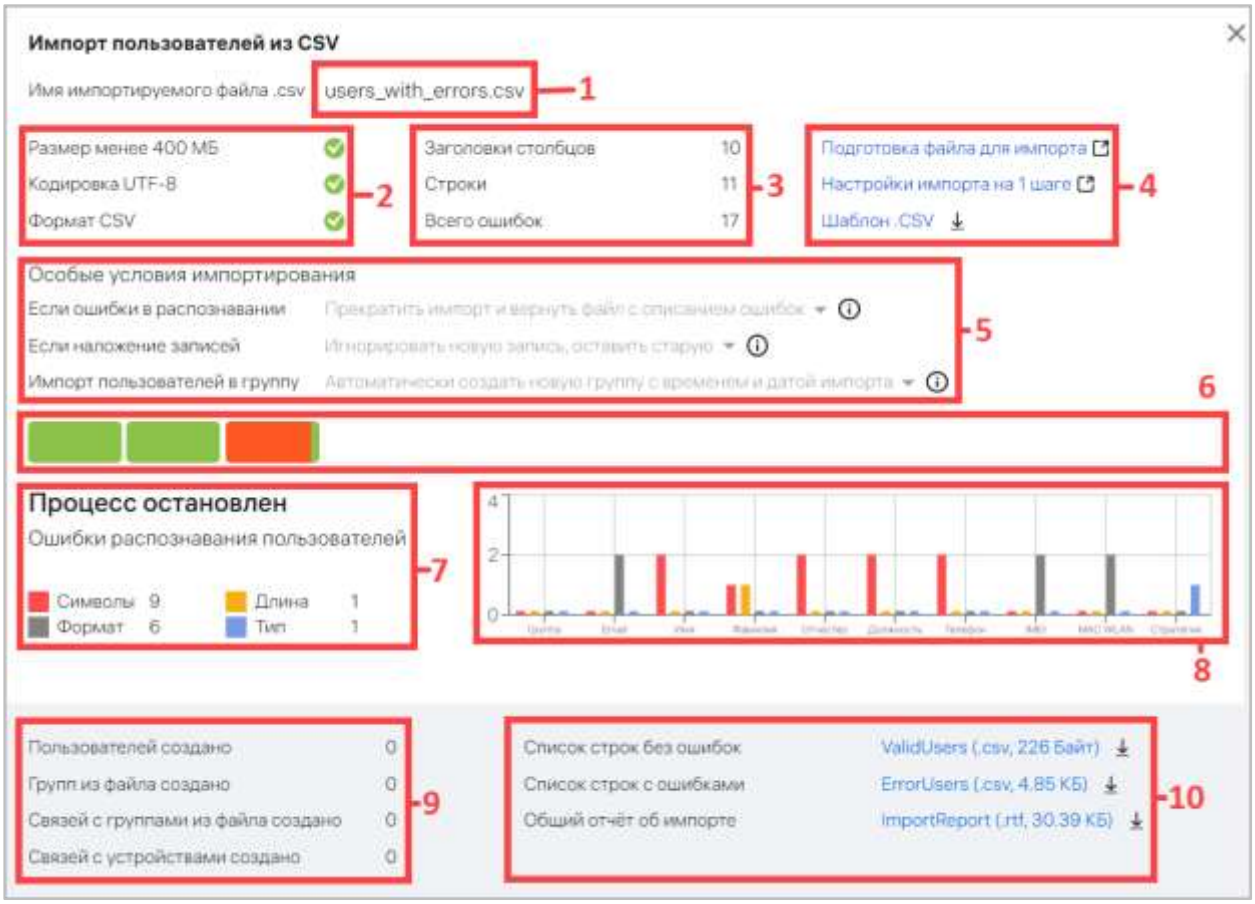

Рисунок 112

В окне с результатами импорта пользователей отображается следующая информация:

– название импортируемого файла (Рисунок 112 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (Рисунок 112 [2]);

– количество столбцов, всех импортируемых строк и ошибок в файле (при их наличии) (Рисунок 112 [3]);

– Ссылки (Рисунок 112 [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 ((Рисунок 112 [5]), см. Таблица 23);

– шкала прогресса импорта (Рисунок 112 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (Рисунок 112 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (Рисунок 112 [8]);

– количество созданных пользователей, групп пользователей, связей пользователей с группами и устройствами (Рисунок 112 [9]);

– ссылки на скачивание отчетов (Рисунок 112 [10]):

- отчет со списком импортированных пользователей. Формат отчета — `.csv`.
- отчет со списком строк, содержащих ошибки и с указанием причины ошибки. Формат отчета — `.csv` (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);
- 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 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).

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 113 [1], Рисунок 114 [1]);

– в списке быстрых действий выбрать значок (Рисунок 113 [2]) или (Рисунок 114 [2]) «Привязать пользователей к группам»;

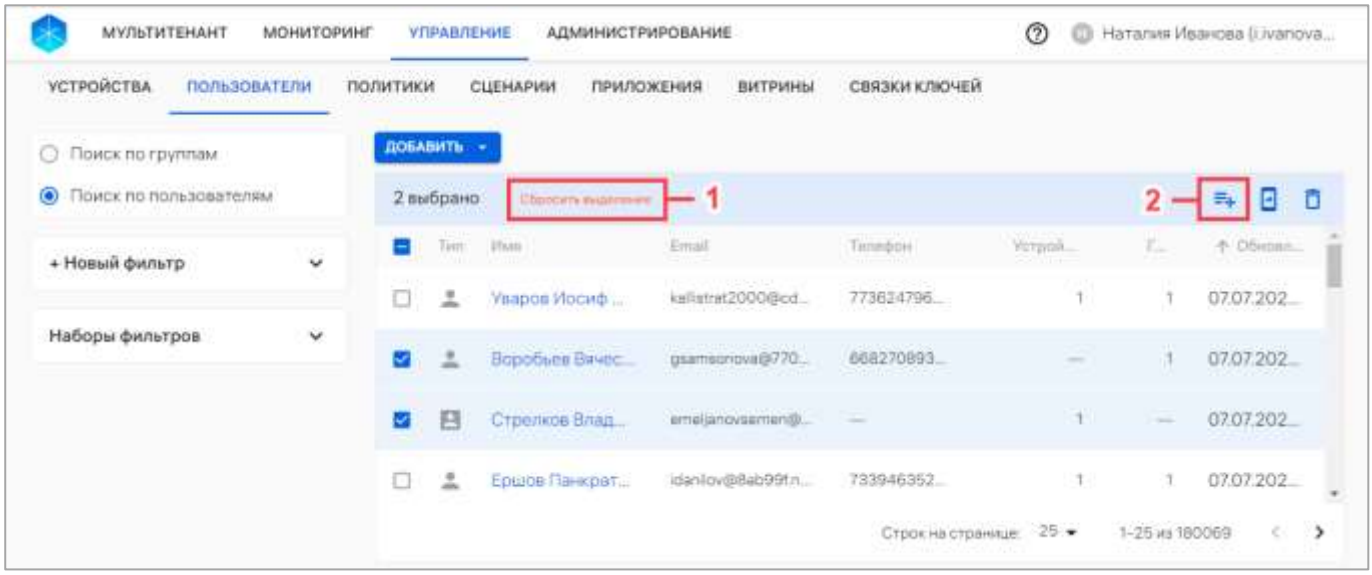

Рисунок 113

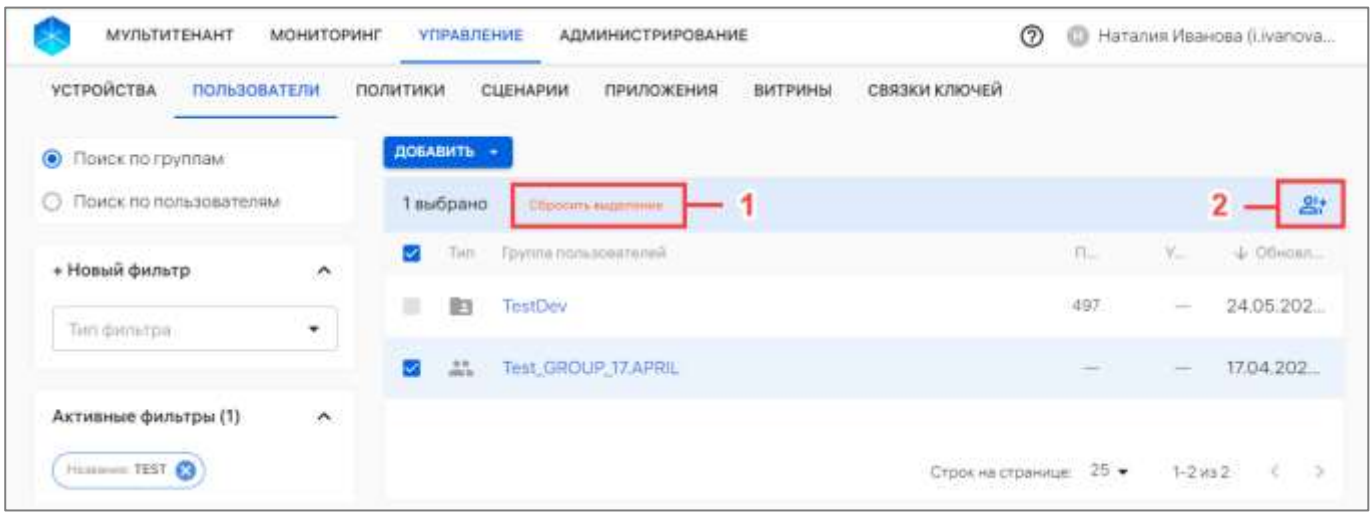

Рисунок 114

– в отобразившемся окне выбрать необходимую группу пользователей (Рисунок 115[1]) или пользователя (Рисунок 116 [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 115 [3], Рисунок 116 [3]);

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

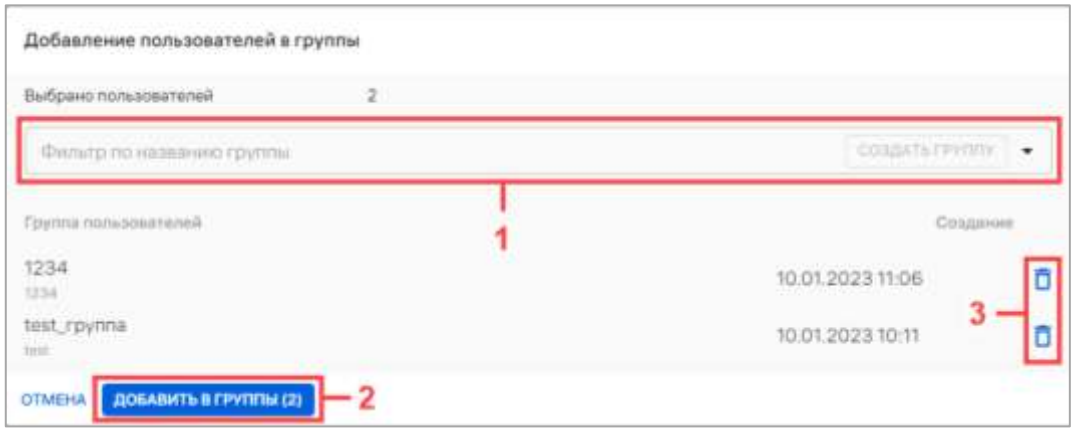

Рисунок 115

Рисунок 116

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» (Рисунок 117 [1]) и нажав кнопку «Создать группу» (Рисунок 117 [2]). В результате отобразится сообщение «Группа успешно создана»;

Рисунок 117

– нажать кнопку «Добавить в группы» (см. Рисунок 115 [2]) или «Добавить пользователей» (см. Рисунок 116 [2]). В результате отобразится сообщение об успешной привязке пользователей к группам.

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»;

– выбрать пользователя из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку пользователя;

– в открывшейся карточке пользователя перейти во вкладку «Группы»;

– нажать кнопку «Добавить в группы» (Рисунок 118);

– в отобразившемся окне (см. Рисунок 115) выполнить действия, описанные в пп. 2.3.4.1.

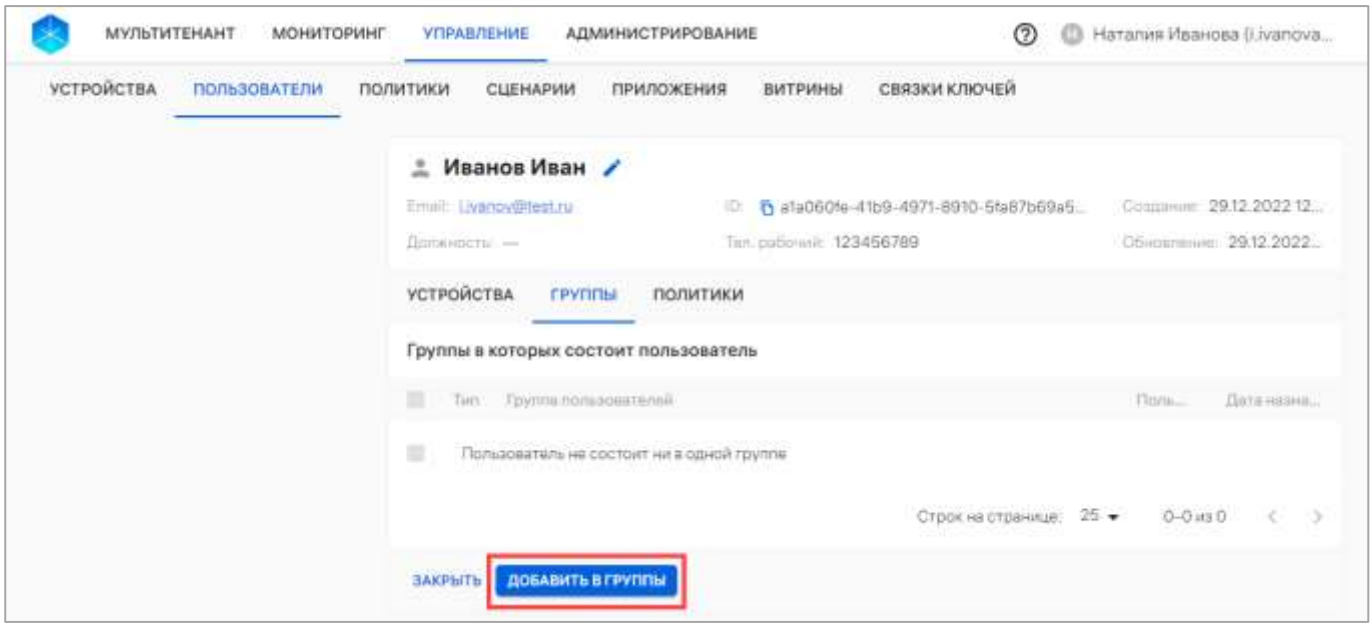

Рисунок 118

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»;

– выбрать группу пользователей из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке группы перейти во вкладку «Пользователи»;

– нажать кнопку «Привязать пользователей» (Рисунок 119);

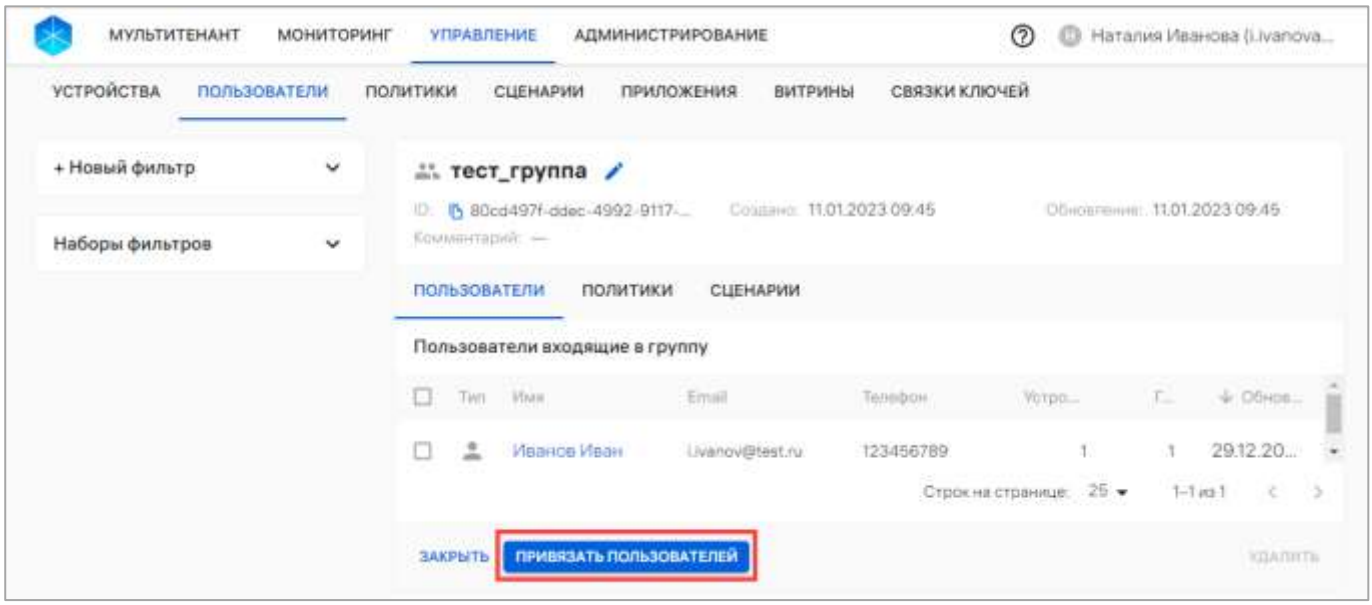

Рисунок 119

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте или номеру телефона (Рисунок 120 [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 120 [3]);

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

Рисунок 120

– далее нажать кнопку «Добавить пользователей» (Рисунок 120 [2]). В результате отобразится сообщение «К группе успешно привязан [количество пользователей] пользователь».

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 121 [1]);

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям» (Рисунок 121 [2]);

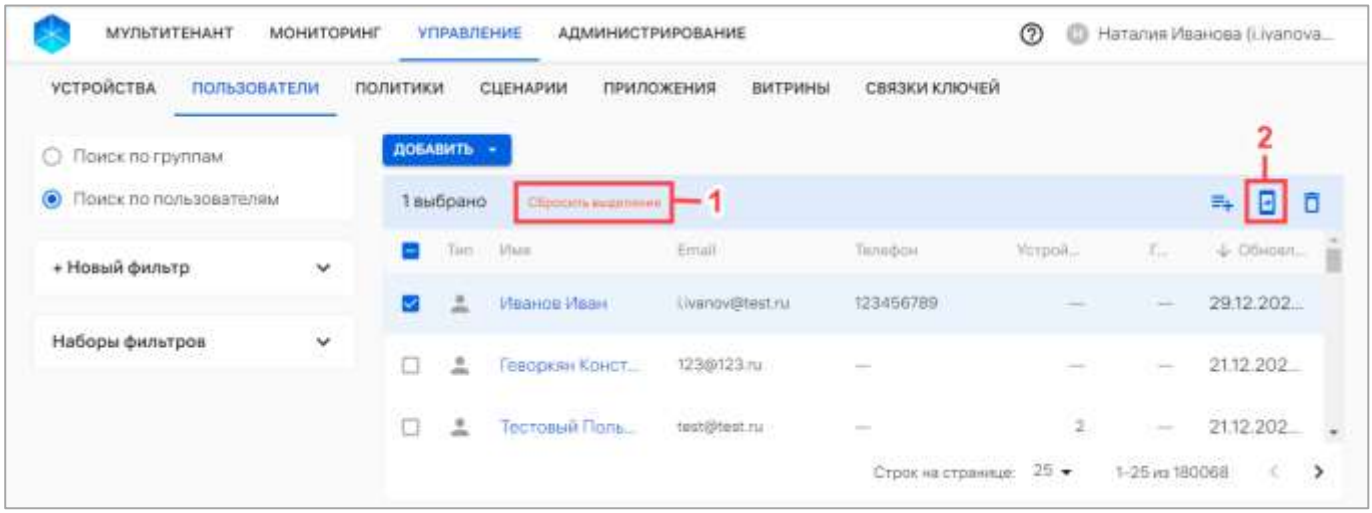

Рисунок 121

– в отобразившемся окне выбрать устройства из раскрывающегося списка или воспользоваться фильтром по IMEI, WLAN MAC или комментарию (Рисунок 122 [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 122 [3]);

Рисунок 122

– нажать кнопку «Привязать устройства» (Рисунок 122 [2]).

В результате успешной привязки устройства отобразится сообщение «[количество устройств] устройство успешно привязано к [количество пользователей] пользователю».

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»;

– выбрать пользователя из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку пользователя;

– в открывшейся карточке пользователя перейти во вкладку «Устройства»;

– нажать кнопку «Привязать устройства» (Рисунок 123);

– в отобразившемся окне (см. Рисунок 122) выполнить действия, описанные в пп. 2.3.5.1.

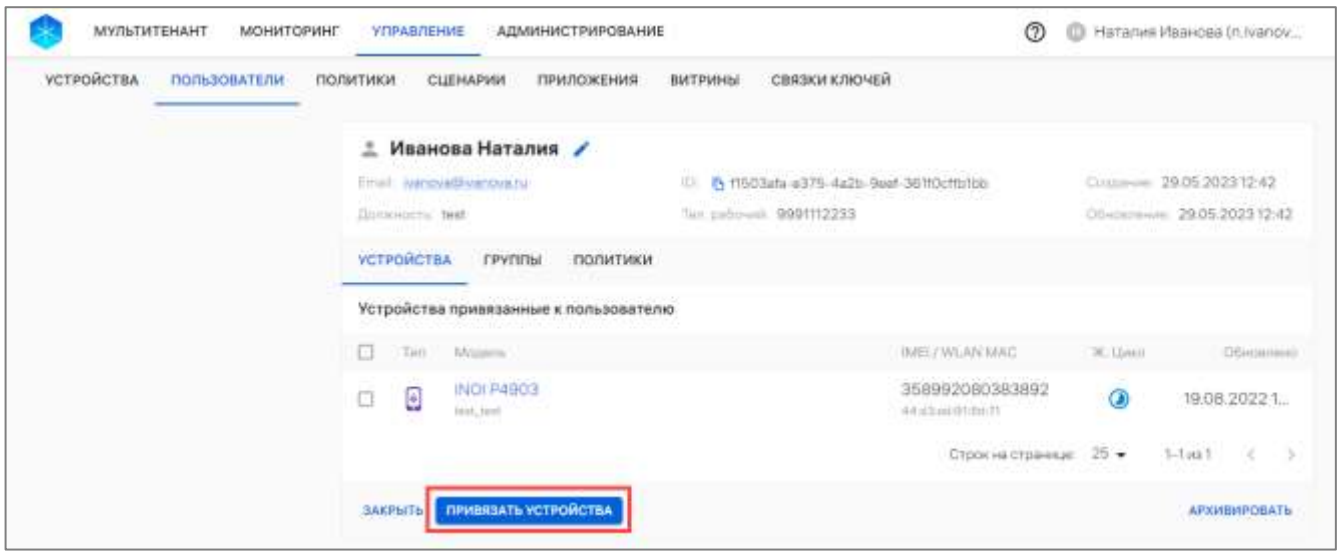

Рисунок 123

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 124);

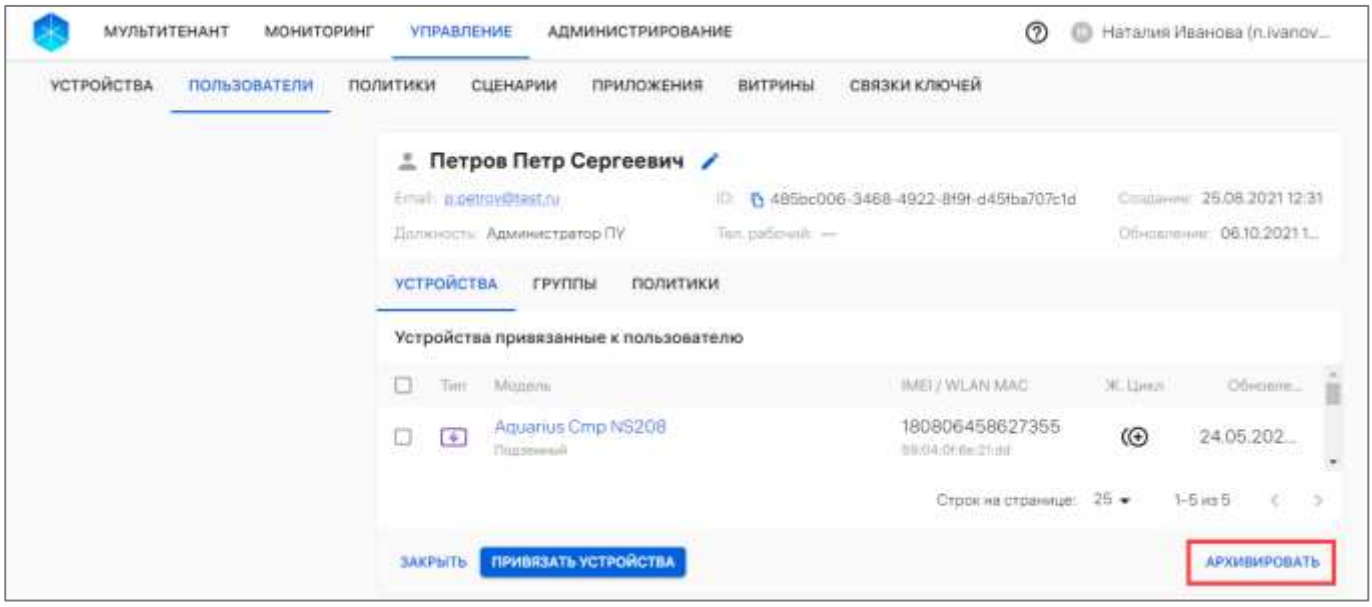

Рисунок 124

– в отобразившемся окне «Архивирование пользователя» подтвердить либо отменить действия (Рисунок 125);

Рисунок 125

2) с помощь списка быстрых действий. Для это необходимо:

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

– 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 126 [1]);

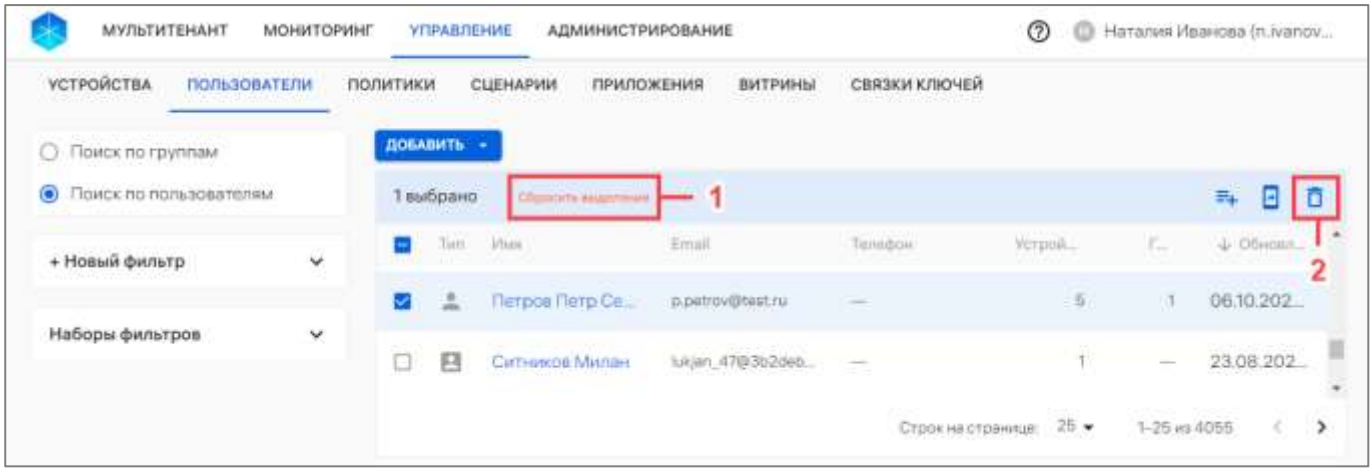

Рисунок 126

– в списке быстрых действий выбрать значок (Рисунок 126 [2]);

– в отобразившемся окне «Архивирование пользователя» подтвердить либо отменить действия (Рисунок 125).

В результате успешного архивирования отобразится сообщение «Пользователь успешно архивирован». 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»;

– выбрать группу пользователей из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке пользователя удалить всех пользователей из группы и нажать кнопку «Удалить» (Рисунок 127);

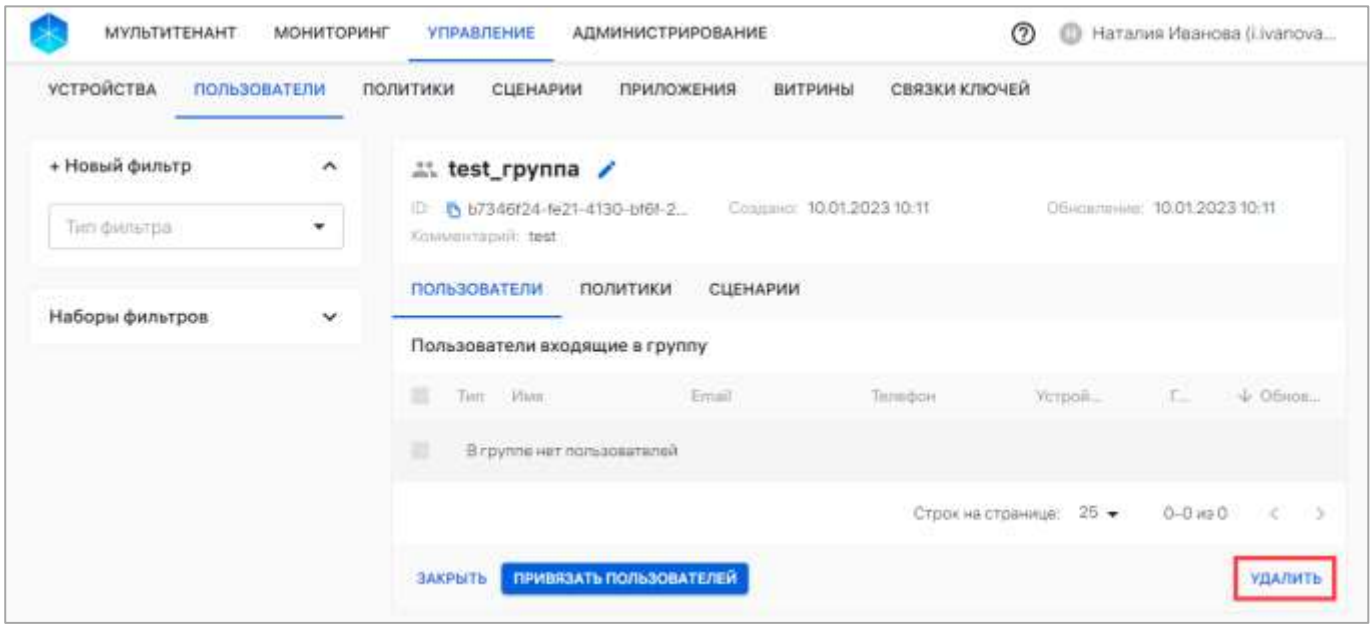

Рисунок 127

– в открывшемся окне (Рисунок 128) подтвердить либо отменить действия.

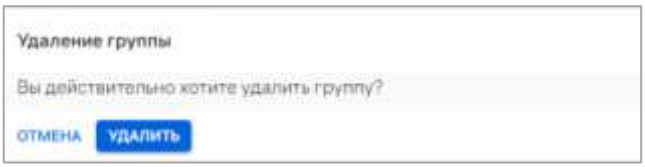

Рисунок 128

В результате успешного удаления отобразится сообщение «Группа удалена».

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.

В рабочей области подраздела «Политики» информация о политике отображается в следующих столбцах, приведенных в таблице (Рисунок 129, Таблица 24).

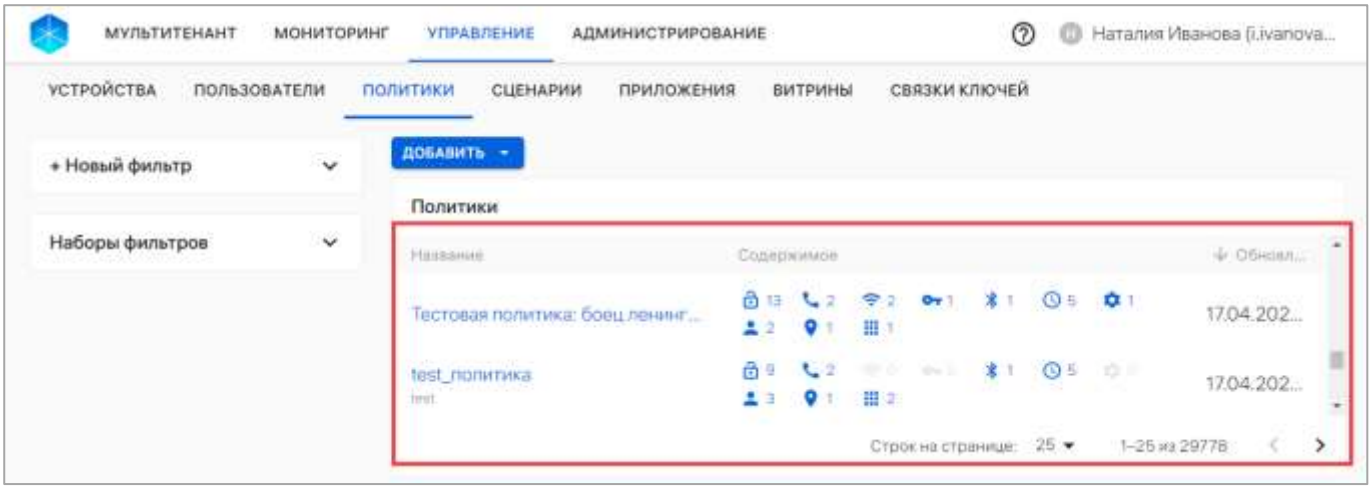

Рисунок 129

Таблица 24

Название столбца	Значение		Описание
Название	Название политики		Представляет собой активную ссылку, при нажатии на которую происходит переход к карточке пользователя
	Комментарий		Дополнительная информация к политике
Содержимое	Категория правил в политике		Ограничение доступа
			Голосовые вызовы
			Конфигурация WLAN

Название столбца	Значение		Описание
			Конфигурация VPN
			Конфигурация Bluetooth®
			Конфигурация
			Система
			Настройки пользователя
			Геопозиционирование
			Установка приложений
	Количество правил		Количество правил в категории
Обновлено	Дата и время последнего обновления офлайн-сценария. Значение столбца отсортировано в направлении стрелки: от старых к новым  , от новых к старым 		

ПРИМЕЧАНИЕ. При отсутствии добавленных политик в подразделе «Политики» отображается сообщение «Нет данных».

Добавление политики возможно одним из следующих способов:

– вручную (п. 2.4.1);

– на основе корпоративного шаблона (п. 2.4.2);

– на основе существующей политики (п. 2.4.3).

Существует возможность добавления в политику правил как вовремя, так и после ее создания. Правила политики имеют различное содержание, приведенное в таблице (Таблица 25).

Таблица 25

Правило/Категория правила	Описание	Доступные значения
Ограничение доступа/Блокировка экрана	Правило позволяет разблокировать или заблокировать экран устройства с выводом сообщения	Выбор значения из списка: – «Заблокирован» - данное значение выбрано по умолчанию при добавлении правила, а также доступно поле для ввода сообщения, которое будет отображаться на заблокированном экране. Экстренные вызовы остаются доступны; – «Разблокирован»
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)
Ограничение доступа/Снимки экрана	Правило разрешает или запрещает создание скриншотов с экрана устройства	
Ограничение доступа/Управление авиарежимом	Правило разрешает или запрещает использование авиарежима на устройствах	
Ограничение доступа/Управление точкой доступа WLAN	Правило фиксирует текущее состояние точки доступа WLAN. Разрешает или запрещает вносить изменения в настройки точки доступа WLAN	

Правило/Категория правила	Описание	Доступные значения
Ограничение доступа/Управление Bluetooth	Правило фиксирует текущее состояние Bluetooth®. Запрещает или разрешает вносить изменения в настройки Bluetooth®	
Ограничение доступа/Использование браузера	Правило разрешает или запрещает использование браузера на устройствах	
Ограничение доступа/Управление датой и временем	Правило фиксирует текущие дату и время на устройствах. Разрешает или запрещает вносить изменения в дату и время. ПРИМЕЧАНИЕ. Для устройств на базе ОС Аврора изменение времени в меньшую сторону от реального может привести к тому, что записи о произошедших операциях перестанут отображаться в журнале клиентского приложения «Аврора Центр». Поэтому рекомендуется назначить политику с правилом по запрету управления датой и времени	

Правило/Категория правила	Описание	Доступные значения
Ограничение доступа/Передача данных MTP	Правило разрешает или запрещает передачу данных через USB-соединение	
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 клиентских 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
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)
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: 1) 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;

Правило/Категория правила	Описание	Доступные значения
		2) 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; 3) При применении запрещающего правила на устройстве INOI P4903 сообщение о блокировке в пункте меню «Хранилище» в подразделе «Настройки» отображается не полностью
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: 1) 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. 2) 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».

Правило/Категория правила	Описание	Доступные значения
		3) Если после применения запрещающего правила SD-карта осталась доступна, необходимо перезагрузить устройство
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)
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
Конфигурация WLAN/Режим работы WLAN	Правило позволяет: – отключать или включать адаптер WLAN; – зафиксировать текущее состояние адаптера WLAN	1) Для работы WLAN выбор значения из списка: – «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)

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. **ВНИМАНИЕ!** Правило не сработает, если на устройствах выключен адаптер WLAN	Для создания правила: 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; 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: 1) 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: 1. Если пароль не задан, то на устройствах с ОС Аврора необходимо будет вручную ввести пароль для подключения к защищенной беспроводной сети; 2. Пароль хранится в системе в нешифрованном виде. Просмотр пароля возможен: – в карточке политики во вкладке «Правила» (пп. 2.1.5.2); – в карточке устройства во вкладке «Политики» (пп. 2.1.1.6). 2) WPA-EAP (в дополнение к созданию подключения будет выпущен и доставлен на устройства пользовательский сертификат для подключения к беспроводной сети):

		– в раскрывающемся списке «Безопасность» необходимо выбрать «WPA-EAP»; – в раскрывающемся списке «Категория сертификата» необходимо 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» необходимо выбрать динамическую перемененную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение: • `{{UserEmail}}` – email из карточки пользователя. • `{{UserPrincipalName}}` – логин пользователя (значение параметра «userPrincipalName» изLDAP-данных о пользователе). ВНИМАНИЕ! 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

Правило/Категория правила	Описание	Доступные значения
Конфигурация Bluetooth/Режим работы Bluetooth	Правило разрешает или запрещает возможность использовать Bluetooth®. **ПРИМЕЧАНИЕ.** Правило действует для устройств на базе ОС Аврора версии 4.0.1 и выше	Выбор значения из списка: – «Выключен»; – «Включен» (при добавлении правила значение выбрано по умолчанию)
Конфигурация/Расписание получения команд	Правило задает расписание на получение оперативных команд и политик	Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.»
Конфигурация/Расписание отправки состояния	Правило задает расписание отправки состояния устройства на ПУ	
Конфигурация/Расписание отправки событий безопасности	Правило задает расписание отправки в ПУ сообщений о событиях безопасности (`security.d journaling daemon`), произошедших на устройстве	
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

Правило/Категория правила	Описание	Доступные значения
		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
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
Система/Установить версию ОС	Правило предназначено для обновления ОС на устройствах и задает: – версию ОС, которая будет установлена на устройствах;	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 АДМГ.20134-01 91 01.

Правило/Категория правила	Описание	Доступные значения
	– 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	Выбор времени старта и завершения обновления в формате: «Установка с [часы]: [минуты] до [часы]: [минуты]»
Настройки пользователя/Требования к паролю	Правило задает следующие параметры: – сложность пароля для разблокировки устройства; – срок действия пароля	Выбор 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.

Правило/Категория правила	Описание	Доступные значения
		ПРИМЕЧАНИЯ: 1. Правило для пароля действует для учетной записи как пользователя, так и администратора устройства; 2. За 6 дней до окончания срока действия пароля приходит уведомление о необходимости сменить пароль
Настройки пользователя/Создать пользователя	Правило разрешает или запрещает создание пользователя при активации устройства	Выбор значения из списка: – «Создавать» (при добавлении правила значение выбрано по умолчанию); – «Не создавать»
Настройки пользователя/Сертификаты пользователя	Правило позволяет создать и передать на устройство сертификаты пользователя, необходимые для подключения к защищенным сетям WLAN. ПРИМЕЧАНИЕ. Для выпуска и доставки на устройства сертификата пользователя необходимо назначить политику с правилом «Настройки пользователя/Создать пользователя на группу устройств» или пользователей, в которую входит устройство. ВНИМАНИЕ!	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)

Правило/Категория правила	Описание	Доступные значения
	– 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	

Правило/Категория правила	Описание	Доступные значения
Геопозиционирование/ Настройки режим 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»:

Правило/Категория правила	Описание	Доступные значения
		• 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

Приложения/Установка приложений на устройство	Правило предназначено для установки клиентского приложения выбранной витрины и версии на устройствах. ПРИМЕЧАНИЕ. Предусмотрена возможность задать дополнительные правила по добавлению нескольких клиентских приложений в политику, выполнив действия, описанные в п. 2.4.4 Чтобы клиентское приложение было доступно для выбора, необходимо выполнение следующих условий: – клиентское приложение должно быть добавлено и опубликовано в ПМ (подробная информация приведена в документе АДМГ.20134-01 90 01-2); – Видимость витрины с приложением включена в настройках интеграции с Сервером приложений Аврора (п. 4.1.4);	Для создания правила необходимо выбрать из раскрывающихся списков: – витрину, в которой размещено клиентское приложение; – приложение, которое необходимо установить на устройства; – номер версии клиентского приложения; – автозапуск (действует только для устройств на базе ОС Аврора). При настройке автозапуска доступны следующие значения: • 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

Правило/Категория правила	Описание	Доступные значения
	– Приложения должны находиться в отдельных витринах (описание процедуры создания витрины с клиентским приложением для ОС Аврора приведено в документе АДМГ.20134-01 90 01-2). После установки с помощью политики приложению будут автоматически выданы все необходимые разрешения, которые пользователь не сможет отозвать. Клиентское приложение будет удалено с устройства, если после установки оно удаляется из правила, заменяется другим клиентским приложением или удаляется из группы, на которую назначена политика	

2.4.1. 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 130);

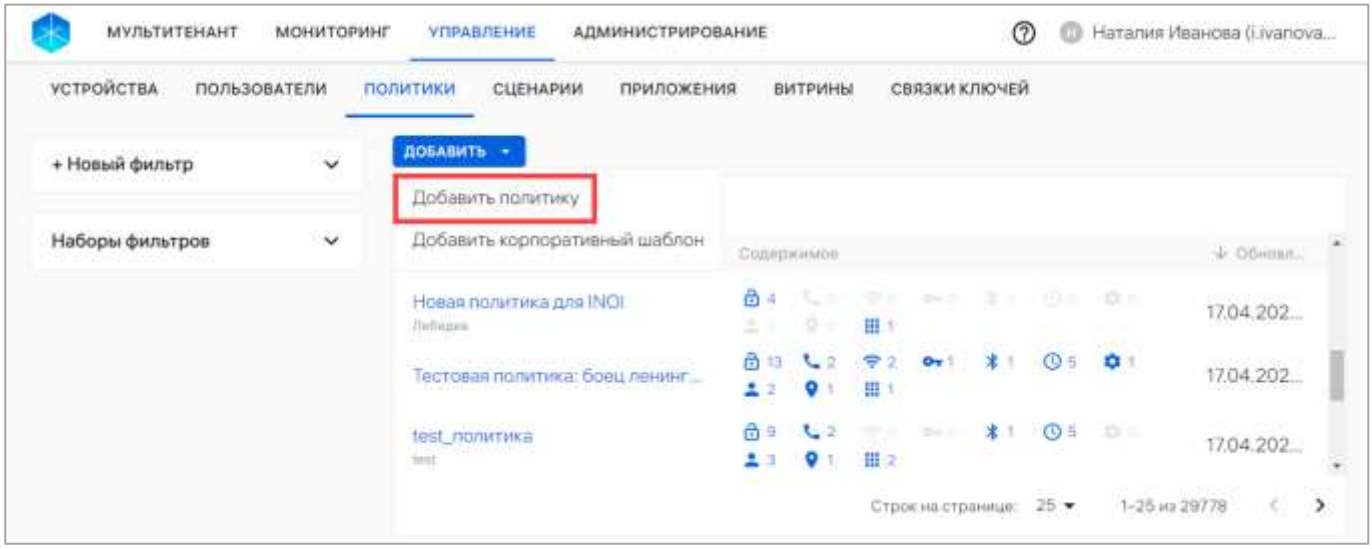

Рисунок 130

– в открывшемся окне «Новая политика» (Рисунок 131 [1]):

- ввести название политики (название политики должно быть уникальным. Поле обязательно для заполнения);
- ввести комментарий (при необходимости ввести дополнительную информацию к политике);
- нажать кнопку «Добавить правило» (Рисунок 131 [2]) и выбрать правило политики из раскрывающегося списка;

Рисунок 131

- задать параметры правила (Рисунок 132 [1]). Описание правил для политик приведено в таблице (см. Таблица 25).

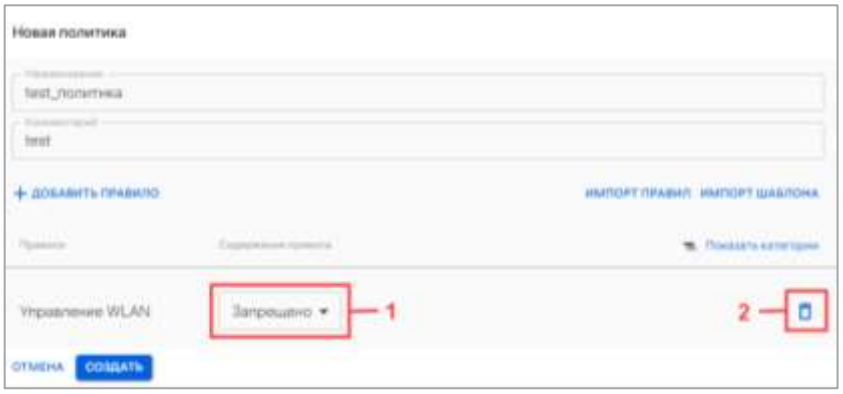

Рисунок 132

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

В случае необходимости удалить правило следует нажать значок «Удалить» (Рисунок 132 [2]), справа от правила.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного сохранения политики отобразится сообщение «Политика успешно создана» и откроется карточка добавленной политики (п. 2.4.4).

2.4.2. 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. 2.4.2.1).

Для добавления политики на основе корпоративного шаблона необходимо в окне «Новая политика» 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 133), в результате чего правила из корпоративного шаблона будут импортированы в новую политику.

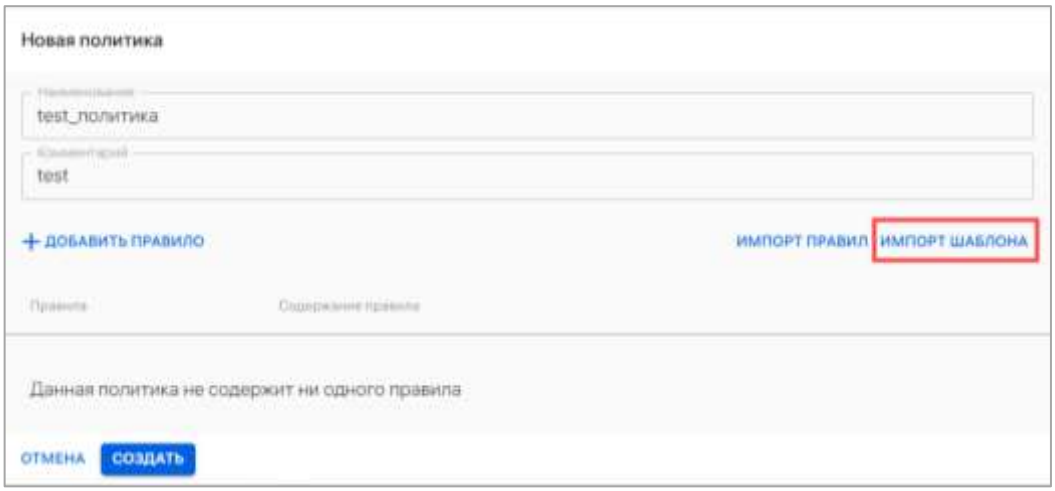

Рисунок 133

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

– изменить (см. Рисунок 132 [1]). Описание правил для политик приведено в таблице (см. Таблица 25);

– добавить правило в политику (см. Рисунок 131 [2]);

– удалить правило (см. Рисунок 132 [2]).

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного добавления политики отобразится сообщение «Политика успешно создана» и откроется карточка добавленной политики.

2.4.2.1. 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 134);

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 136).

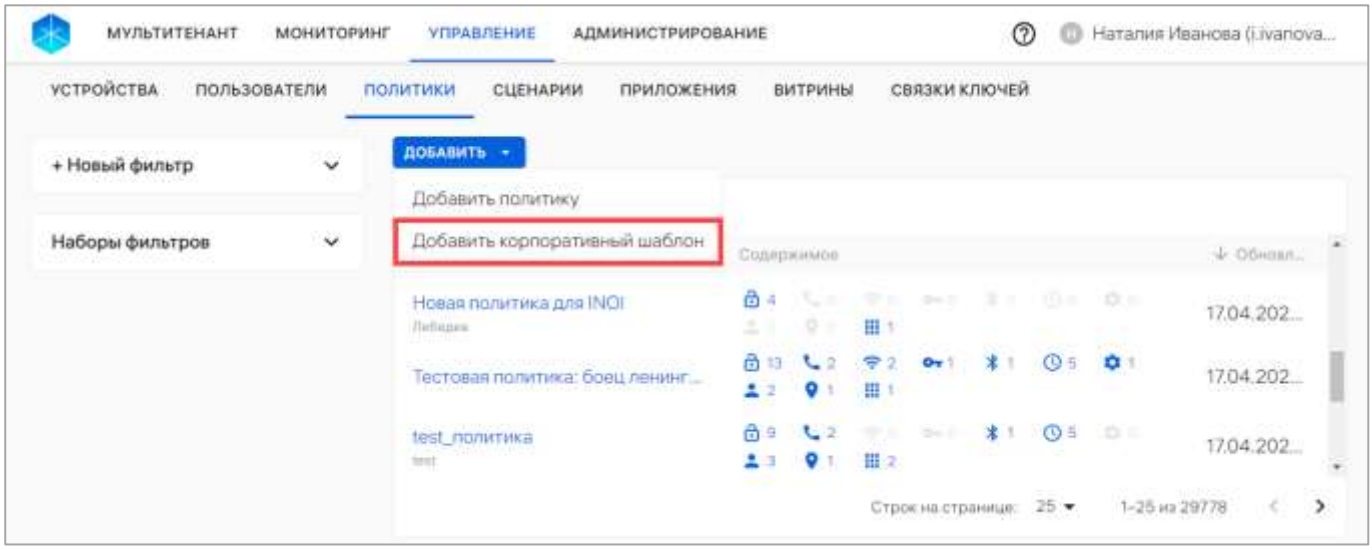

Рисунок 134

– в открывшемся окне «Корпоративный шаблон политики» возможно выполнить следующие действия:

- при необходимости изменить комментарий к корпоративному шаблону (наименование корпоративного шаблона проставляется автоматически) (Рисунок 135 [1]);
- добавить правила в корпоративный шаблон, нажав на кнопку «Добавить правило» (Рисунок 135 [2]). Добавление правила выполняется в соответствии с п. 2.4.1;

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

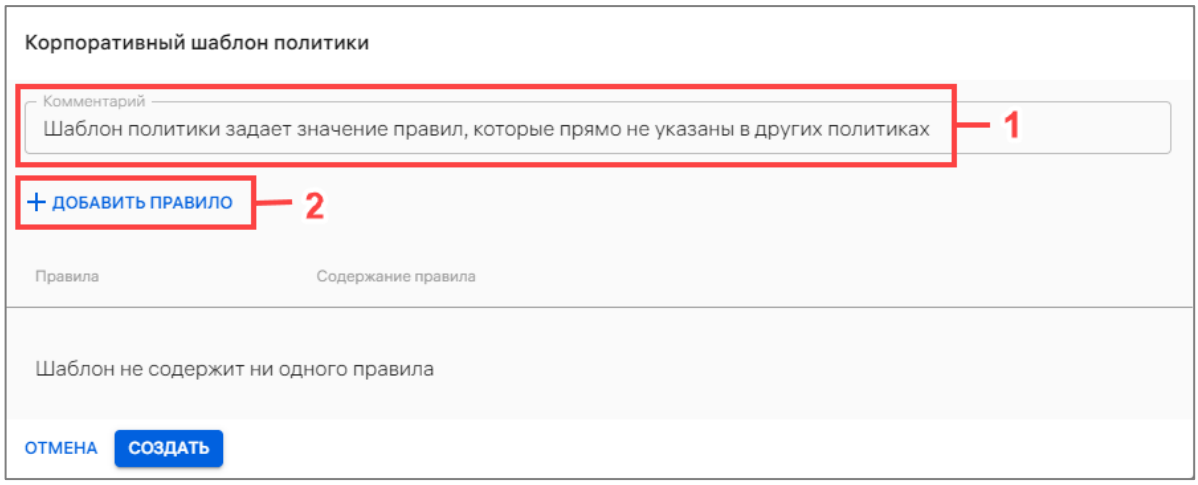

Рисунок 135

– подтвердить либо отменить действия.

В результате успешного создания корпоративного шаблона политики отобразится сообщение «Шаблон политики успешно создан».

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.

2.4.2.2. 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 136);

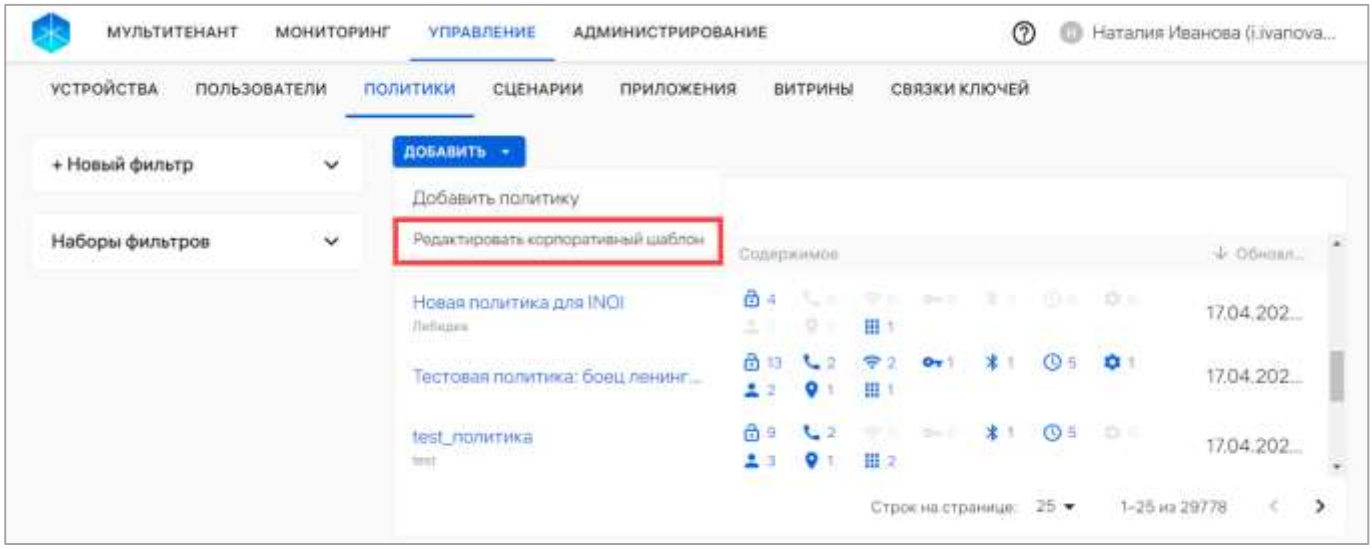

Рисунок 136

– в открывшемся окне «Корпоративный шаблон политики» (см. Рисунок 135) внести изменения, выполнив действия приведенные в пп. 2.4.2.1.

В результате сохранения внесенных в корпоративный шаблон изменений отобразится сообщение «Шаблон политики успешно изменен».

ВНИМАНИЕ! После редактирования корпоративного шаблона для его вступления в силу необходимо отредактировать и применить текущую политику либо отвязать ее и снова применить.

2.4.3. Добавление политики на основе существующей

ПРИМЕЧАНИЕ. Добавление политики на основе существующей возможно только при условии, что добавлена хотя бы 1 политика (п. 2.4.1, п. 2.4.2).

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 137);

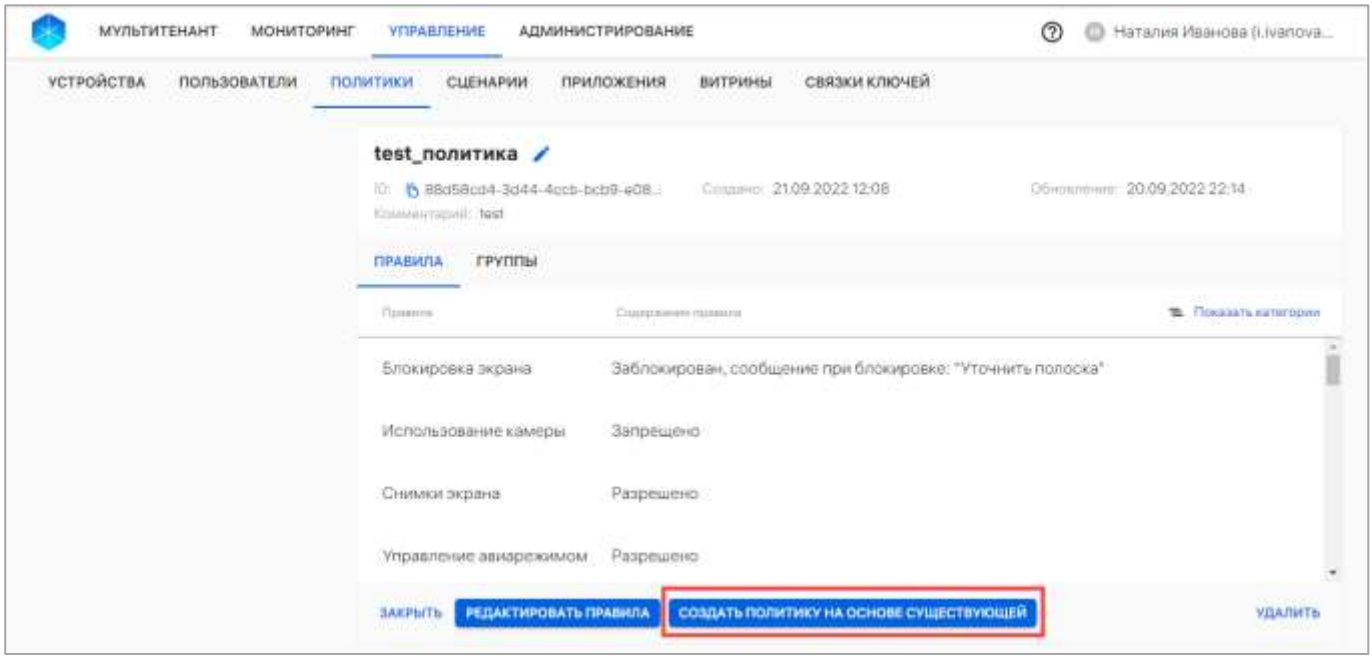

Рисунок 137

- в списке политик нажать кнопку «Добавить» или выбрать из раскрывающегося списка «Добавить политику» (см. Рисунок 130), а затем нажать кнопку «Импорт правил» (Рисунок 138 [1]). Из раскрывающегося списка выбрать правило политики, которое необходимо скопировать (при необходимости воспользоваться фильтром по названию политики) (Рисунок 138 [2]). В результате правила из выбранной политики будут импортированы в новую политику;

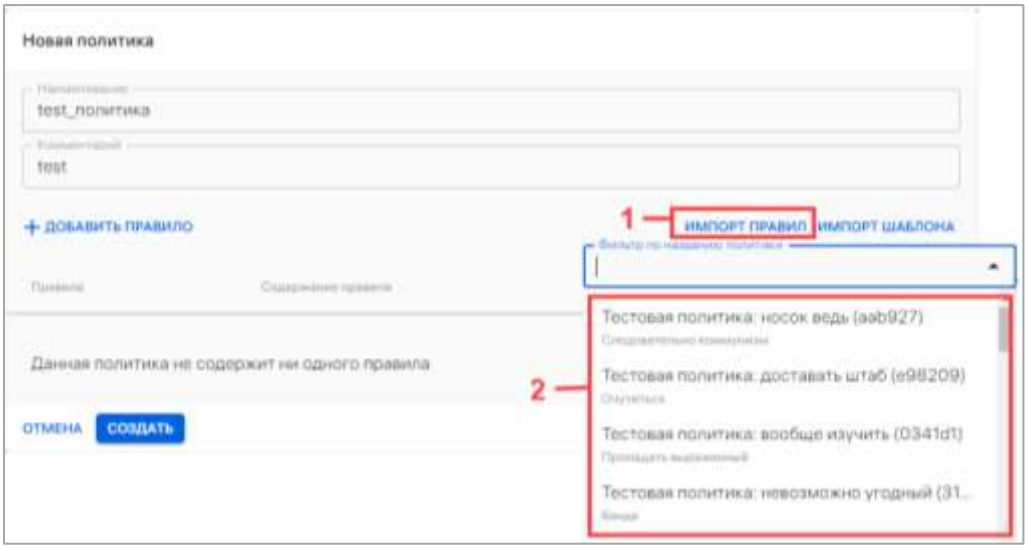

Рисунок 138

– в открывшемся окне «Новая политика»:

- 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 25).

Если необходимо добавить правило в политику или удалить правило следует выполнить действия, описанные в п. 2.4.1.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

2.4.4. 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 139);

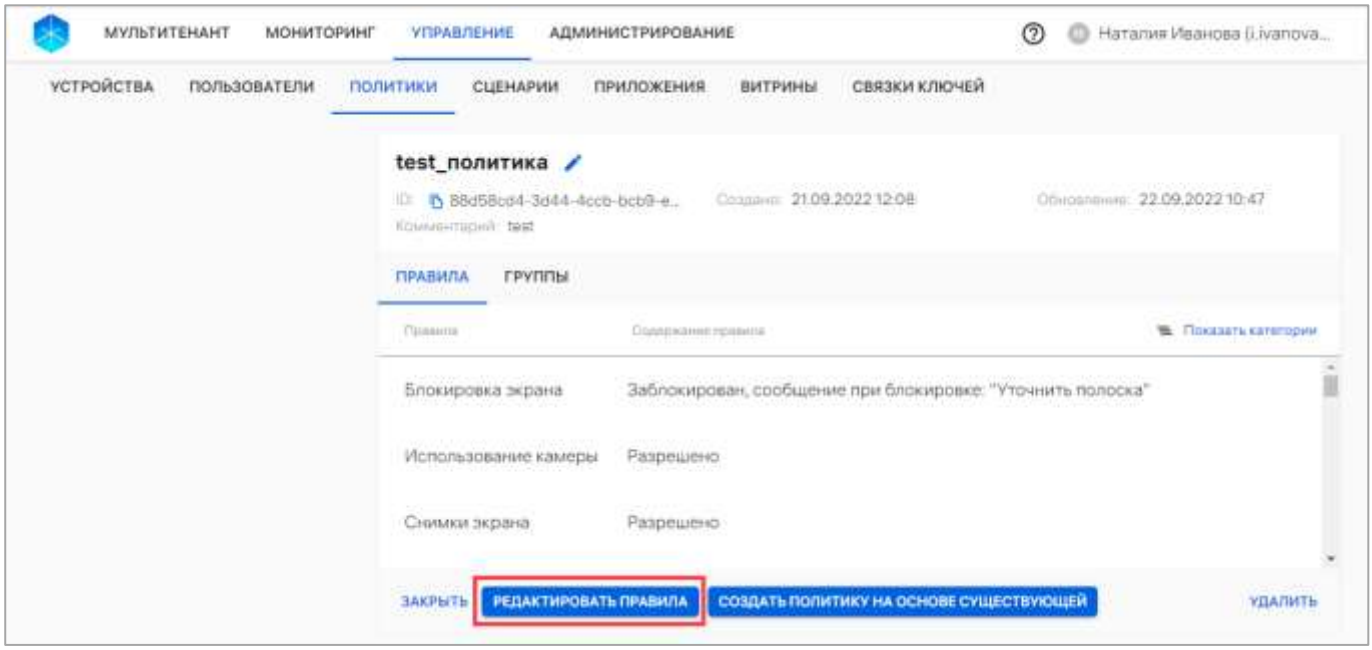

Рисунок 139

– в открывшемся окне «Редактирование правил политики» внести изменения в правилах политики (Рисунок 140 [2]) в соответствии с таблицей (см. Таблица 25);

– для добавления дополнительных правил нажать кнопку «Добавить правило» (Рисунок 140 [1]) и выбрать правило политики из раскрывающегося списка и задать его параметры (при необходимости);

– для удаления правил из политики нажать значок 🗑 «Удалить» (Рисунок 140 [3]) справа от правила (при необходимости);

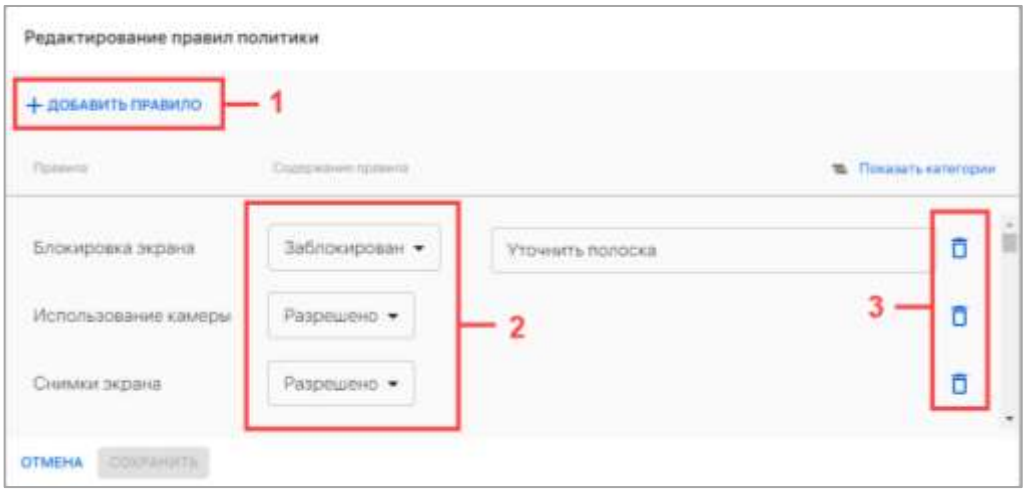

Рисунок 140

– 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 141 [1]).

Для автоматического применения политики следует нажать кнопку «Подтвердить» (Рисунок 141 [2]), не дожидаясь результата проверки, в результате чего политика с обновленными правилами будет назначена на все устройства.

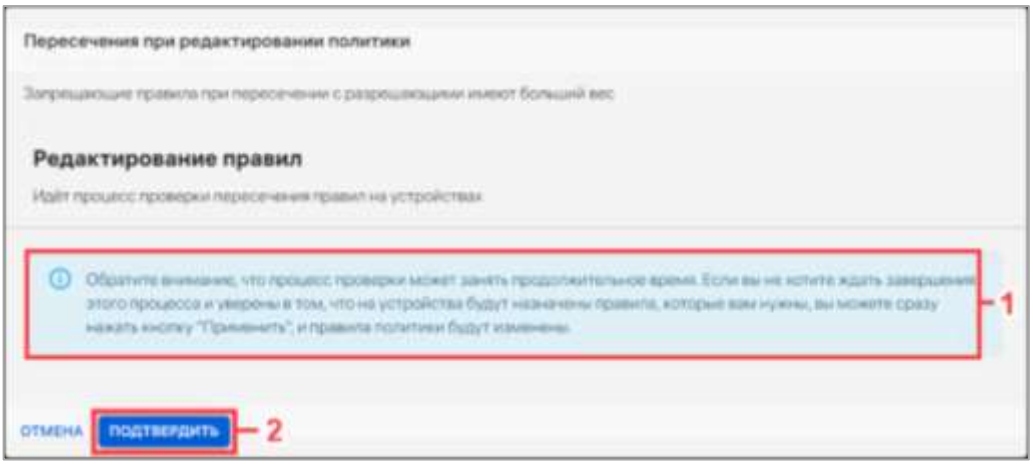

Рисунок 141

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 142), 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.

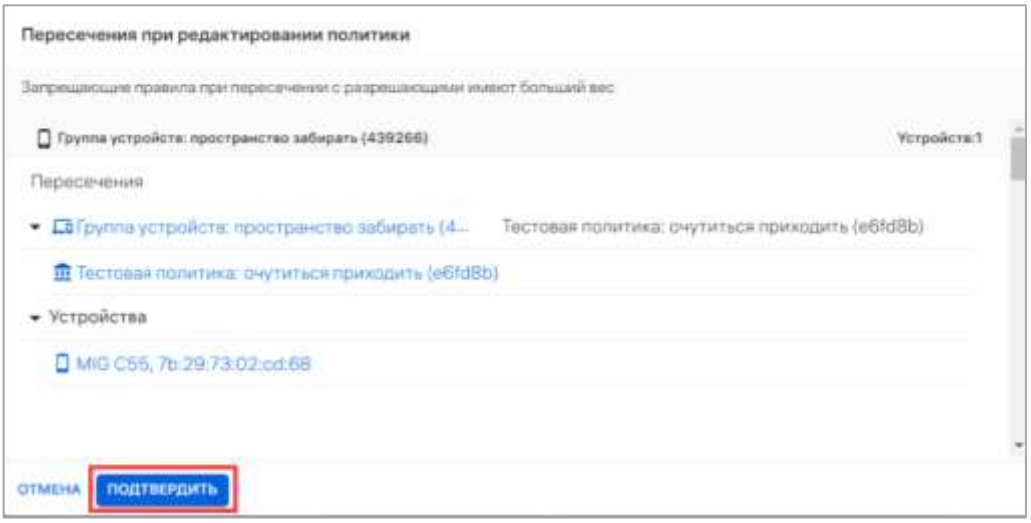

Рисунок 142

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 клиентского 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.

2.4.5. Назначение политики на группы устройств или группы пользователей

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

– карточку политики (пп. 2.4.5.1);

– карточку группы устройства (пп. 2.4.5.2);

– карточку группы пользователей (пп. 2.4.5.3).

2.4.5.1. 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»;

– выбрать политику из списка, при необходимости воспользовавшись фильтром (подраздел 1.5);

– в открывшейся карточке политики перейти во вкладку «Группы»;

– нажать кнопку «Редактировать группы» (Рисунок 143);

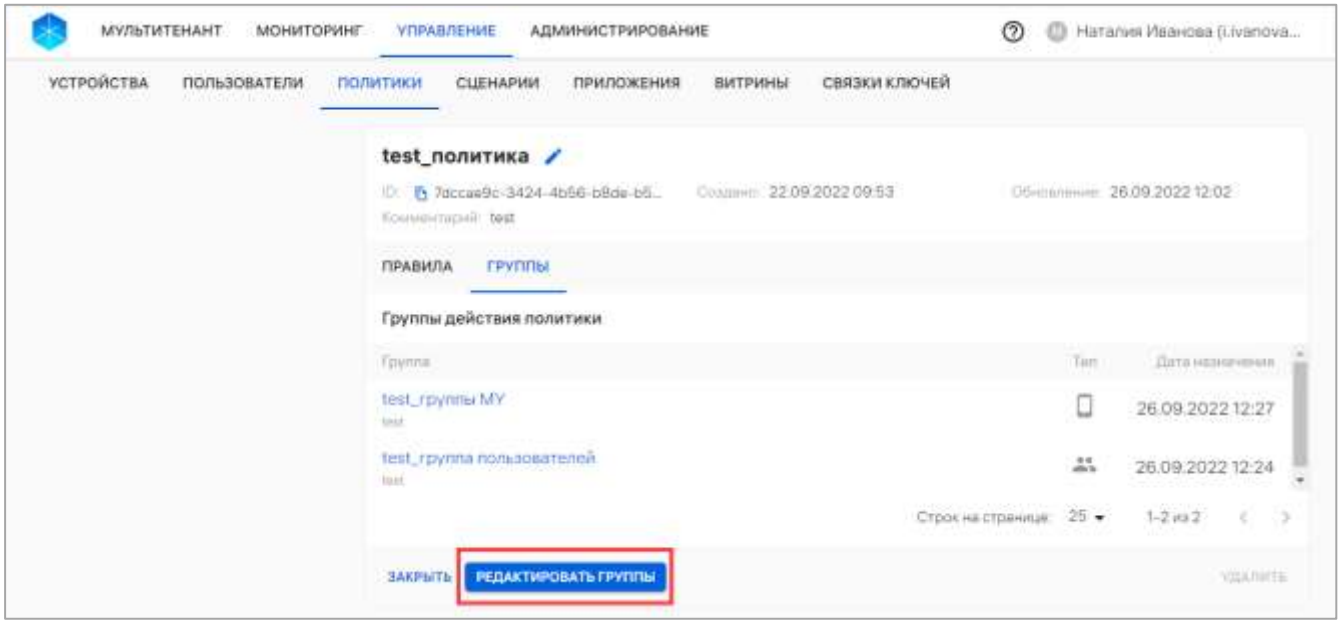

Рисунок 143

– в открывшемся окне «Редактирование групп политики» нажать кнопку «Добавить» (Рисунок 144 [1]);

– в раскрывающемся списке выбрать тип группы (Рисунок 144 [2]):

- «Группу устройств»;
- «Группу пользователей».

Рисунок 144

– 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. 2.4.4.

В результате успешного назначения политики на группы устройств и/или группы пользователей отобразится сообщение «Политика успешно назначена на группу [Название группы]».

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.

2.4.5.2. 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 – 2.4.3.

Для назначения политик на группу устройств необходимо выполнить следующие действия:

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

– в области фильтров выбрать «Поиск по группам»;

– выбрать группу устройств из списка, при необходимости воспользовавшись фильтром (подраздел 1.5) и перейти в карточку группы;

– в открывшейся карточке группы устройств перейти во вкладку «Политики»;

– нажать кнопку «Назначить политики» (Рисунок 145);

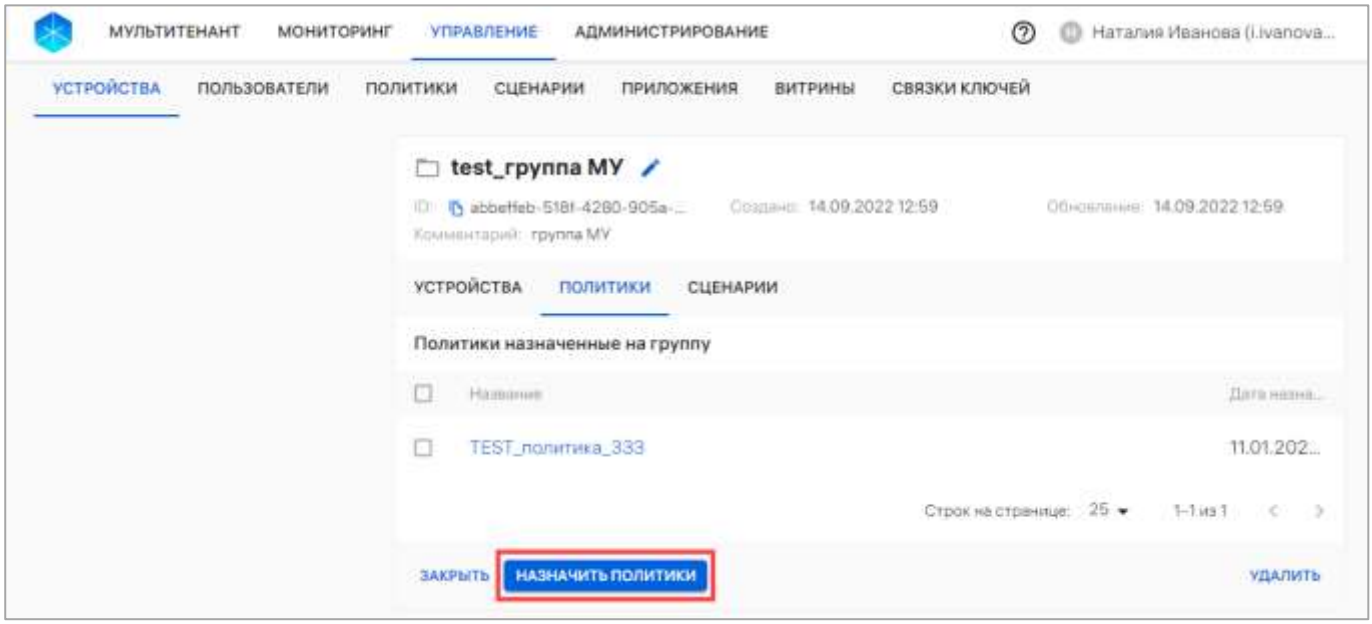

Рисунок 145

– в отобразившемся окне выбрать необходимую политику из раскрывающегося списка или воспользоваться фильтром (Рисунок 146 [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 146 [3]);

Рисунок 146

– нажать кнопку «Назначить политики» (Рисунок 146 [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. 2.4.4.

В результате отобразится сообщение «На группу успешно назначена [количество политик] политика».

ПРИМЕЧАНИЕ. Если устройство, входящее в группу, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.5.3. 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»;

– выбрать группу пользователей из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке группы пользователей перейти во вкладку «Политики»;

– нажать кнопку «Назначить политики» (Рисунок 147);

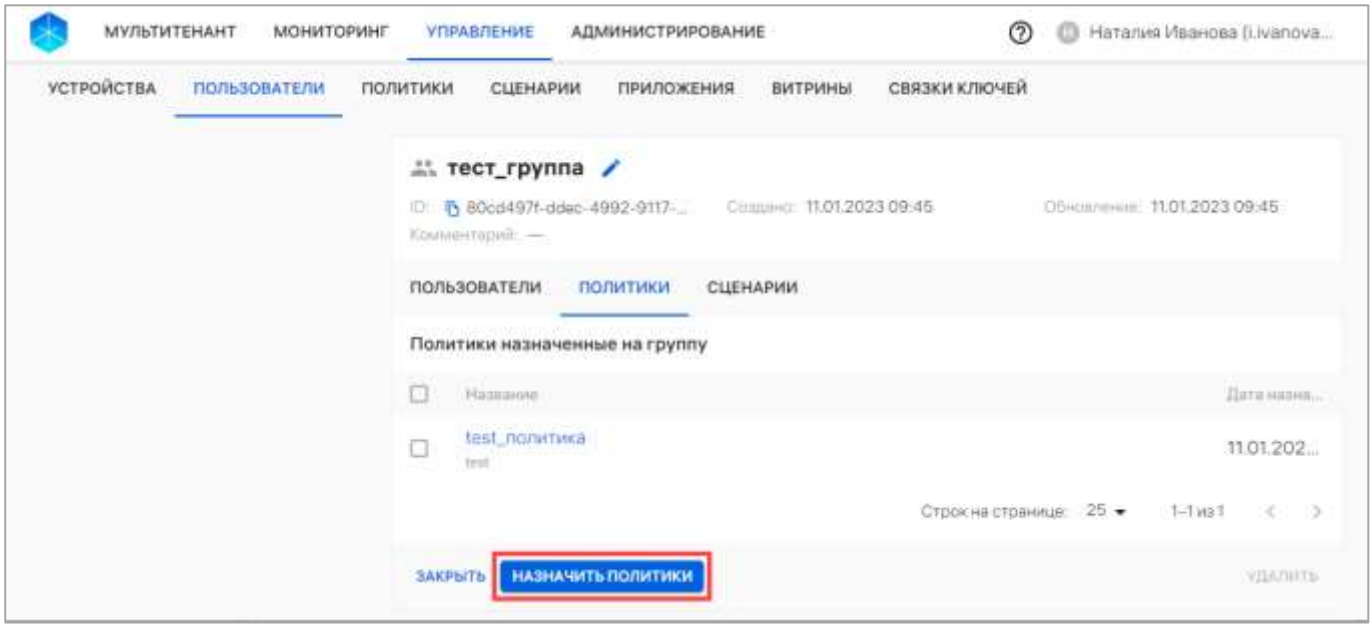

Рисунок 147

– в открывшемся окне (см. Рисунок 146) выполнить действия, приведенные в пп. 2.4.5.2.

В результате успешного назначения политики на группу пользователей отобразится сообщение «На группу успешно назначена [количество политик] политика».

ПРИМЕЧАНИЕ. Если устройство, привязанное к пользователю из группы, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.6. Отвязка политики от группы устройств или группы пользователей

Отвязать политики от группы устройств и/или группу пользователей возможно через:

– карточку политики (пп. 2.4.6.1);

– карточку группы устройств (пп. 2.4.6.2);

– карточку группы пользователей (пп. 2.4.6.3).

2.4.6.1. 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»;

– выбрать политику из списка, при необходимости воспользовавшись фильтром (подраздел 1.5);

– в открывшейся карточке политики перейти во вкладку «Группы»;

– нажать кнопку «Редактировать группы» (см. Рисунок 143);

– в открывшемся окне «Редактирование групп политики» нажать значок «Отвязать политику от группы» (Рисунок 148).

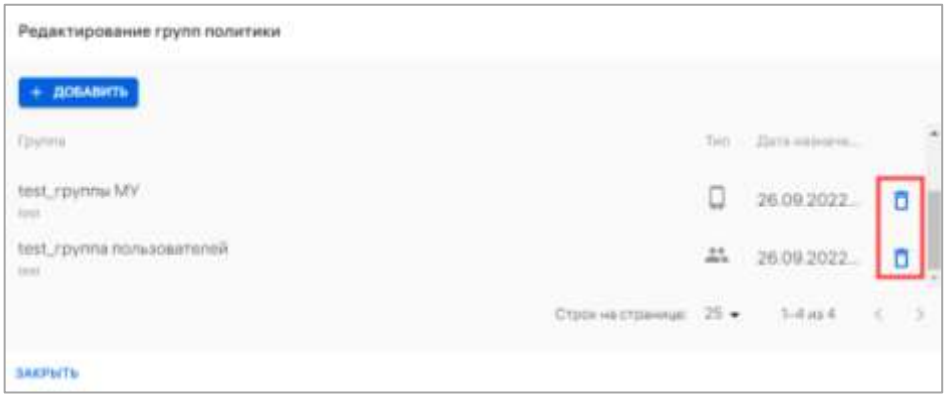

Рисунок 148

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. 2.4.4.

В результате успешной отвязки политика будет отвязана от группы устройств или групп пользователей.

2.4.6.2. Отвязка политики от группы устройств через карточку группы

Для отвязки политики от группы устройств необходимо выполнить следующие действия:

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

– в области фильтров выбрать «Поиск по группам»;

– выбрать группу устройств из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– 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 149 [1]);

– в списке быстрых действий выбрать значок 🗑 «Отвязать политики от группы» (Рисунок 149 [2]).

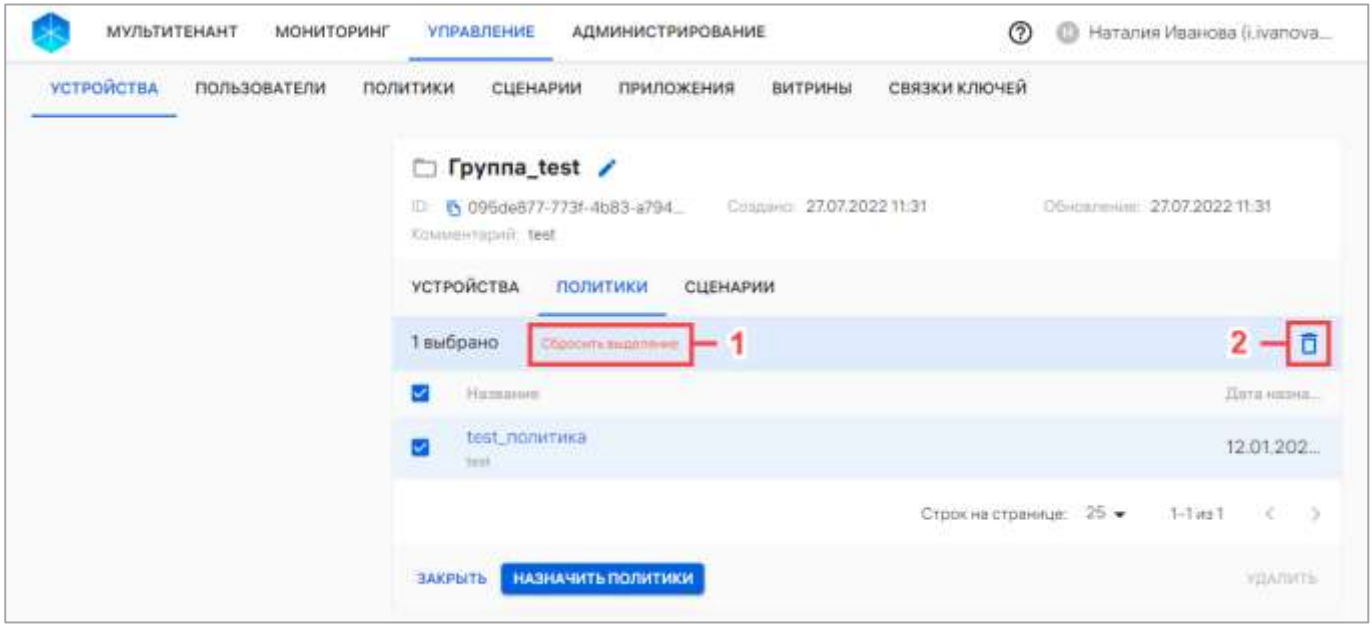

Рисунок 149

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. 2.4.4.

В результате отобразится сообщение «[Количество политик] политика успешно отвязана от группы».

2.4.6.3. 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»;

– выбрать группу пользователей из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– 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 150 [1]);

– в списке быстрых действий выбрать значок «Отвязать политики от группы» (Рисунок 150 [2]).

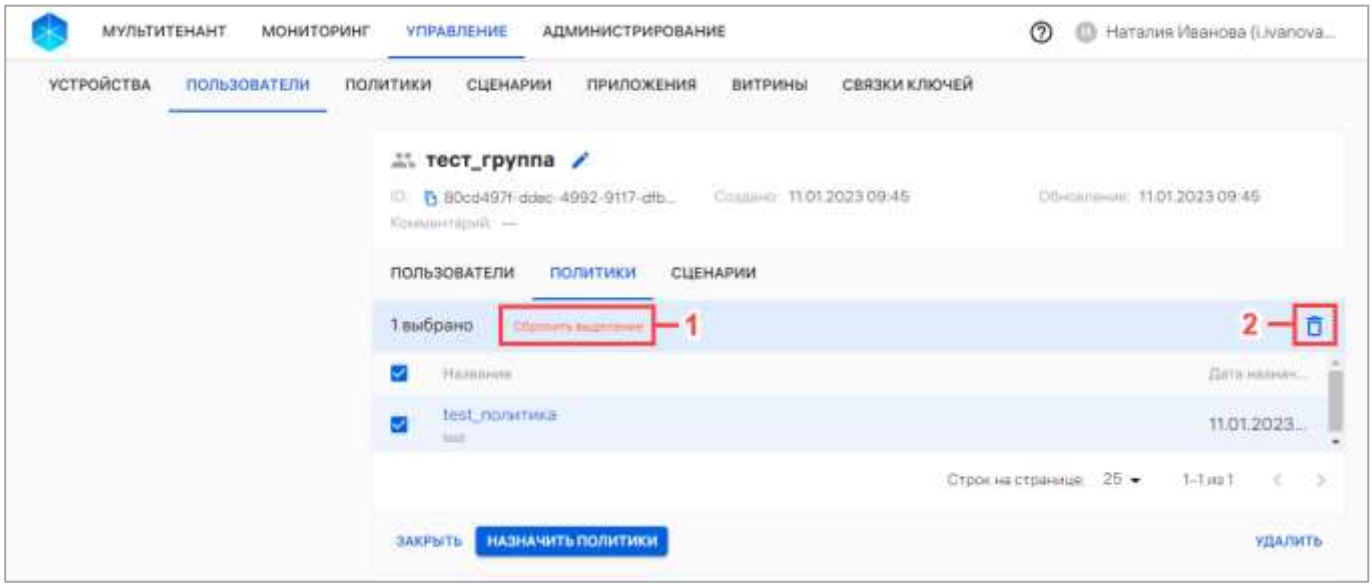

Рисунок 150

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. 2.4.4.

В результате отобразится сообщение «[Количество политик] политика успешно отвязана от группы».

2.4.7. Удаление политики

ПРИМЕЧАНИЕ. Перед удалением политики необходимо предварительно отвязать ее от всех групп устройств или групп пользователей в соответствии с п. 2.4.6.

Для удаления политики из ПУ необходимо выполнить следующие действия:

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

– выбрать необходимую политику из списка, при необходимости воспользовавшись фильтром (подраздел 1.5);

– в карточке политики нажать кнопку «Удалить» (Рисунок 151);

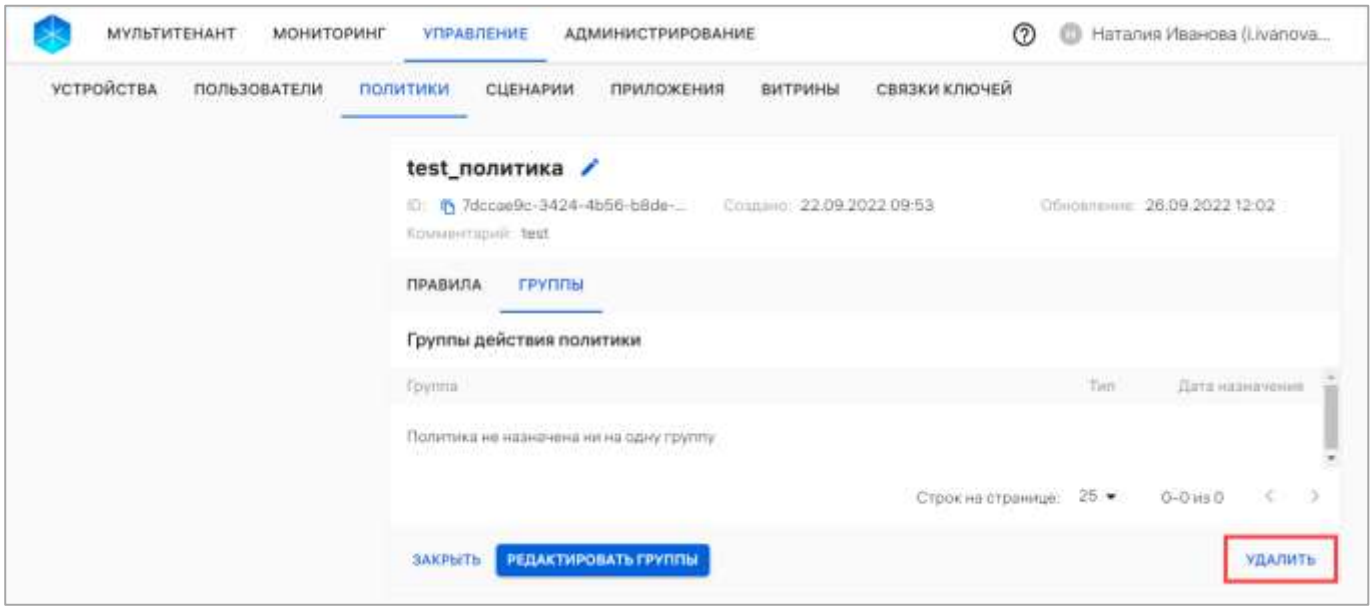

Рисунок 151

– в отобразившемся окне «Удаление политики» подтвердить либо отменить действия (Рисунок 152).

Рисунок 152

В результате успешного удаления отобразится сообщение «Политика успешно удалена».

2.5. Подраздел «Сценарии»

Подраздел «Сценарии» Консоли администратора ПУ предназначен для создания офлайн-сценариев и применения их на устройствах.

ПРИМЕЧАНИЕ. На устройствах, функционирующих под управлением ОС Аврора, возможно применение всех офлайн-сценариев.

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.

ПРИМЕЧАНЕ. На группу устройств или группу пользователей может быть одновременно назначено несколько офлайн-сценариев.

Подробное описание применения каждого сценария на устройствах приведено в документе АДМГ.20134-01 90 01-6.

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Управление», подраздел «Сценарии». В результате отобразится список сценариев (Рисунок 153 [1]).

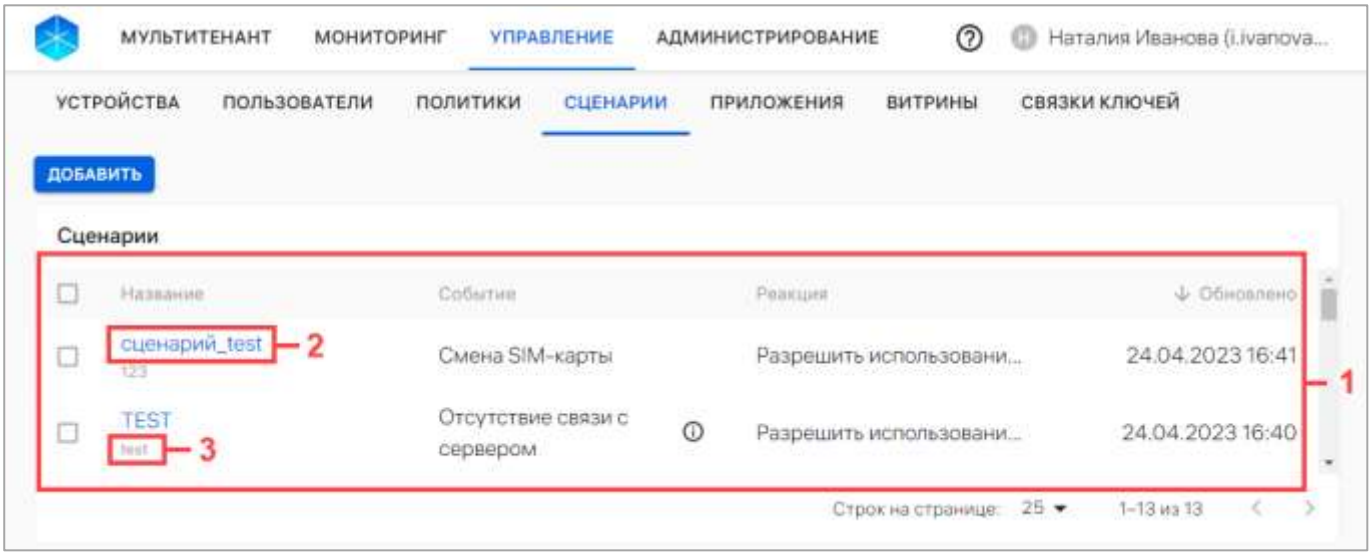

Рисунок 153

В рабочей области подраздела «Сценарии» информация отображается в столбцах, приведенных в таблице (Таблица 26).

Таблица 26

Название столбца	Описание
Название	Название офлайн-сценария. Представляет собой активную ссылку (Рисунок 153 [2]), при нажатии на которую осуществляется переход в карточку офлайн-сценария
	Комментарий – дополнительная информация к офлайн-сценарию (Рисунок 153 [3])
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 27)). 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 27))
Обновлено	Дата и время последнего обновления офлайн-сценария. Значение столбца отсортировано в направлении стрелки: от старых к новым ↑, от новых к старым ↓

При отсутствии добавленных офлайн-сценариев отображается сообщение «Нет данных».

2.5.1. Добавление офлайн-сценария

ПРИМЕЧАНИЕ. Доступно создание 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 «Создание офлайн-сценария» (Рисунок 154) заполнить поля, приведенные в таблице (Таблица 27).

Таблица 27

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** – реакция устройства на смену SIM-карты;

Параметр	Значения
	– Отсутствие связи с сервером – реакция устройства на отсутствие связи с сервером. Дополнительно необходимо указать временной интервал (формат: [ДД] : [ЧЧ] : [ММ]) отсутствия связи с сервером, после наступления которого устройство среагирует; – Вне зоны действия WLAN – реакция устройства на отключение от определенной WLAN. 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 - реакция устройства на подключение к определенной WLAN; 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 - реакция устройства на считывание NFC-меток при входе и выходе с территории объекта. ПРИМЕЧАНИЕ. При выборе события «Нахождение на территории, определяемой NFC-метками» отображаются дополнительные 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
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;

Параметр	Значения
	– **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

– после заполнения полей необходимо подтвердить либо отменить действия (Рисунок 154).

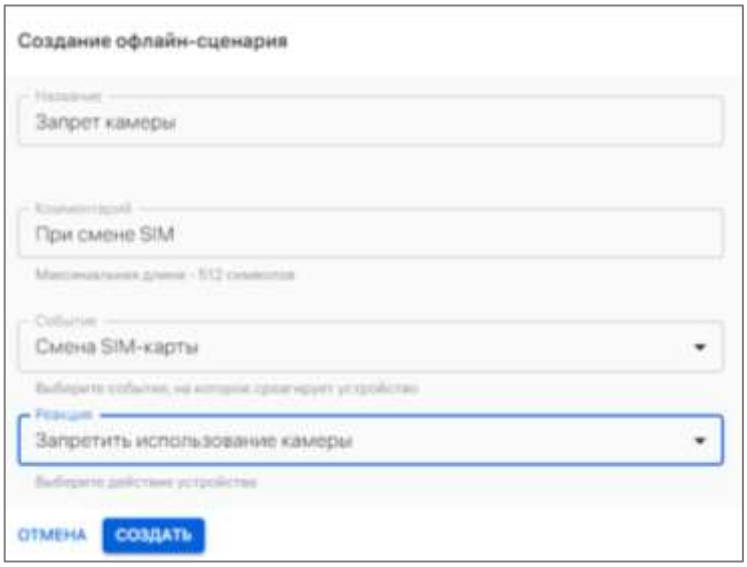

Рисунок 154

При успешном создании офлайн-сценария отобразится сообщение «Офлайн-сценарий создан».

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 155);

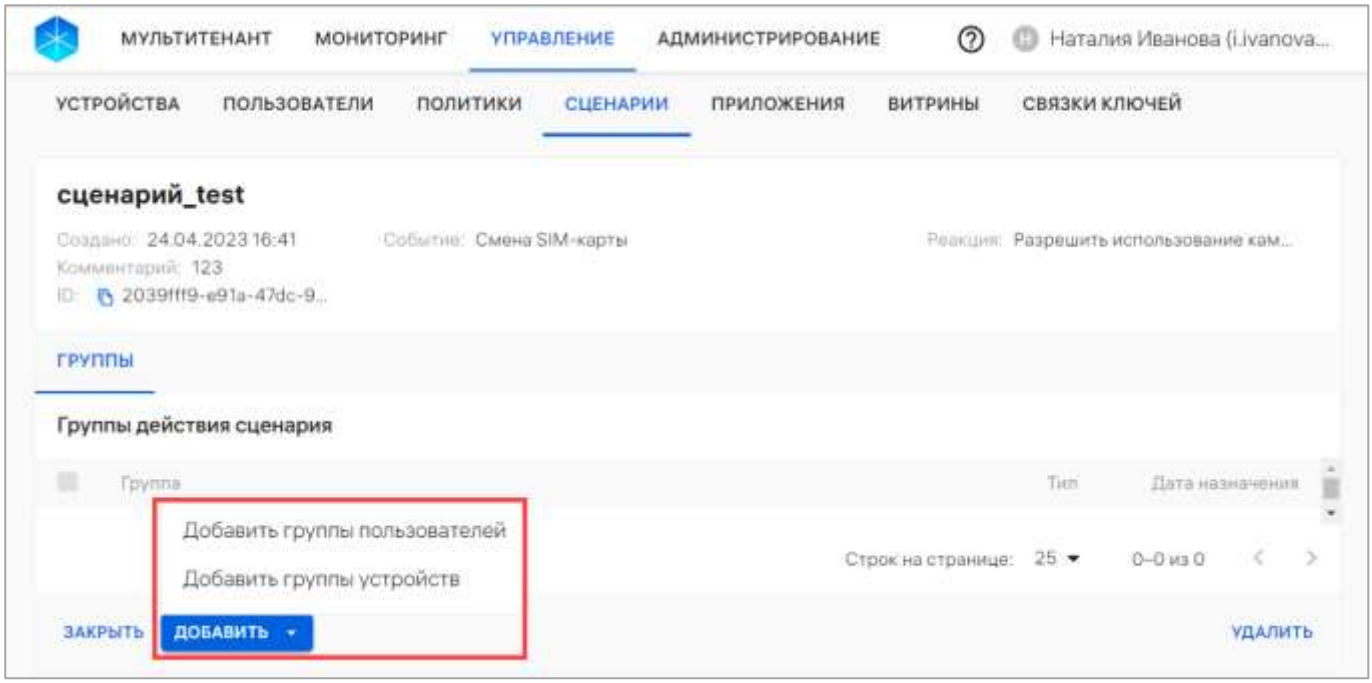

Рисунок 155

– в открывшемся окне «Назначение сценариев на группы» выбрать группу из списка, при необходимости воспользовавшись фильтром по названию группы (Рисунок 156);

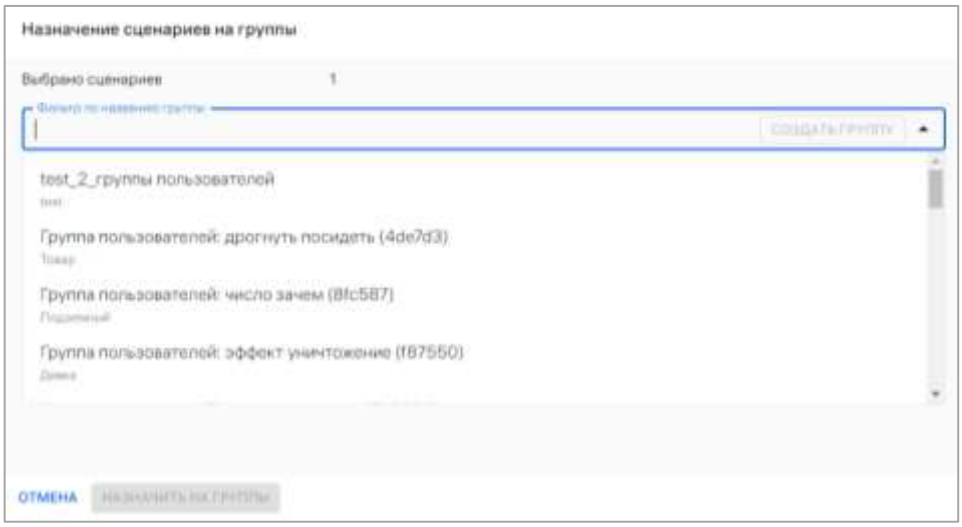

Рисунок 156

– добавленная группа отобразится в списке. При необходимости удалить добавленную группу из списка возможно, нажав значок 🗑 (Рисунок 157 [1]). 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» (Рисунок 157 [3]) либо отменить все последние действия нажатием кнопки «Отмена» (Рисунок 157 [2]).

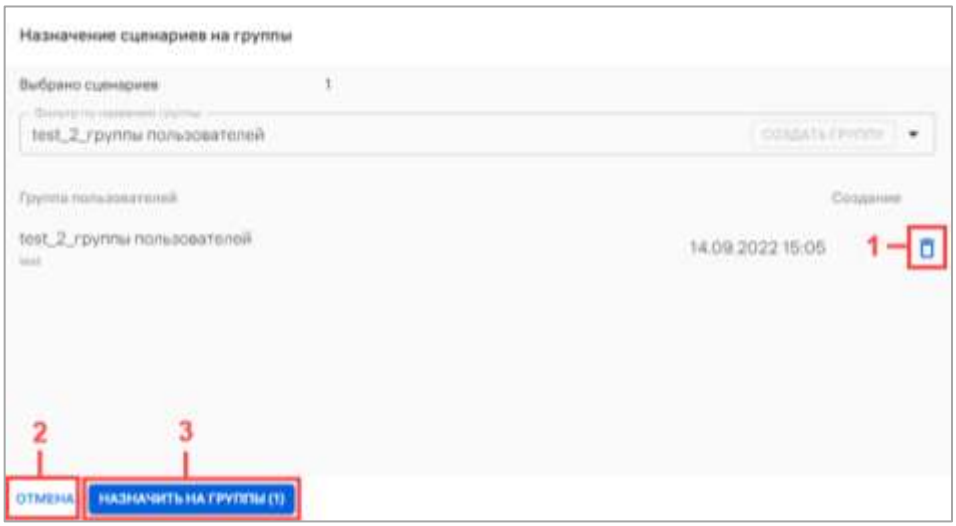

Рисунок 157

В результате применения офлайн-сценария отобразится сообщение «Сценарий успешно назначен на [Количество группы] группу».

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 158 [1]);

– в списке быстрых действий выбрать:

- значок для назначения офлайн-сценария на группу пользователей;
- значок для назначения офлайн-сценария на группу устройств;

– в открывшемся окне «Назначение сценариев на группы» выполнить действия приведенные в пп. 2.5.2.1.

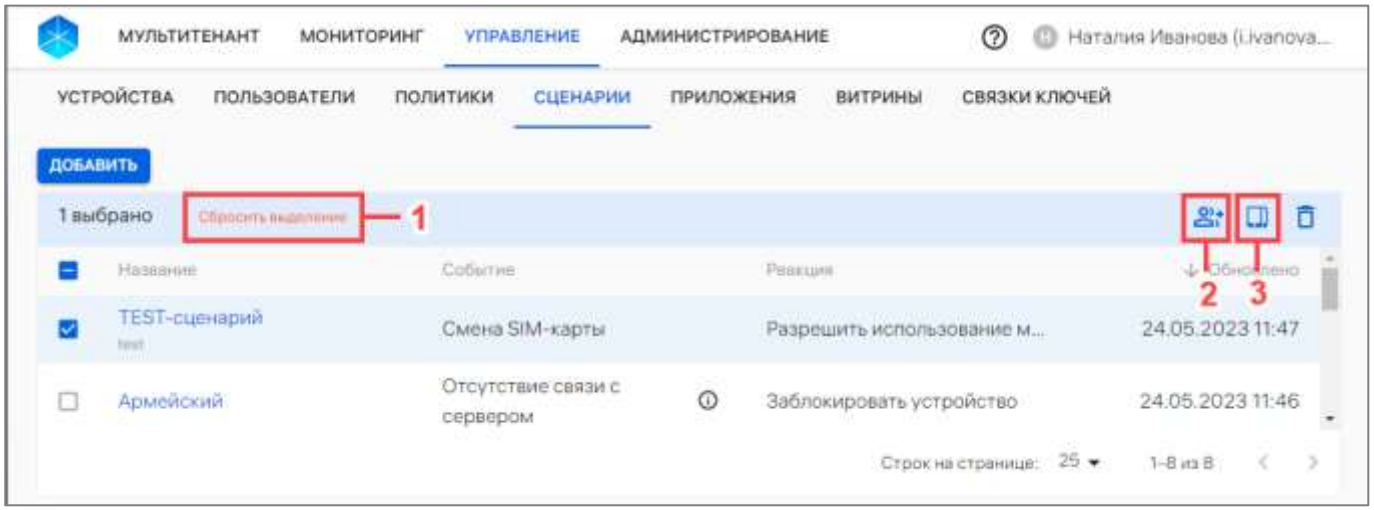

Рисунок 158

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»;

– выбрать группу устройств, при необходимости воспользоваться фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке перейти во вкладку «Сценарии»;

– нажать кнопку «Назначить сценарии» (Рисунок 159);

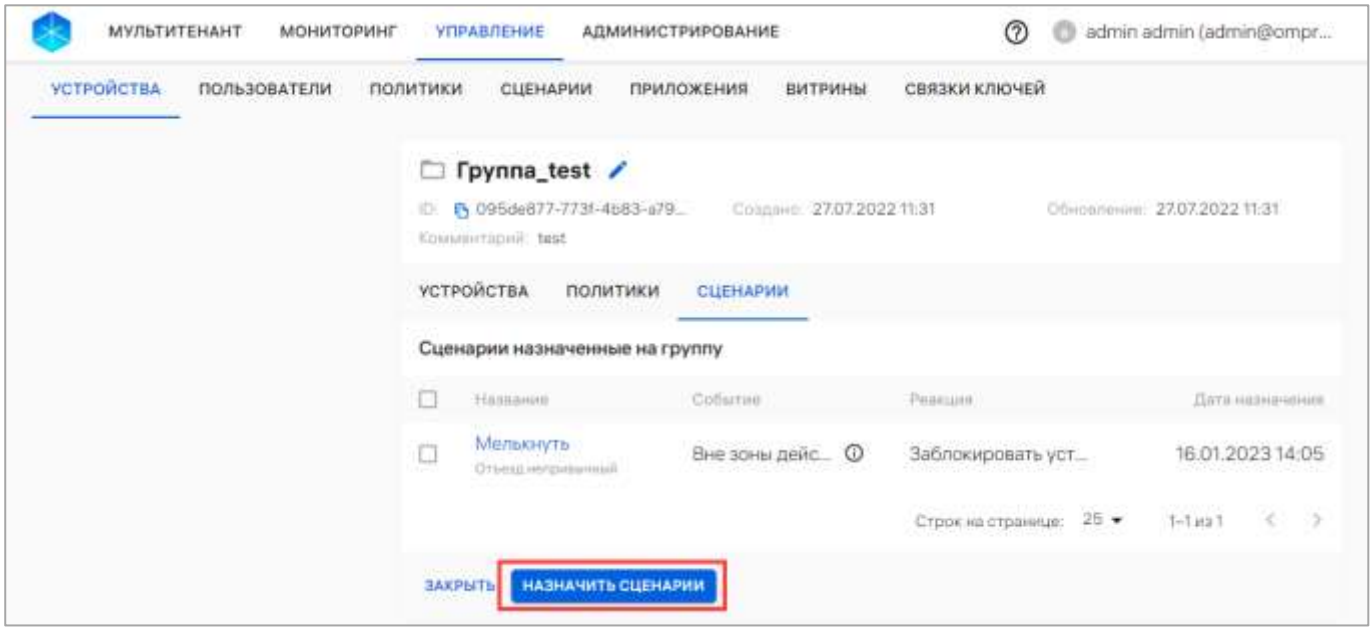

Рисунок 159

– в отобразившемся окне выбрать офлайн-сценарий из раскрывающегося списка или воспользоваться фильтром (Рисунок 160 [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 160 [3]);

Рисунок 160

– нажать кнопку «Назначить сценарии» (Рисунок 160 [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»;

– выбрать группу пользователей, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке перейти во вкладку «Сценарии»;

– нажать кнопку «Назначить сценарии» (Рисунок 161);

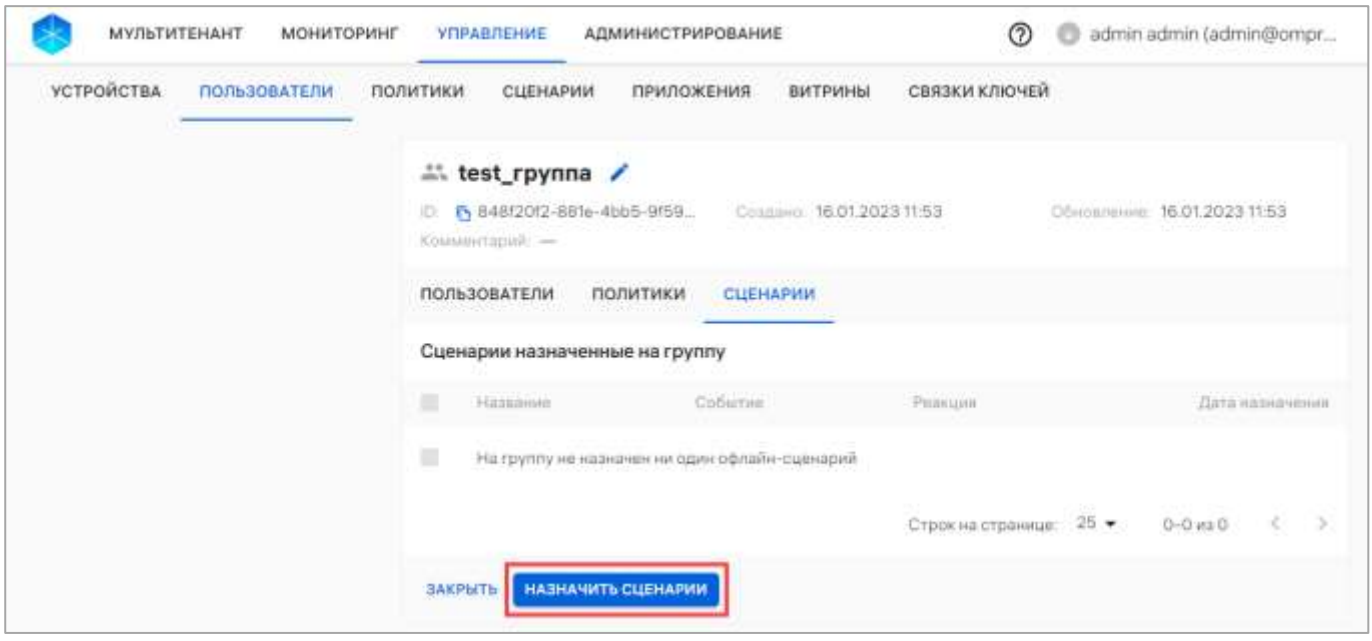

Рисунок 161

– 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 или 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 (пп. 2.5.3.2);

– через карточку группы пользователей (пп. 2.5.3.3).

2.5.3.1. Отвязка офлайн-сценария от группы устройств или группы пользователей через карточку офлайн-сценария

Для отвязки офлайн-сценария от группы устройств или группы пользователей необходимо выполнить следующие действия:

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

– перейти в карточку офлайн-сценария (п. 2.1.6);

– установить галочку в чекбоксе напротив группы, от которой необходимо отвязать офлайн-сценарий (Рисунок 162 [1]);

– нажать значок (Рисунок 162 [2]);

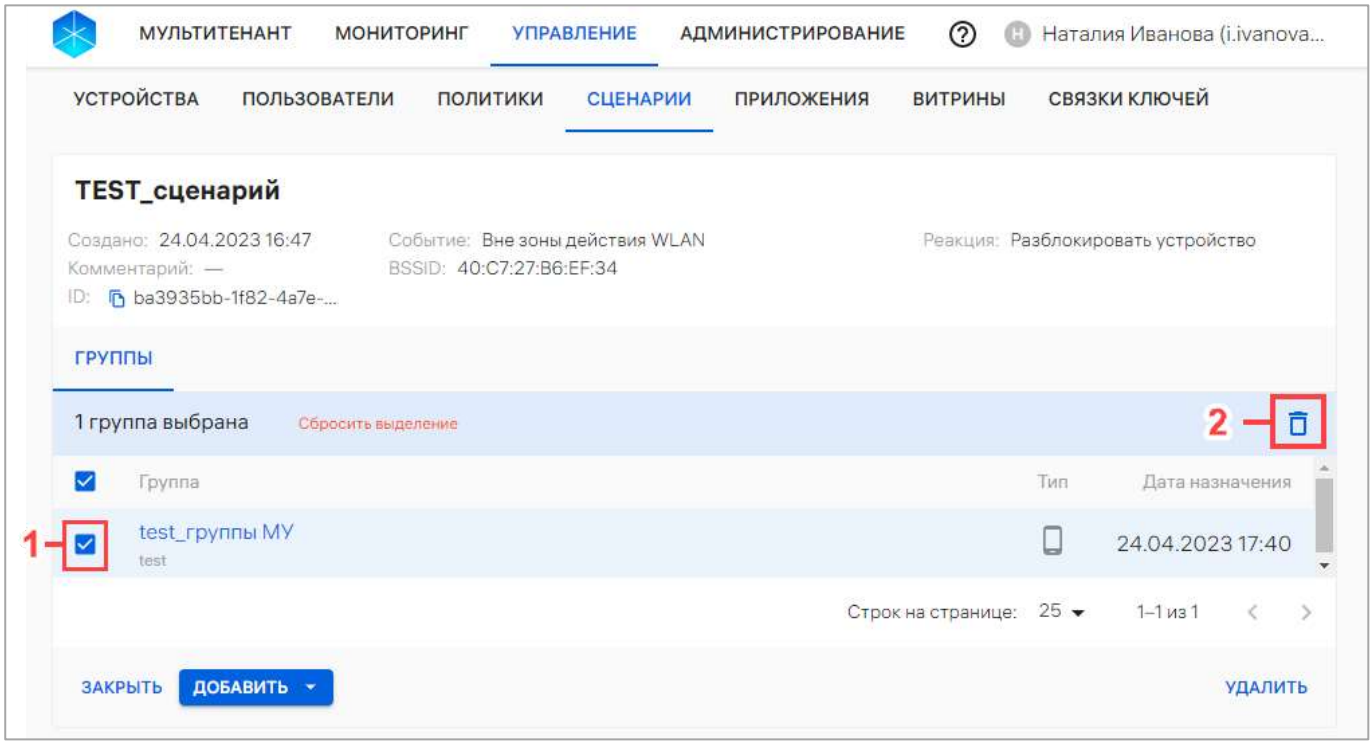

Рисунок 162

– в отобразившемся окне «Отвязка сценария от группы» подтвердить либо отменить действие (Рисунок 163).

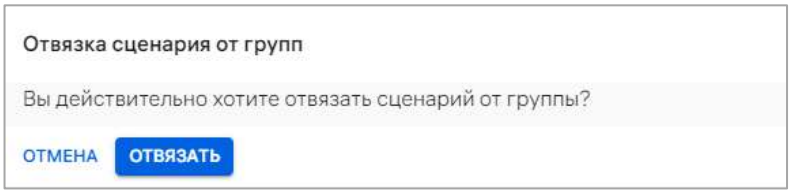

Рисунок 163

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-сценарий от группы устройств через карточку группы

Для отвязки офлайн-сценария от группы устройств через карточку группы необходимо выполнить следующие действия:

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

– в области фильтров выбрать «Поиск по группам»;

– выбрать необходимое группу устройств из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке группы устройств 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 164 [1]);

– в списке быстрых действий выбрать значок «Отвязать сценарии от группы» (Рисунок 164 [2]);

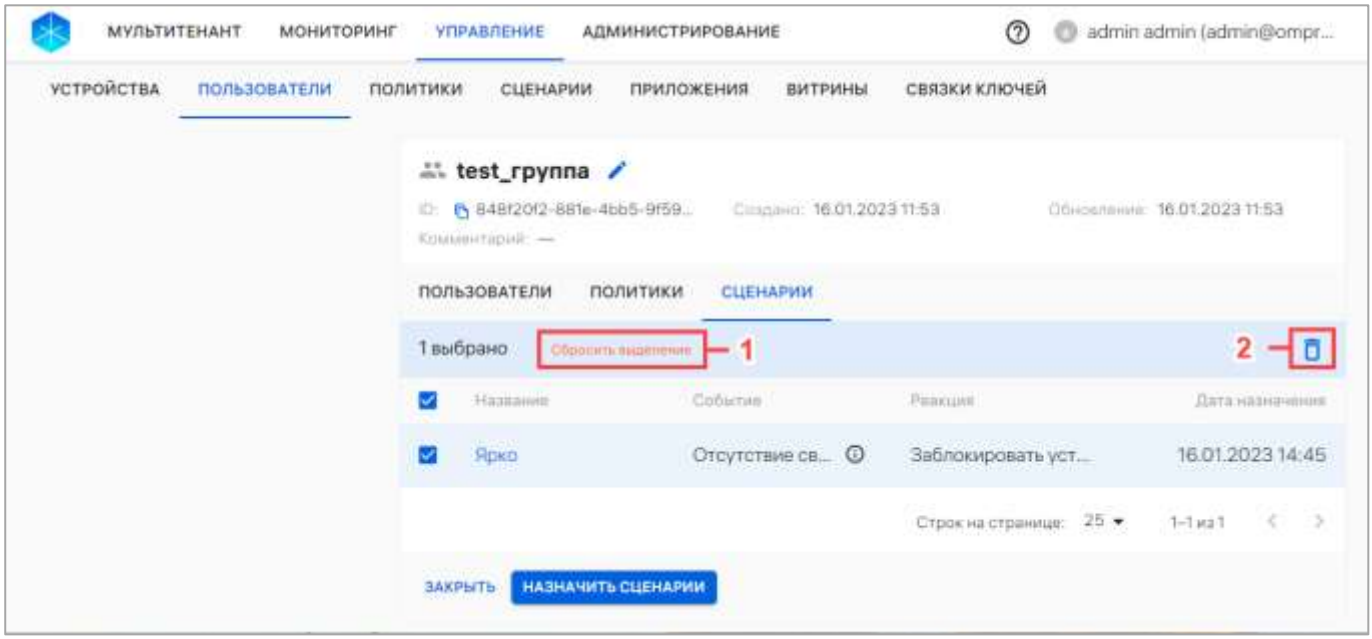

Рисунок 164

– в отобразившемся окне «Отвязка сценариев от группы» подтвердить либо отменить действия (Рисунок 165).

Рисунок 165

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

ВНИМАНИЕ! Если эффект данного офлайн-сценария уже применен на устройствах и при этом на них не назначена политика с противоположным действием, после отвязки офлайн-сценария его эффект не будет отменен.

2.5.3.3. Отвязка офлайн-сценарий от группы пользователей через карточку группы

Для отвязки офлайн-сценария от группы пользователей через карточку группы необходимо выполнить следующие действия:

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

– выбрать в области фильтров «Поиск по группам»;

– выбрать группу пользователей из списка, при необходимости воспользовавшись фильтром (подраздел 1.5), и перейти в карточку группы;

– в открывшейся карточке группы перейти во вкладку «Сценарии»;

– далее выполнить действия, описанные в пп. 2.5.3.2.

В результате офлайн-сценарий будет отвязан от группы пользователей.

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 166 [1]);

– в списке быстрых действий выбрать значок (Рисунок 166 [2]);

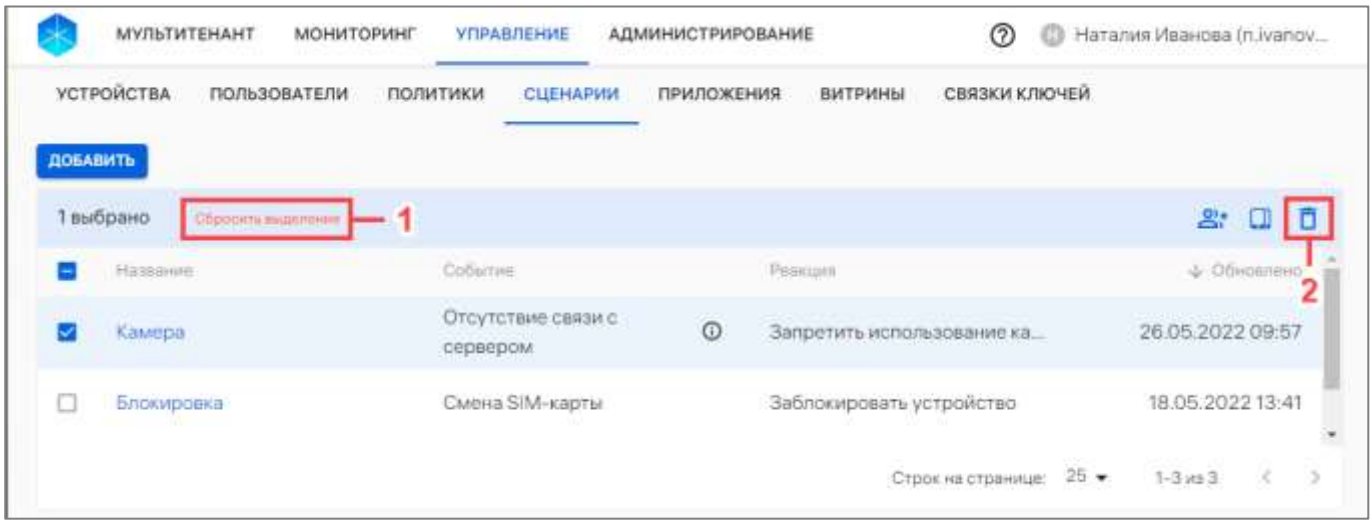

Рисунок 166

– в отобразившемся окне «Подтверждение операции» подтвердить либо отменить действия (Рисунок 167);

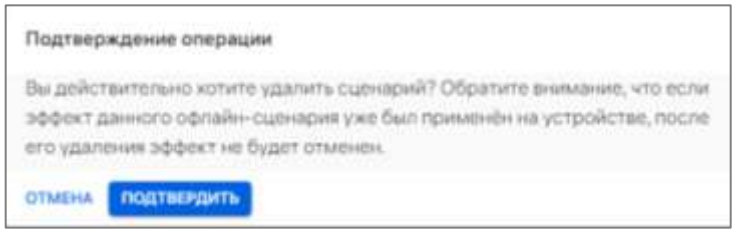

Рисунок 167

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 168);

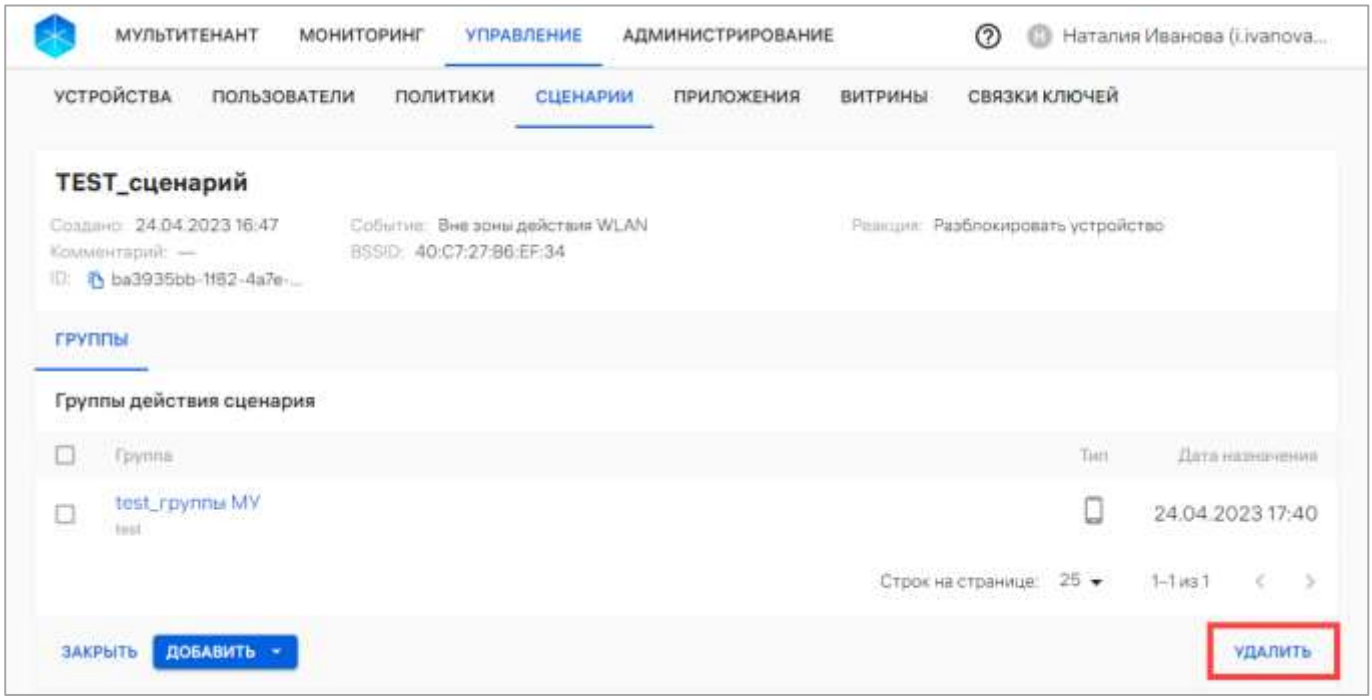

Рисунок 168

– в отобразившемся окне «Подтверждение операции» подтвердить либо отменить действия (см. Рисунок 167).

В результате успешного удаления офлайн-сценария отобразится сообщение «[Количество офлайн-сценариев] сценарий успешно удален из системы». При удалении офлайн-сценария 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.

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 169):

– «Подключение устройств»;

– «Соответствие политике»;

– «Активация устройств»;

– «Процессы».

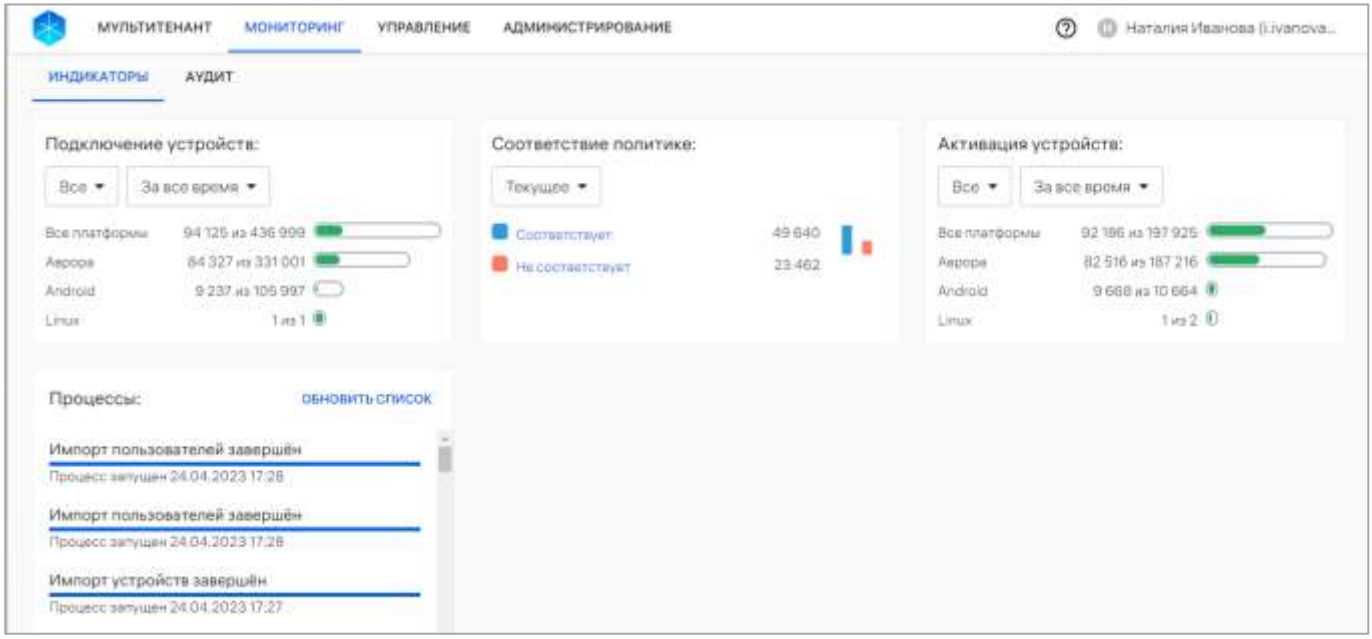

Рисунок 169

В подразделе «Индикаторы» предусмотрена возможность выбрать период отображения данных из раскрывающегося списка (Рисунок 170):

– «За все время» (недоступно для части «Соответствие политике»);

– «Текущее» (недоступно для части «Подключение устройств» и «Активация устройств»);

– «За сутки»;

– «За неделю»;

– «За месяц».

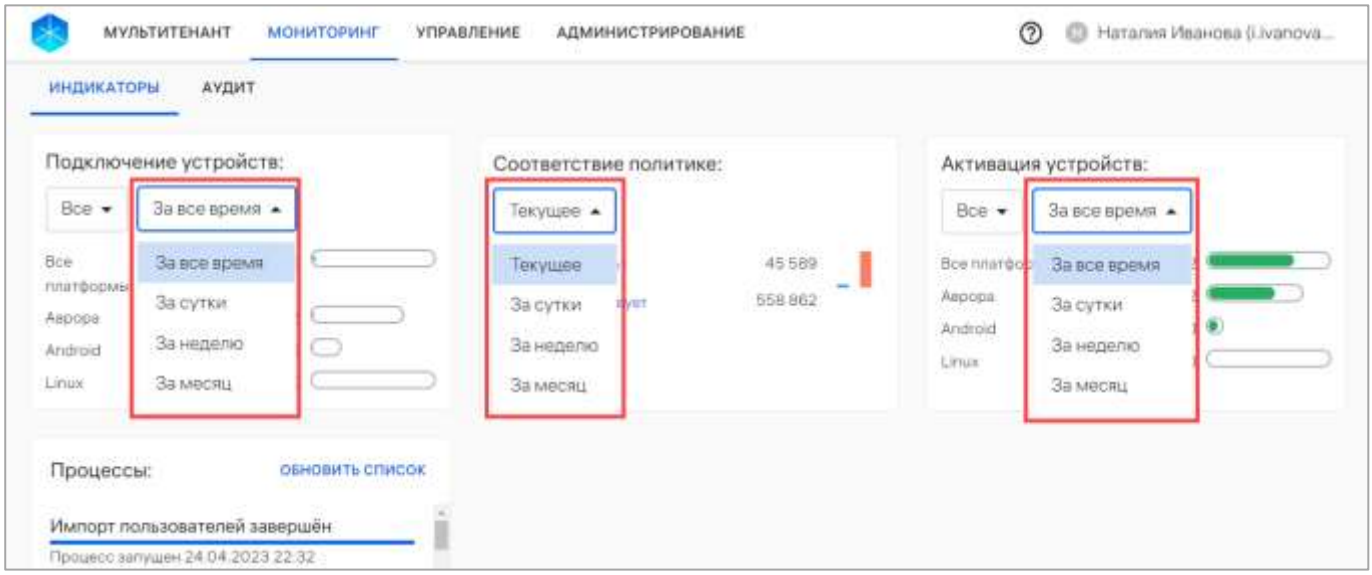

Рисунок 170

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 171):

– «Подключение устройств»:

- Все платформы (количество всех подключившихся устройств);
- Аврора (количество подключившихся устройств, функционирующих под управлением ОС Аврора);

– «Активация устройств»:

- Все платформы (количество всех активированных устройств);

- Аврора (количество активированных устройств, функционирующих под управлением ОС Аврора).

ВНИМАНИЕ! ОС Android, а также ОС семейства Linux, в комплект поставки не входят.

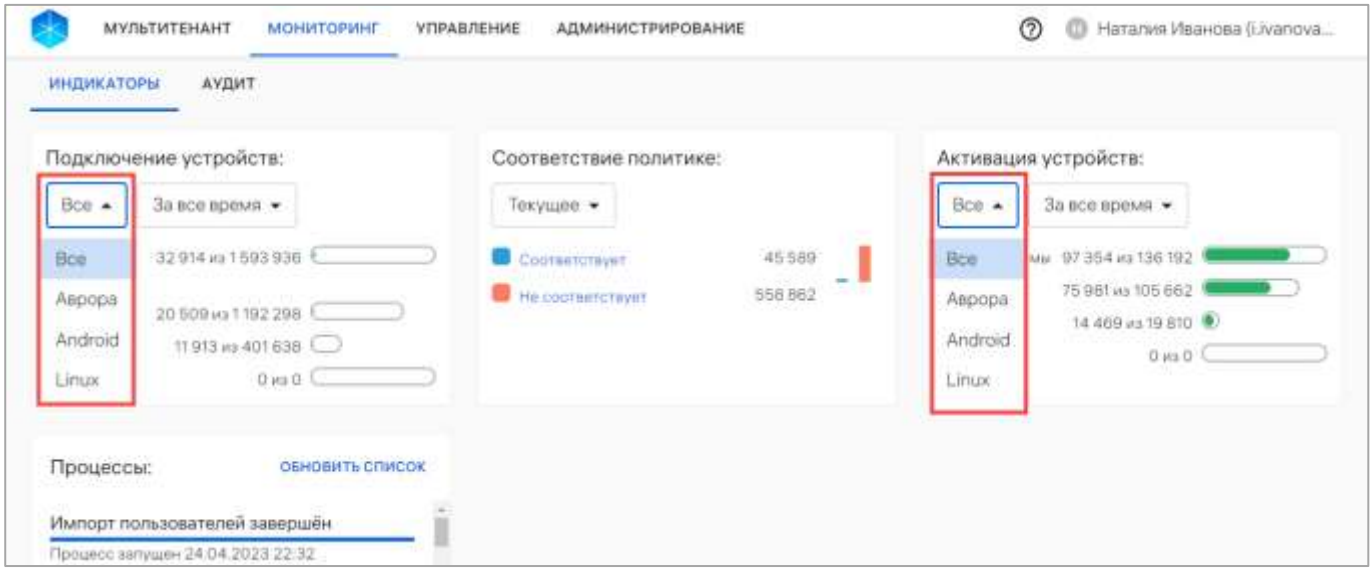

Рисунок 171

В результате отобразится диаграмма, а также количество подключенных или активированных и находящихся в процессе активации устройств для выбранной платформы (Рисунок 172).

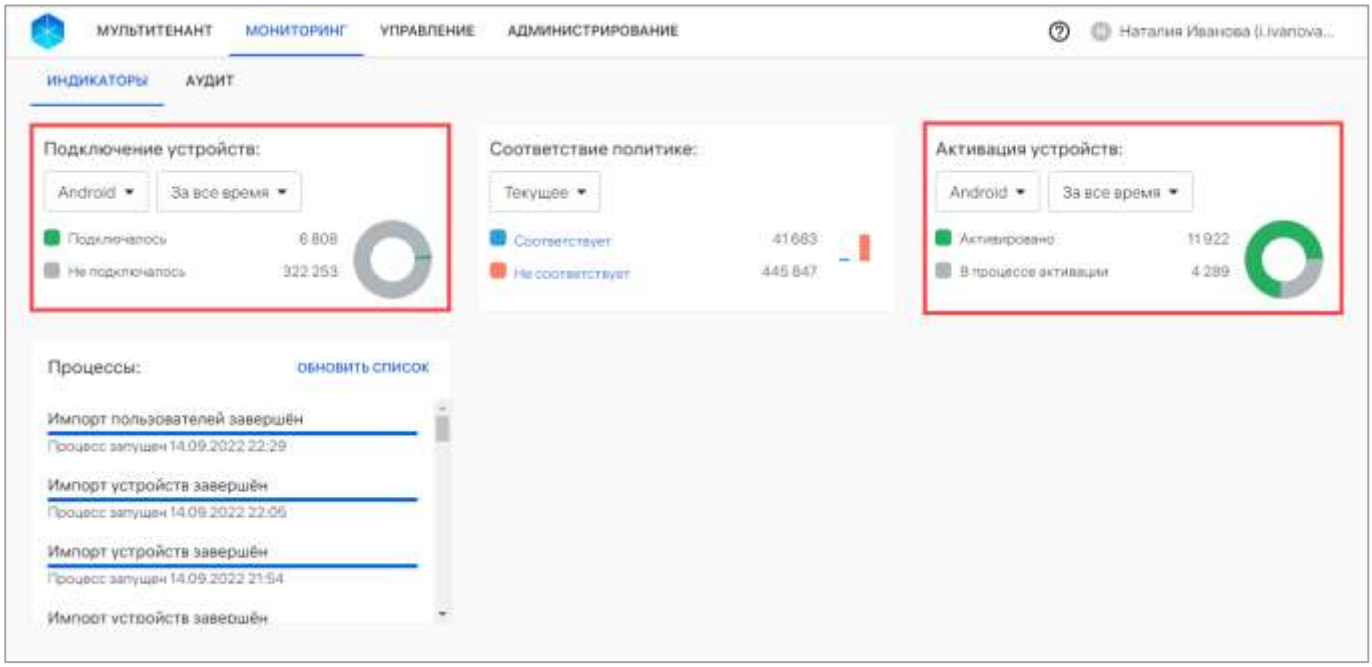

Рисунок 172

В окне «Соответствие политике» отображается информация по следующим показателям (Рисунок 173 [1]):

– Соответствуют политикам (количество устройств, соответствующих политикам);

– Не соответствуют политикам (количество устройств, не соответствующих политикам).

Указанные показатели выделены цветом и представляют собой активные ссылки. При переходе по ссылке:

– «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.

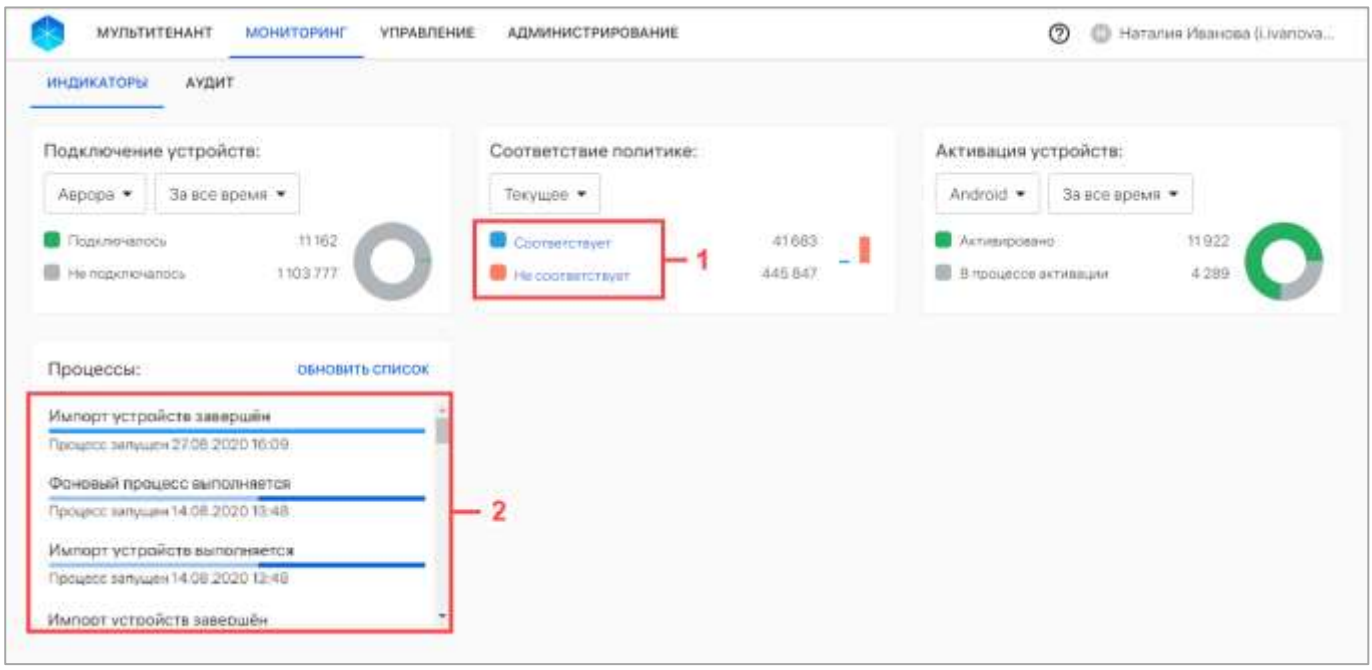

Рисунок 173

В окне «Процессы» отображаются завершенные и текущие процессы импорта устройств, пользователей и их групп из CSV-файла (Рисунок 173 [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 53, Рисунок 54).

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 (Рисунок 174 [1]);

– добавления и просмотра категорий пользовательских сертификатов (Рисунок 174 [2]);

– управления отображением архивных устройств (Рисунок 174 [3]);

– просмотра информации о (Рисунок 174 [4]):

- Сервере приложений (также представлена возможность включения/отключения витрин с клиентским 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);
- Центры сертификации.

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

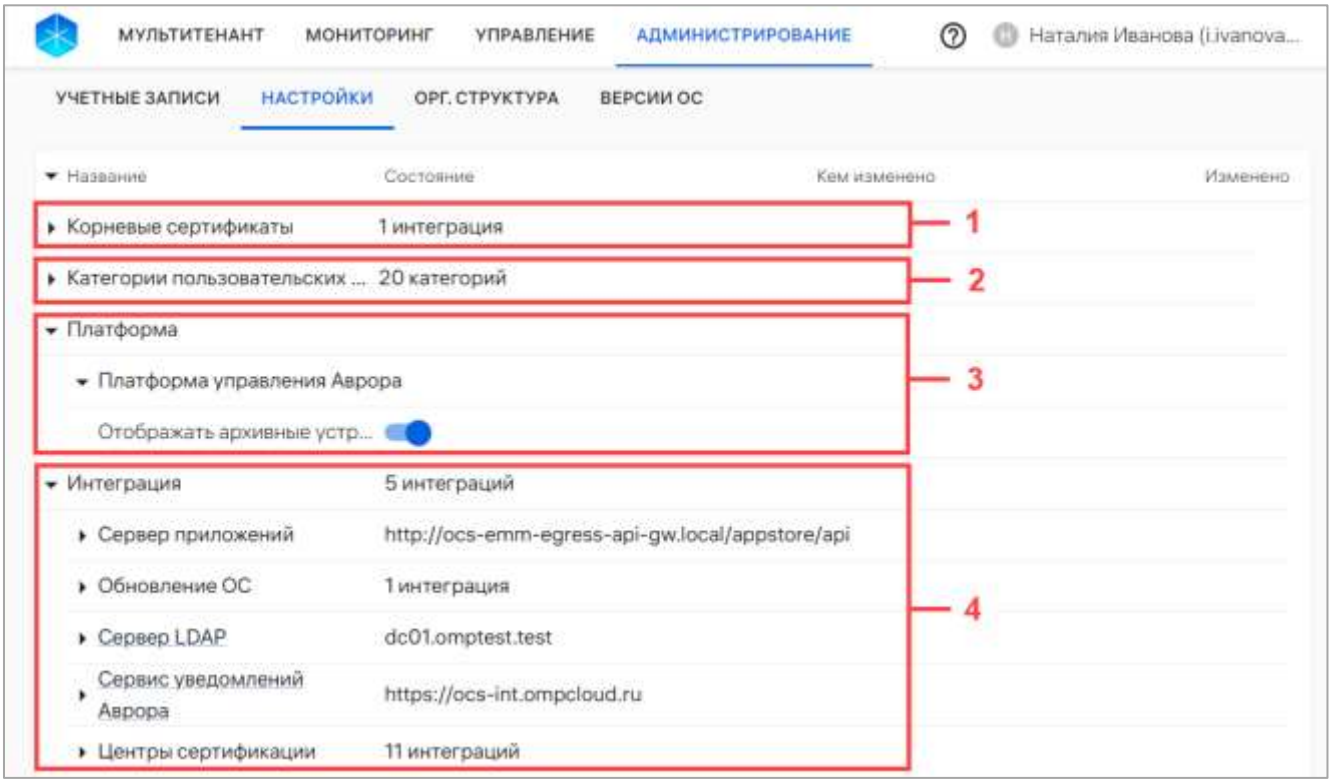

Рисунок 174

4.1.1. Доверенные сертификаты

В раскрывающейся строке «Корневые сертификаты» при нажатии на значок (см. Рисунок 174) отображается список доверенных сертификатов, добавленных в ПУ (Рисунок 175 [2]).

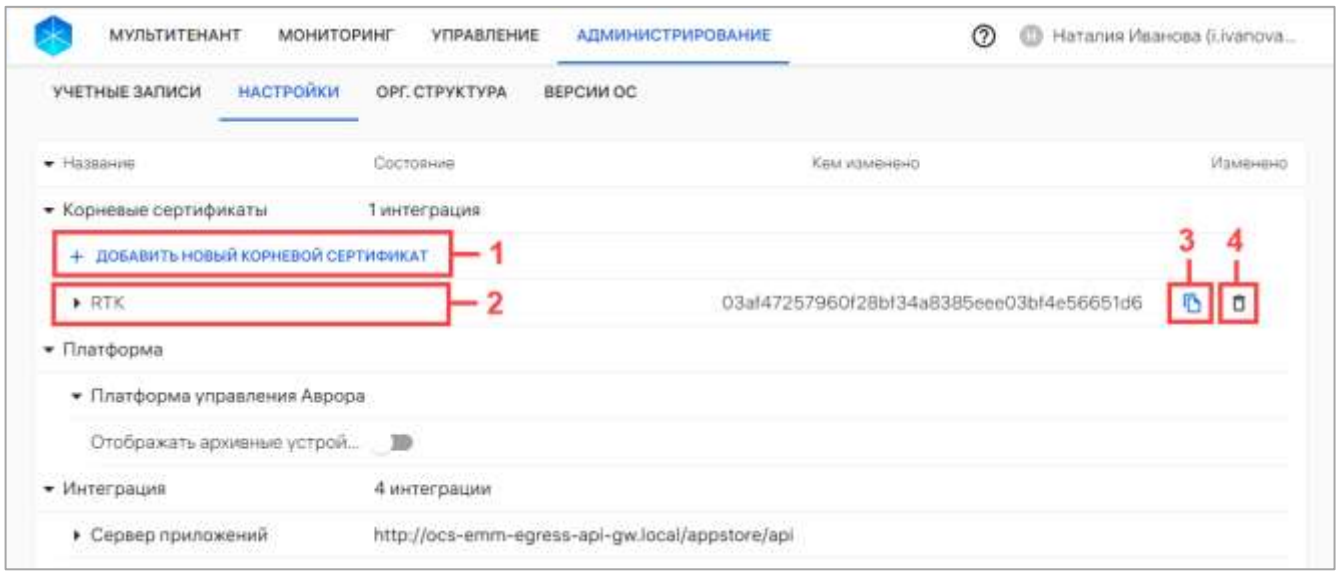

Рисунок 175

Для просмотра информации о доверенном сертификате необходимо в раскрывающейся строке названия сертификата нажать значок , в результате чего отобразится следующая информация (Рисунок 176):

– название удостоверяющего центра;

– дата выпуска сертификата;

– срок действия сертификата.

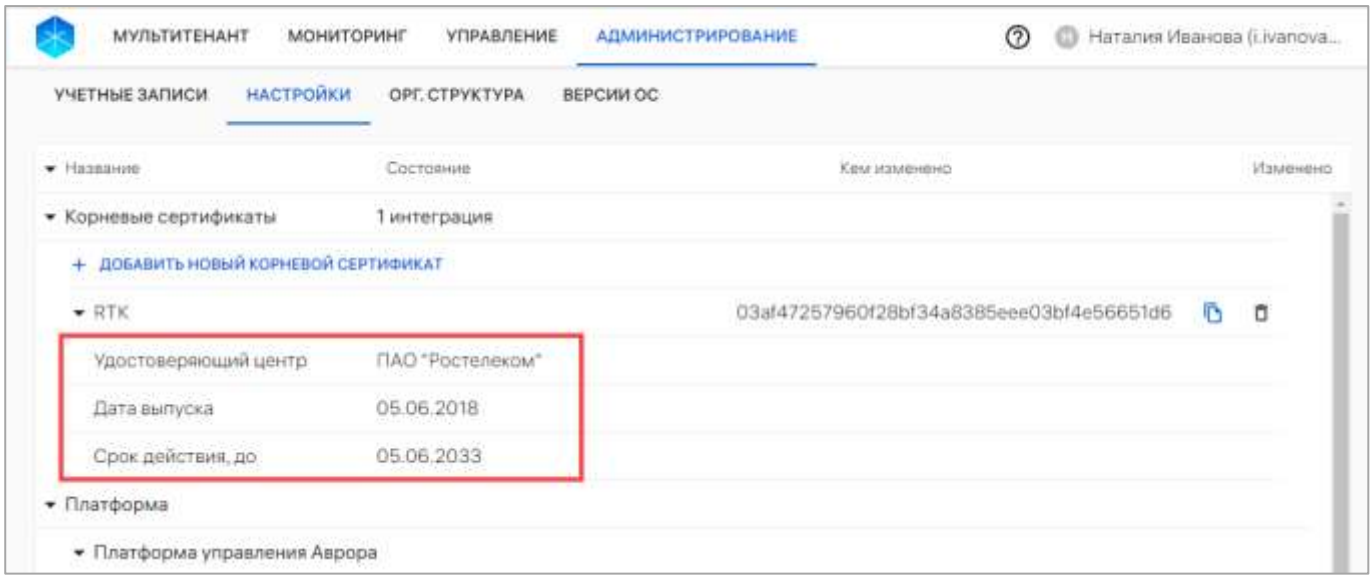

Рисунок 176

Для добавления новых сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить новый корневой сертификат» (Рисунок 175 [1]);

– в открывшемся окне в поле «Имя корневого сертификата» ввести название сертификата (Рисунок 177 [1]). Максимальная длина - 32 символа;

– нажать кнопку «Загрузить файл» (Рисунок 177 [2]) для последующего выбора файла для загрузки. Допустимые форматы: `.crt`, `.cer`, `.pem`;

– подтвердить либо отменить действия (Рисунок 177 [3]).

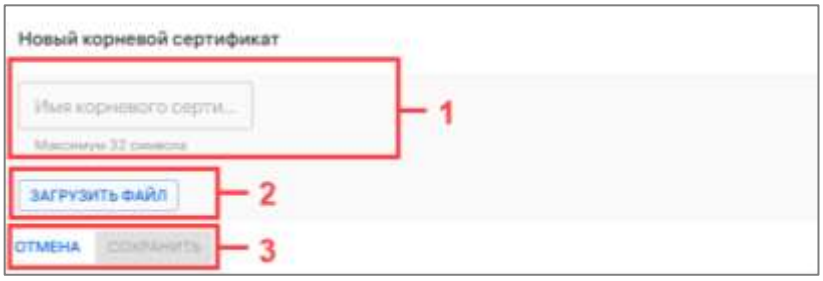

Рисунок 177

При успешном сохранении добавленный сертификат отобразится в списке доверенных сертификатов.

Также представлена возможность удалить сертификаты, выполнив следующие действия:

– нажать кнопку «Удалить сертификат» в строке сертификатов (см. Рисунок 175 [4]);

– в открывшемся окне «Удаление корневого сертификата» подтвердить либо отменить действия (Рисунок 178).

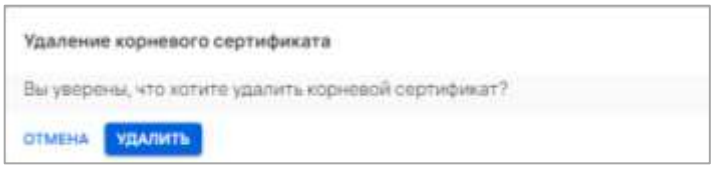

Рисунок 178

При успешном удалении сертификат будет удален из ПУ.

ПРИМЕЧАНИЕ. При следующем подключении устройства к Серверу приложений ПУ добавленные сертификаты будут установлены на устройстве, а удаленные сертификаты будут удалены с устройства.

При необходимости цифровой отпечаток (Fingerprint) сертификата возможно скопировать в буфер обмена нажатием значка «Копировать в буфер обмена» (см. Рисунок 175 [3]) в строке с сертификатом.

4.1.2. Категории пользовательских сертификатов

Категории пользовательских сертификатов используются для выпуска разных типов сертификатов для разных подключений определенному пользователю.

Список созданных категорий возможно посмотреть в раскрывающейся строке «Категории пользовательских сертификатов» при нажатии значка (см. Рисунок 174 [2]).

Для добавления категории пользовательских сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить категорию» (Рисунок 179);

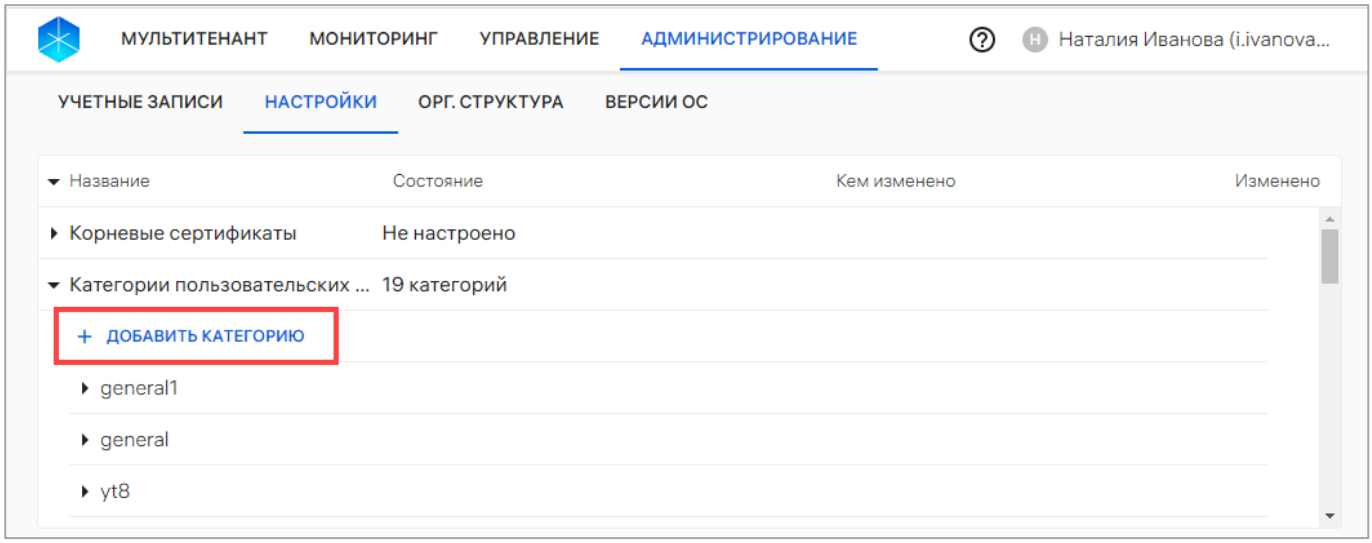

Рисунок 179

– в открывшемся окне (Рисунок 180) заполнить поля, приведенные в таблице (Таблица 28);

– 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.

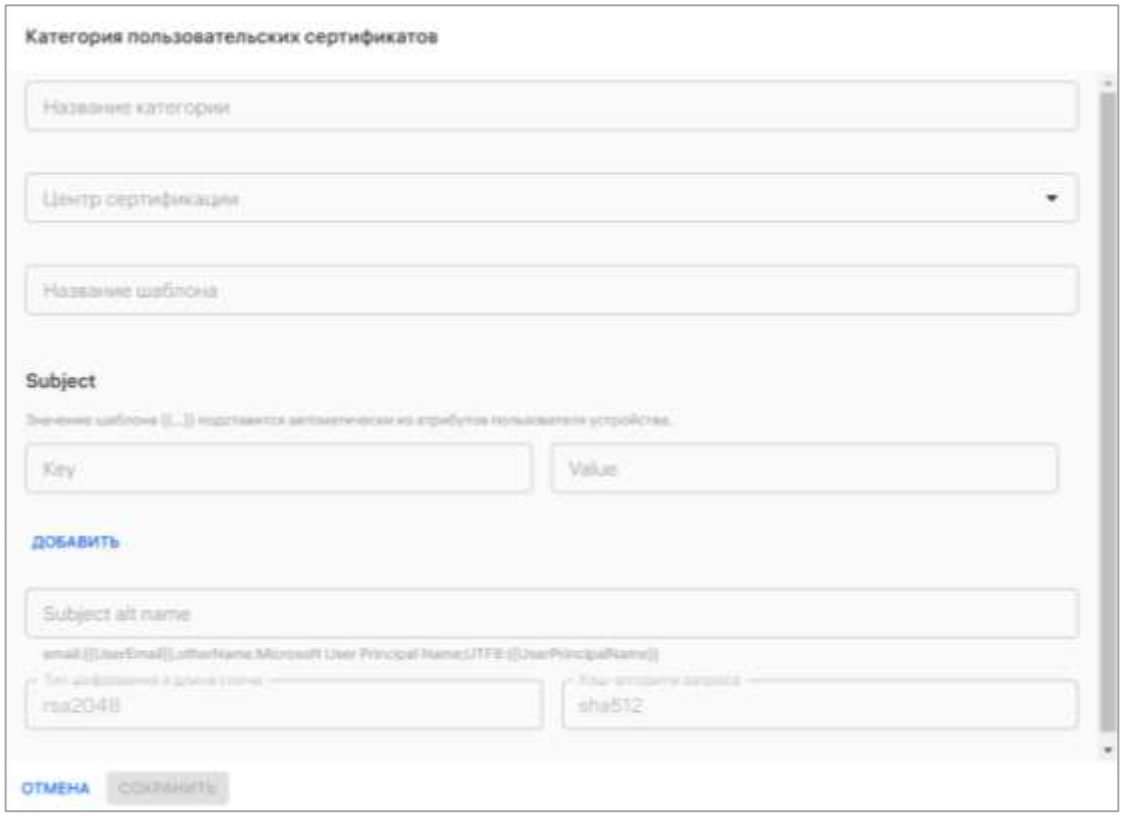

Рисунок 180

Таблица 28

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
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»

Параметр		Описание
	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. ВНИМАНИЕ! Ввод других динамических переменных недоступен. Поле обязательно для заполнения. 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). – {{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 174 [3]) необходимо активировать переключатель . В результате в подразделе «Устройства» раздела «Управление» в списке устройств будут отображаться архивные устройства (Рисунок 181).

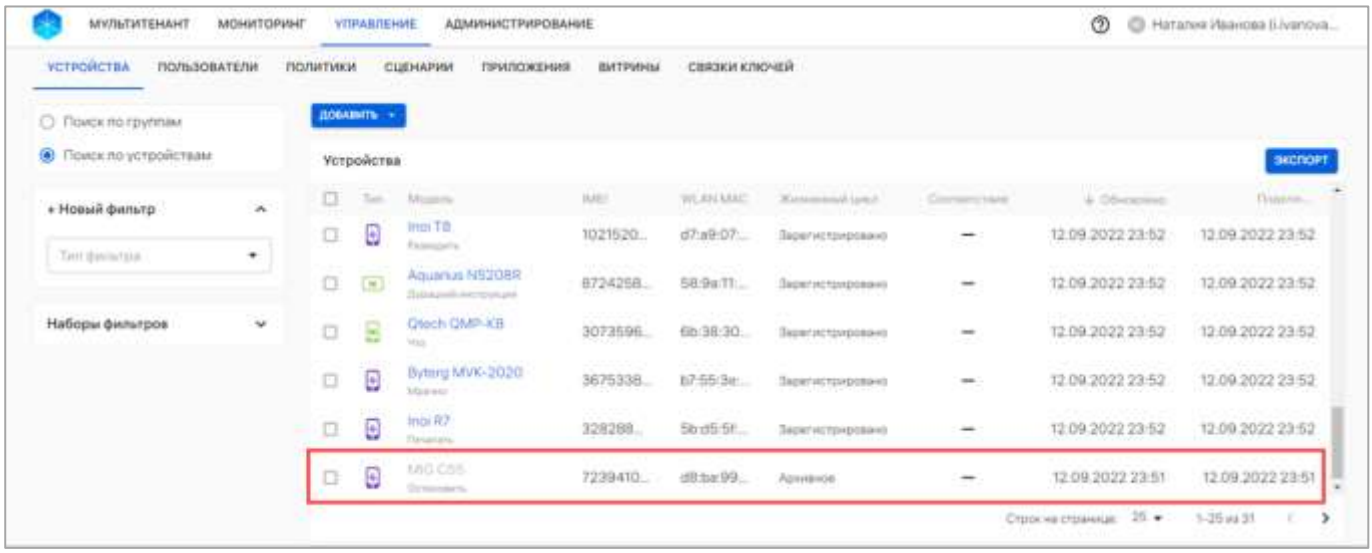

Рисунок 181

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 182 [1]) и список опубликованных витрин на Сервере приложений ПМ (Рисунок 182 [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 клиентские приложения на устройствах установлены с помощью политики, они не будут удалены с устройств после отключения витрины.

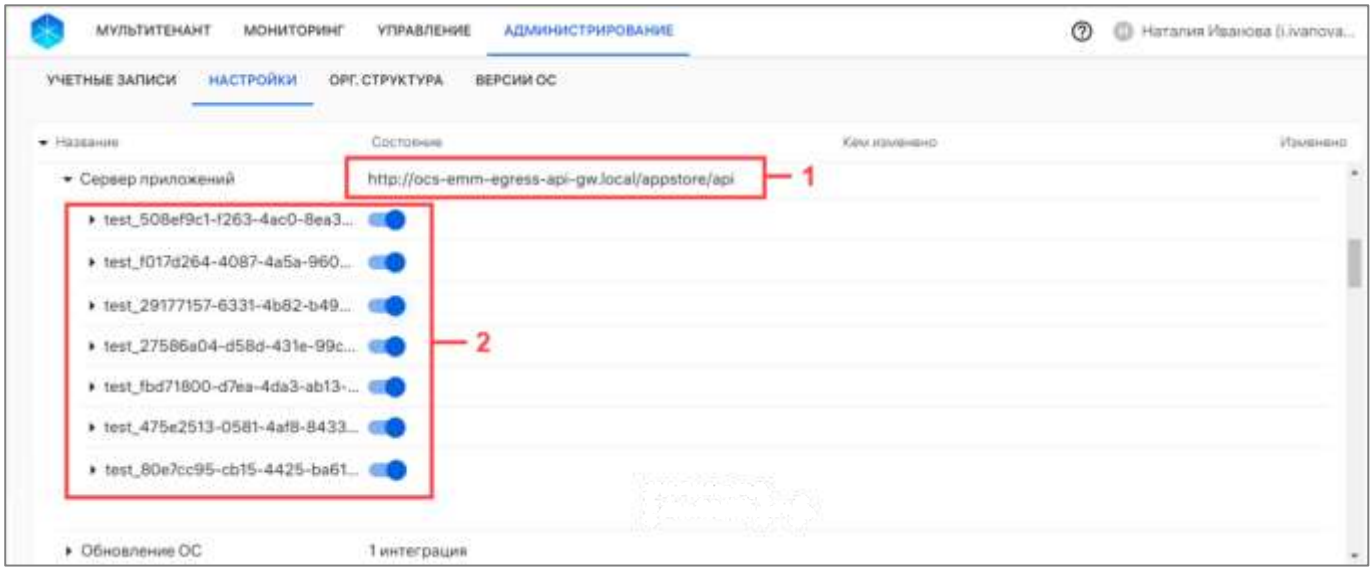

Рисунок 182

Для просмотра детальной информации о витринах во вложенных строках, которые доступны созданному тенанту, следует нажать значок .

Список опубликованных клиентских приложений формируется в ПМ. При отсутствии на сервере опубликованных МП 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 АДМГ.20134-01 90 01-2.

4.1.4.2. Обновление ОС

Обновление ОС - адрес сервера обновления ОС.

Для просмотра версий ОС необходимо нажать значок в строке «Обновление ОС».

4.1.4.3. Сервер LDAP

Сервер LDAP - адрес сервера LDAP. Во вкладке «Сервер LDAP» предусмотрена возможность 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:

1. Поддержка интеграции с другими LDAP-серверами не гарантируется;

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

3. ПУ поддерживает синхронизацию с LDAP-серверами, в которых пользователи и группы безопасности хранятся в одном или разных организационных юнитах (`Organizational Unit`);

4. 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 183);

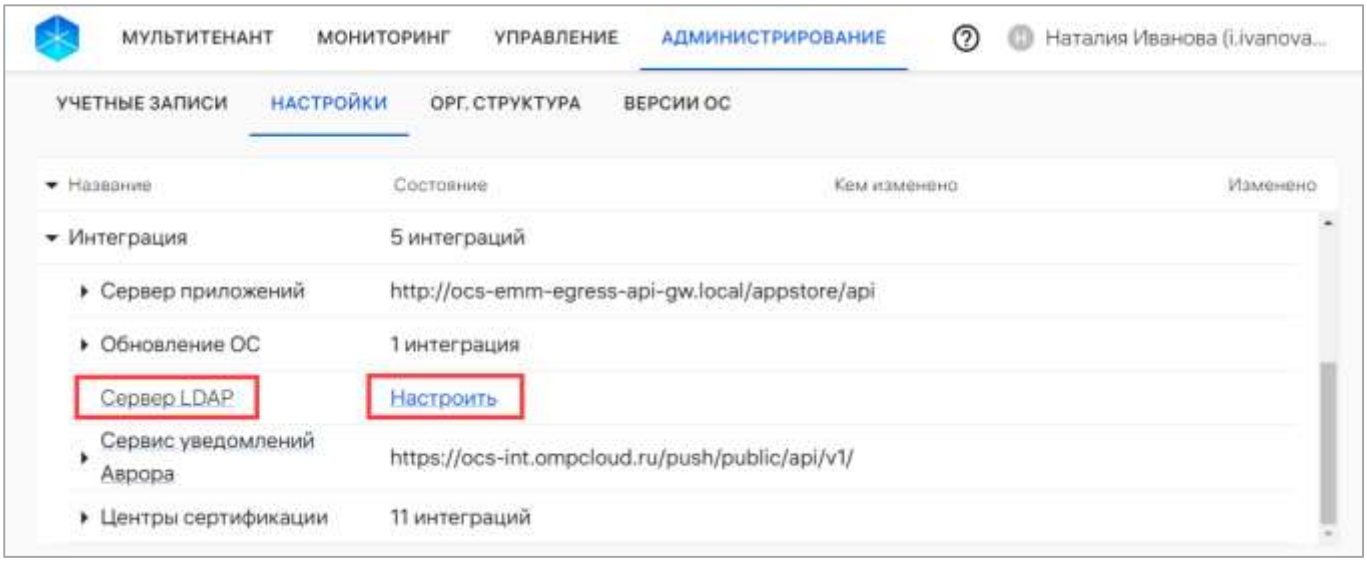

Рисунок 183

– задать настройки для подключения к LDAP-серверу (Рисунок 184 [1]) согласно таблице (Таблица 29);

Таблица 29

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
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)» установлен. 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

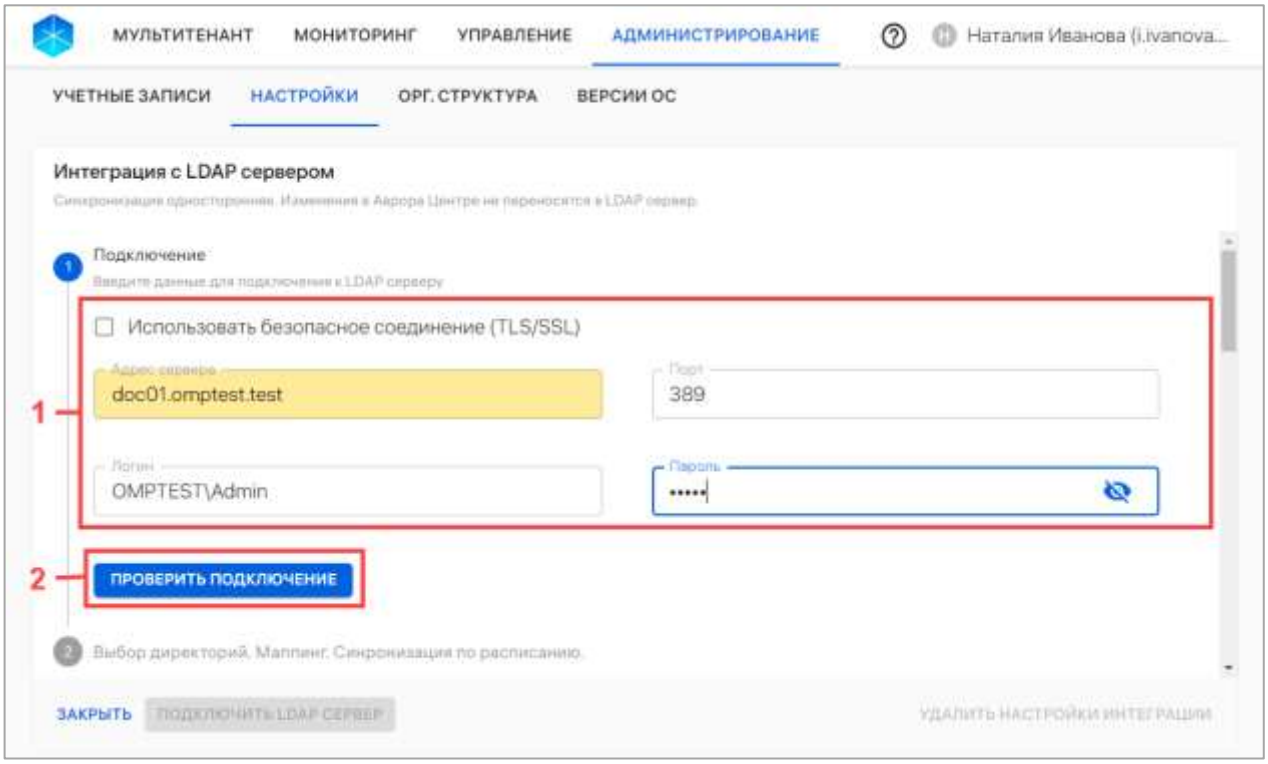

Рисунок 184

– нажать кнопку «Проверить подключение», чтобы проверить работоспособность подключения к LDAP-серверу с заданными настройками (Рисунок 184 [2]).

В случае успешной проверки отобразится сообщение «Подключение доступно» (Рисунок 185).

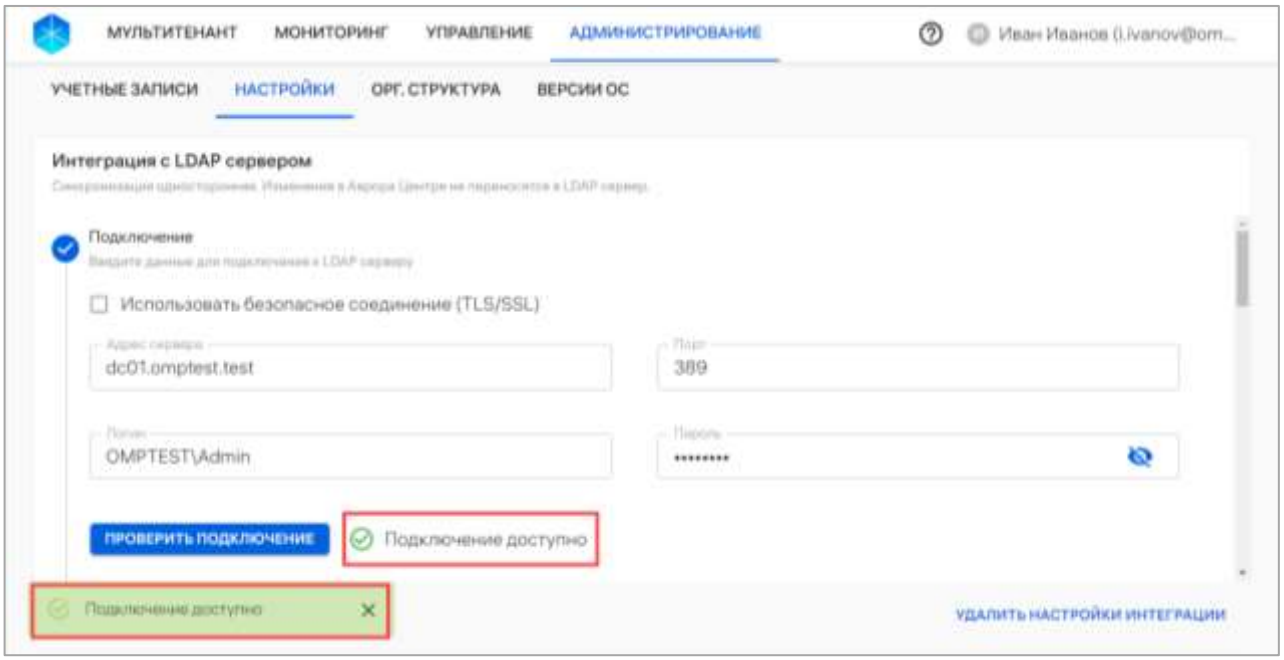

Рисунок 185

В случае неудачного завершения проверки отобразится сообщение об ошибке (Рисунок 186[1]), которую необходимо устранить и повторить проверку или обратиться к системному администратору/администратору LDAP.

Для ознакомления с полным текстом ошибки следует нажать «Подробнее» (Рисунок 186 [2]).

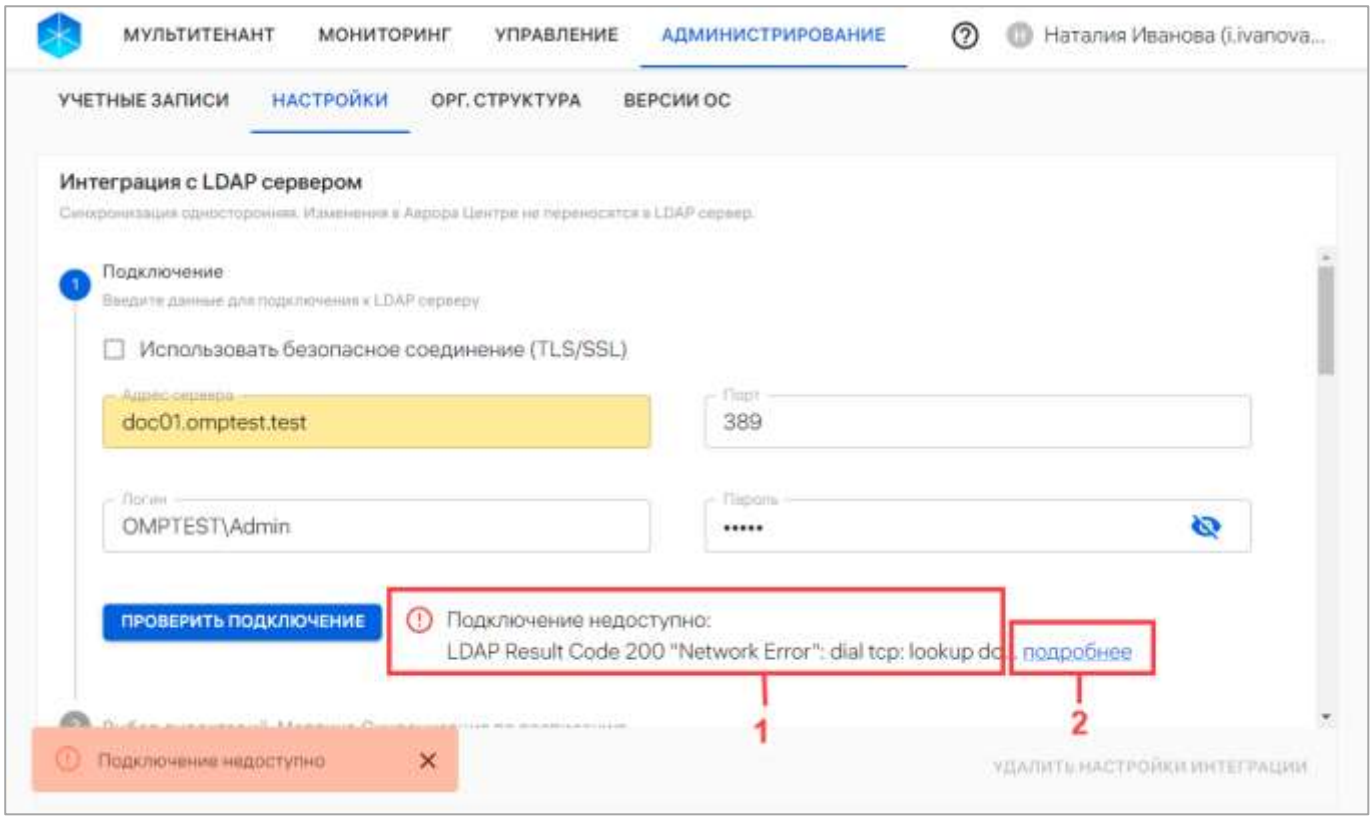

Рисунок 186

Задать область поиска в LDAP-сервере можно согласно таблице (Таблица 30), данные из которой будут синхронизироваться с ППО (Рисунок 187 [1]).

Таблица 30

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`.

Поле	Описание
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)`.

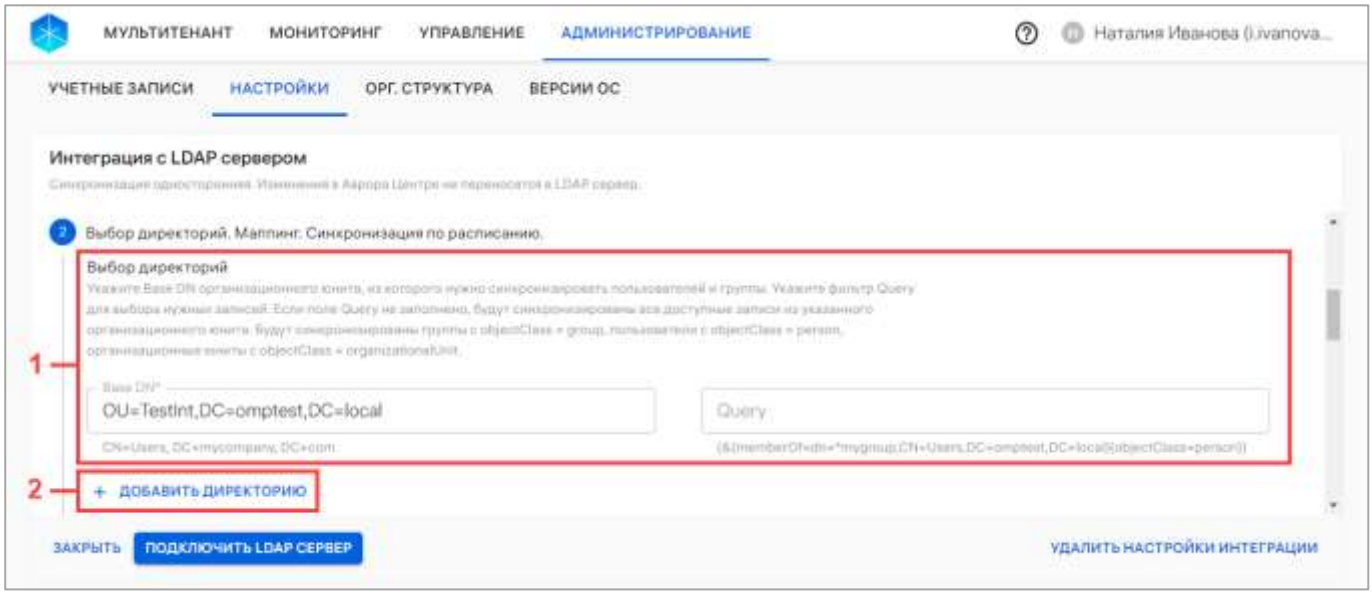

Рисунок 187

При необходимости добавить еще 1 директорию для синхронизации следует нажать «Добавить директорию» (см. Рисунок 187 [2]) и заполнить для нее поля «Base DN» и «Query» согласно таблице (Таблица 30).

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 188), приведенных в таблице (Таблица 31).

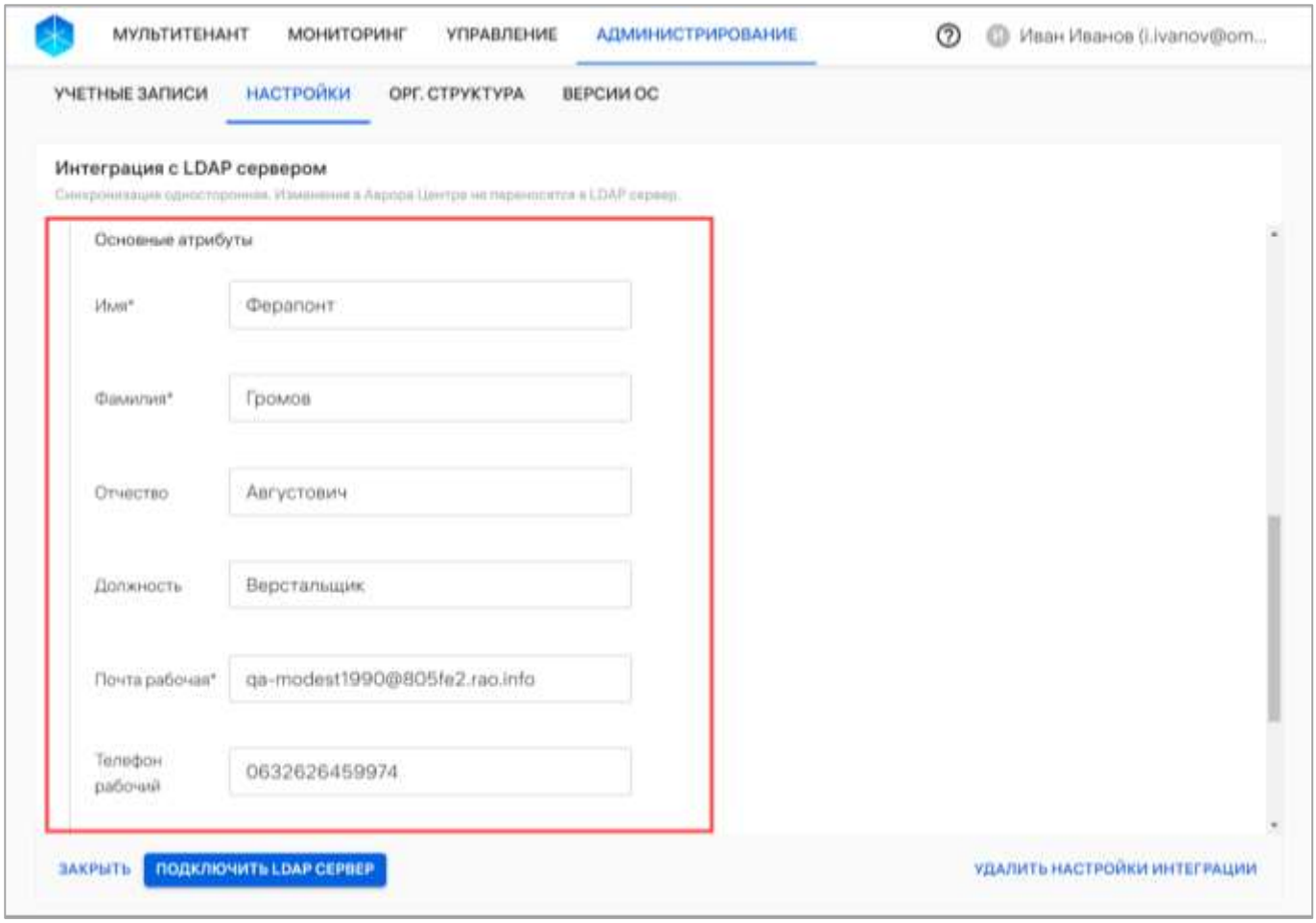

Рисунок 188

Таблица 31

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 32).

Таблица 32

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

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 189 [1]);

– изменить частоту синхронизации, то следует ввести нужный временной интервал в поле «Повторять каждые» (Рисунок 189 [2]).

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных.

Далее нажать «Подключить LDAP-сервер» (Рисунок 189 [3]).

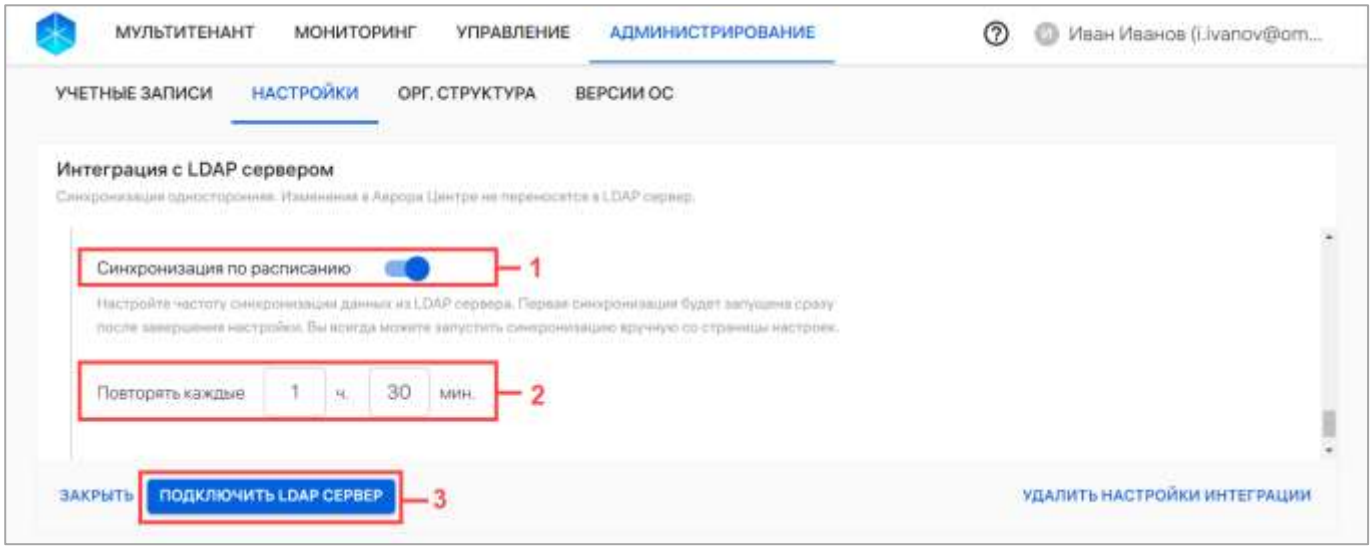

Рисунок 189

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 190).

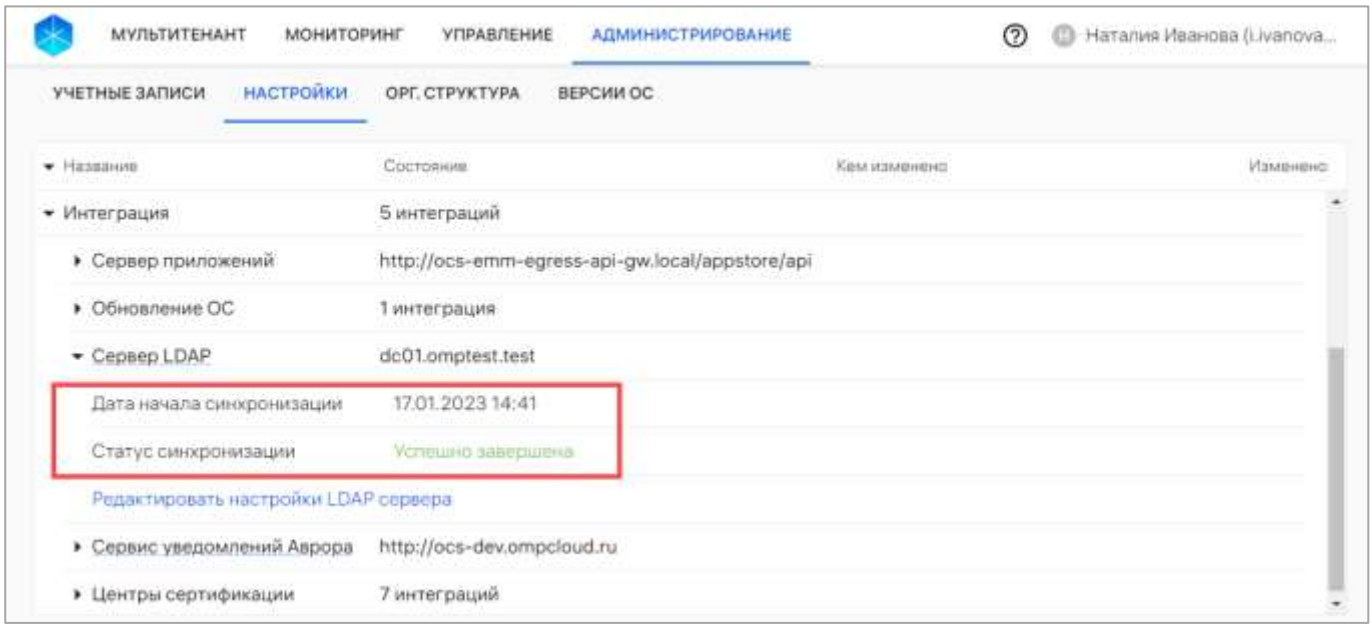

Рисунок 190

В случае ошибки синхронизации данных (Рисунок 191 [1]) для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (Рисунок 191 [2]).

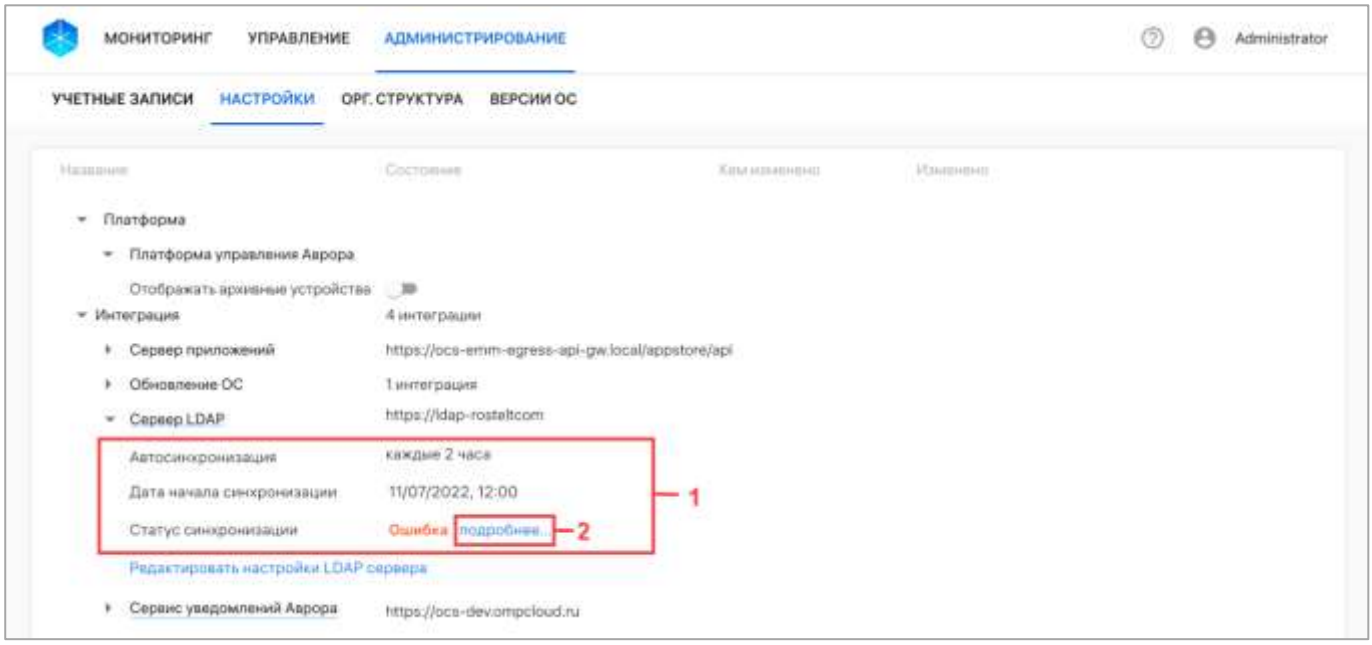

Рисунок 191

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 192 [1]) или развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера» (Рисунок 192 [2]);

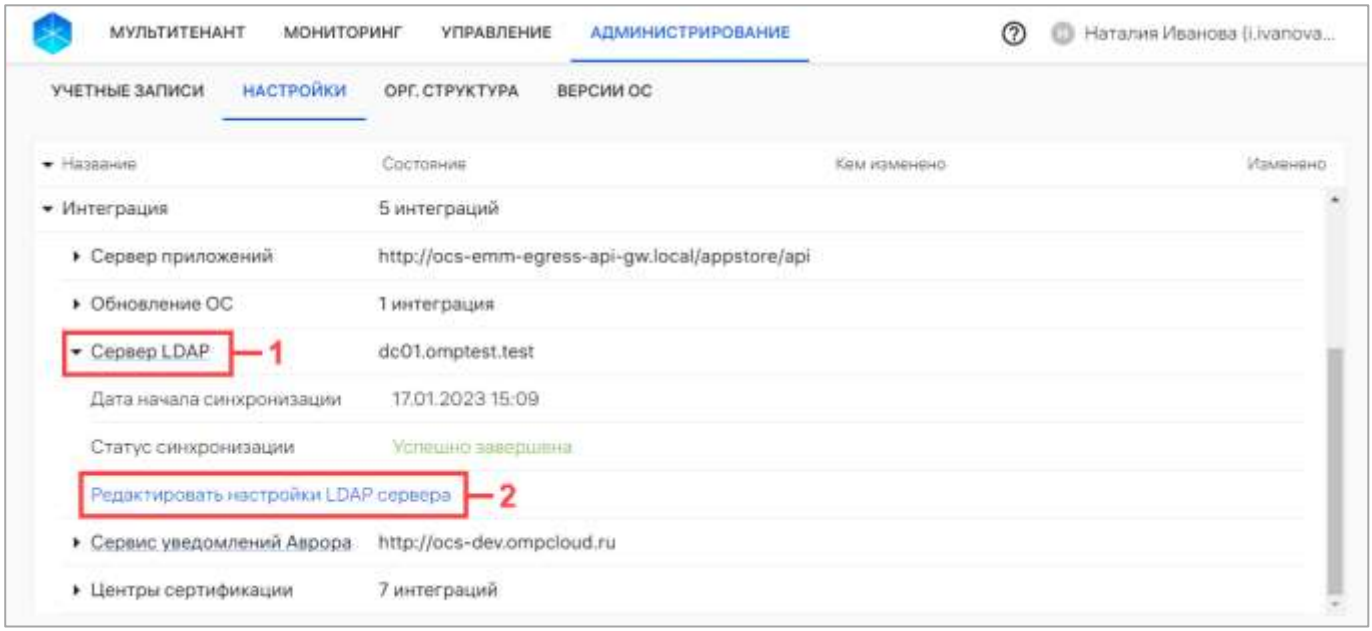

Рисунок 192

– 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 192 [1]) или развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера» (см. Рисунок 192 [2]);

– нажать кнопку «Удалить настройки интеграции» (Рисунок 193);

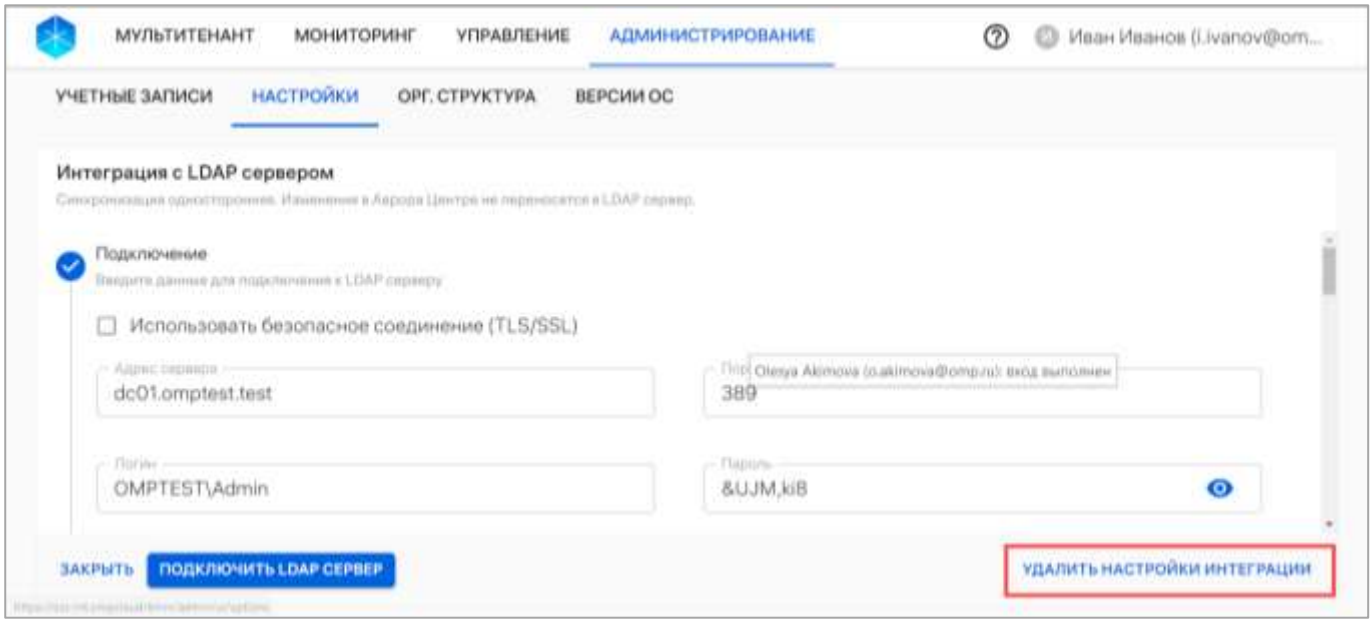

Рисунок 193

– в отобразившемся окне подтвердить либо отменить действия (Рисунок 194).

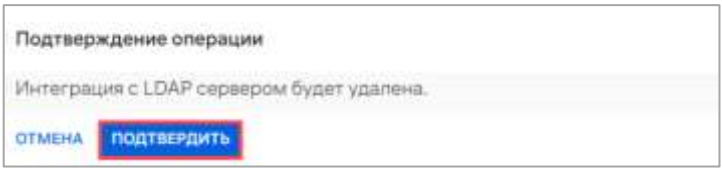

Рисунок 194

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 АДМГ.20134-01 90 01-7.

Описание работы ПСУ приведено в документе АДМГ.20134-01 90 01-5.

Для просмотра настроек ПСУ необходимо нажать значок , в результате чего отобразятся параметры, приведенные в таблице (Таблица 33).

Таблица 33

Настройки	Описание
Интеграция с СУА	Определяет включение отправки настроек ПСУ для клиентского приложения «Аврора Центр»
Настройки устройства	
Адрес для мобильного клиента	Адрес ПСУ для клиентского приложения «Аврора Центр»
Порт для мобильного клиента	Порт уведомлений для клиентского приложения «Аврора Центр»
ID приложения	Идентификатор клиентского приложения «Аврора Центр», с которым оно регистрируется в ПСУ
Дополнительные параметры (отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО	
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 клиентского 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 195 [1]);

– нажать «Редактировать настройки Сервиса уведомлений Аврора» (Рисунок 195 [2]).

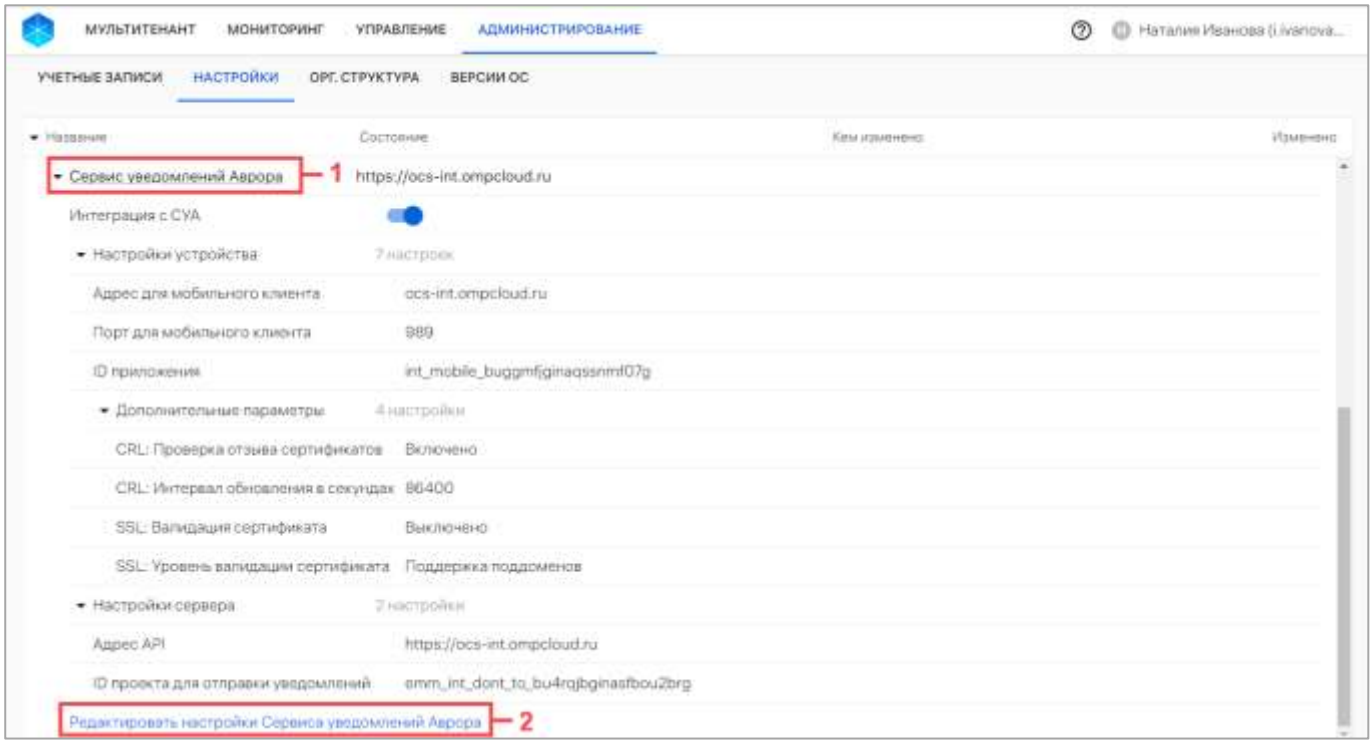

Рисунок 195

В результате выполнения одного из указанных действий будут доступны поля для редактирования настройки ПСУ одним из следующих способов (Рисунок 196):

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

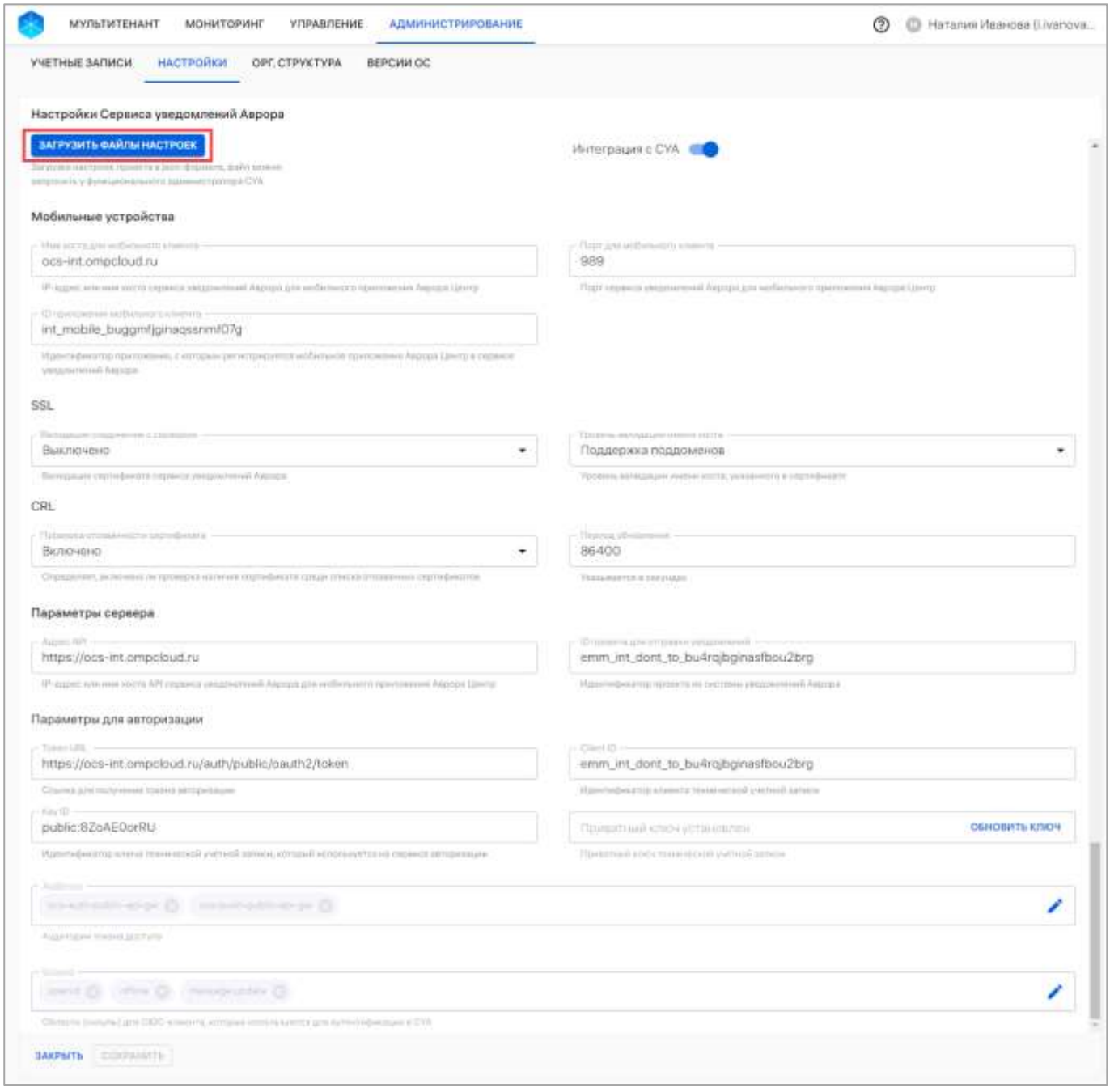

Рисунок 196

– внесение изменений вручную в соответствии с таблицей (Таблица 34).

Таблица 34

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

Поле	Описание
Мобильные устройства	
Имя хоста для мобильного клиента	IP-адрес или имя хоста ПСУ для клиентского приложения «Аврора Центр»
Порт для мобильного клиента	Номер порта уведомлений для клиентского приложения «Аврора Центр»
ID приложения мобильного клиента	Идентификатор приложения, с которым клиентское приложение «Аврора Центр» регистрируется в ПСУ
SSL (параметры SSL отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО	
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	
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 дляклиентского 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

После внесения уточнения необходимо подтвердить либо отменить действия.

4.1.4.5. Центры сертификации

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 197);

– заполнить поля ввода, приведенные в таблице (Таблица 35);

– нажать кнопку «Создать».

В результате интеграция с центром сертификации будет добавлена в ППО.

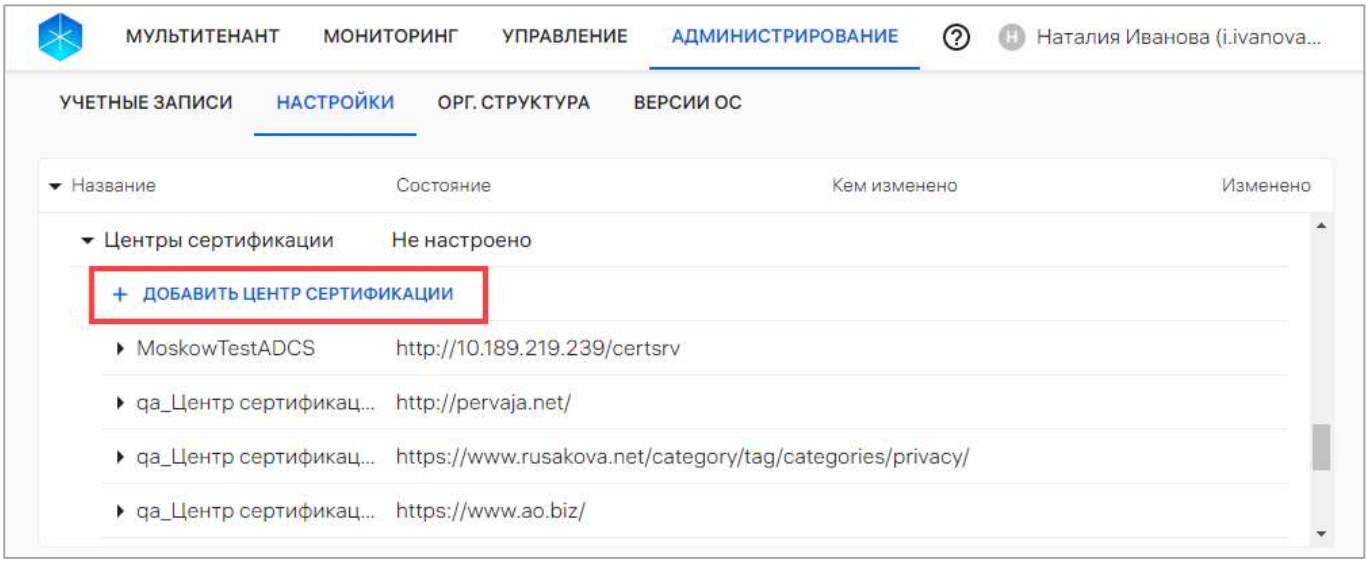

Рисунок 197

Таблица 35

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

4.2. 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). 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 198 [2]) либо при его отсутствии отобразится «Нет дочерних элементов» (Рисунок 198 [1]).

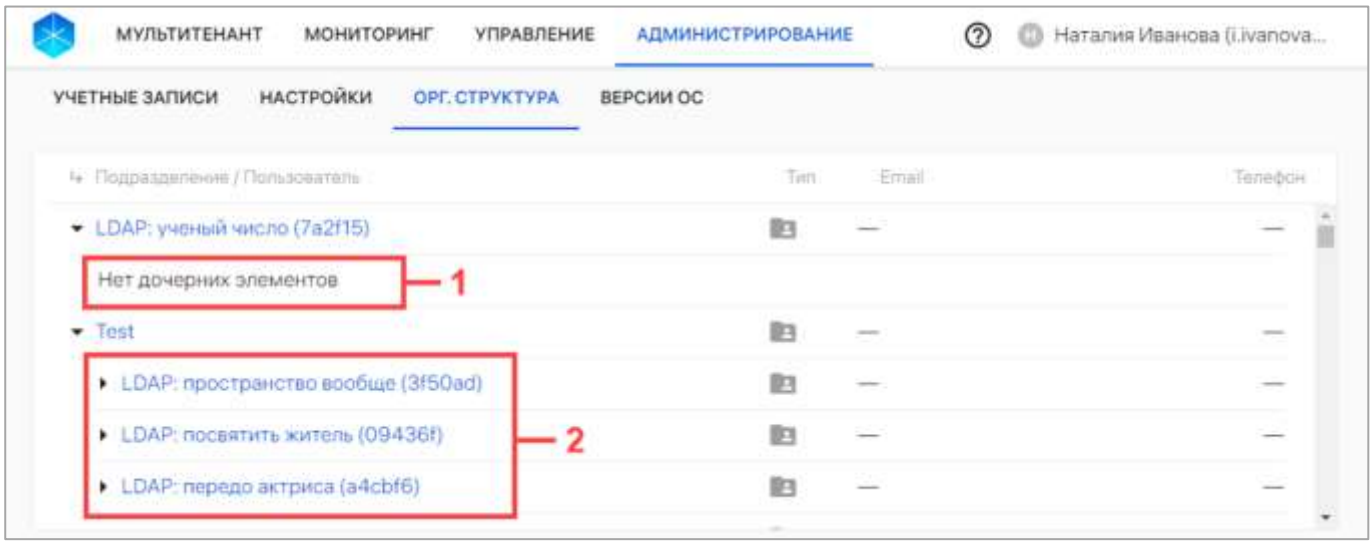

Рисунок 198

При отсутствии добавленных данных в подразделе «Орг.структура» отображается сообщение «Нет данных».

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 36).

Таблица 36

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
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. Подробная информация приведена в п. 2.2.7
7.	Произошла ошибка на стороне сервера. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
8.	Не удалось считать данные из JSON. Попробуйте другой JSON файл или исправьте этот	Загрузка некорректного JSON-файла. Необходимо поверить корректность загружаемого файла. Подробная информация приведена в п. 2.2.7
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 устройства
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
12.	Устройство с таким IMEI уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в подразделе 4.2
15.	Нельзя удалить непустую группу	Попытка удалить группу с назначенными устройств или пользователями. Необходимо исключить все дочерние элементы из группы, затем произвести удаление
16.	В JSON-файле не указан ID активации (`enrollmentID`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным `enrollmentID`. Подробная информация приведена в п. 2.2.7
17.	В JSON-файле не указан пароль (`password`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным паролем. Подробная информация приведена в п. 2.2.7

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
18.	В JSON-файле не указан адрес активации (`gatewayURI`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным адресом сервера активации. Подробная информация приведена в п. 2.2.7
19.	В JSON-файле не указан срок истечения (`expiredAt`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с актуальным сроком действия. Подробная информация приведена в п. 2.2.7
20.	Динамическая группа с такими условиями уже существует в системе	Попытка создания динамической группы с аналогичными условиями. Подробная информация приведена в п. 2.2.2
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
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». Подробная информация приведена в п. 2.2.2
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

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
28.	Редактирование динамических групп не допускается	Динамическая группа не подлежит редактированию. Подробная информация приведена в п. 2.2.4
29.	Проверьте корректность заполнения правил	Необходимо проверить корректность заполнения правил. Подробная информация приведена в пп. 2.4.2.1
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
33.	Некорректная структура файла. Проверьте файл на соответствие шаблону	Необходимо сверить заполненный CSV-файл с установленным шаблоном. Подробная информация приведена в п. 2.2.3 и 2.3.3
34.	Файл не содержит данных. Убедитесь, что выбран нужный файл	Необходимо загрузить CSV-файл с заполненными данными. Подробная информация приведена в п. 2.2.3 и 2.3.3
35.	Некорректная модель устройства	Необходимо проверить корректность заполненных данных в CSV-файле. Подробная информация приведена в п. 2.2.3 и 2.3.3
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

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
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
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. Подробная информация приведена в п. 2.2.3 и п. 2.3.3
52.	Указанные данные не прошли проверку. Скорректируйте данные перед отправкой	Указанные данные не прошли проверку. Необходимо скорректировать данные перед отправкой

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
53.	Ошибка валидации заголовка. Указаны некорректные названия колонок. Правильные названия колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта. Подробная информация приведена в п. 2.2.3 и 2.3.3
54.	Ошибка валидации заголовка. Указаны не все колонки. Количество колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта. Подробная информация приведена в п. 2.2.3 и 2.3.3
55.	Ошибка валидации заголовка. Неправильный порядок колонок. Правильный порядок колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта. Подробная информация приведена в п. 2.2.3 и 2.3.3
56.	Ошибка при разборе файла. Убедитесь, что выбран нужный файл	Необходимо проверить корректность выбранного CSV-файла для импорта. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
58.	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Необходимо проверить корректность заполненных данных в CSV-файле. Подробная информация приведена в п. 2.2.3 и 2.3.3
59.	WLAN MAC устройства (WLAN_MAC). Ошибка валидации значения. Рекомендуем проверить указанное значение на соответствие WLAN MAC	Необходимо проверить корректность заполненных данных в CSV-файле, в частности WLAN_MAC. Подробная информация приведена в п. 2.2.3 и 2.3.3

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
	устройства	
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
61.	Комментарий (COMMENT). Ошибка валидации значения. Длина должна быть до 512 символов	Необходимо проверить корректность заполненных данных в CSV-файле, в частности COMMENT. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в п. 2.2.3
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. Подробная информация приведена в п. 2.2.3
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в п. 2.3.3

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
67.	Отчество (PATRONYMIC). Ошибка валидации значения. Отчество может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, PATRONYMIC. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
69.	Должность (JOB_TITLE). Ошибка валидации значения. Должность может содержать: а-я ё a-z A-Я Ё A-Z - пробел	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, JOB_TITLE. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
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. Подробная информация приведена в п. 2.3.3
79.	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Необходимо проверить корректность заполненных данных в CSV-файле, в частности, IMEI. Подробная информация приведена в п. 2.3.3
80.	Ошибка импорта. Файл содержит только заголовок. Файл должен быть заполнен данными	Необходимо проверить корректность заполненных данных в CSV-файле. Подробная информация приведена в п. 2.2.3 и 2.3.3
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. Подробная информация приведена в п. 2.3.3

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
82.	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Необходимо проверить корректность заполненных данных в CSV-файле. Подробная информация приведена в п. 2.2.3 и 2.3.3

5.2. Ограничения

В ходе работы с ПУ выделяют следующие ограничения, приведенные в таблице (Таблица 37).

Таблица 37

№ 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	– **Вариант1**. Необходимо закончить повторную активацию устройства, отсканировав QR-код. В результате устройство подключится к ПУ и будет получать операции с новым токеном;

№ п/п	Ограничение	Решение
		– 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
6.	Возможна рассинхронизация времени сервера и клиентского 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, оффлайн-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 клиентским приложением «Аврора Центр» было активировано в тенанте, созданном из дефолтного, а затем очищено, то для его повторной активации в тенанте необходимо обновить клиентское 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 клиентского приложения «Аврора Центр» (с помощью `omp-ocs-updater`); 3. После установки обновления клиентского 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», 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.	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
13.	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 указанным в сертификате	Необходимо учитывать это ограничение при назначении политик на устройствах

14.	После переактивации устройства на другом сервере могут не устанавливаться приложения	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>`

15.	Через 5 секунд после получения команды на очистку осуществляется отправка обновленного состояния устройства и его сброс к заводским	Необходимо учитывать данную особенность при отправке операции по очистке устройства. Выполнение

№ п/п	Ограничение	Решение
	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	операции будет усовершенствовано в следующих версия ППО
16.	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
17.	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
18.	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

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 38).

Таблица 38

Термин/ Сокращение	Расшифровка
Клиентское приложение	Клиентским приложением является мобильное приложение, функционирующее под управлением ОС Аврора.
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»
ПУ	Подсистема Платформа управления
СУА	Сервис уведомлений Аврора
Устройство	Под устройством подразумевается МУ, на которой функционируют соответствующие компоненты ППО
Чекбокс	Элемент управления, предоставляющий возможность осуществить выбор, а также вызвать список быстрых действий
ЭВМ	Электронно-вычислительная машина
CSV	Comma-Separated Values — текстовый формат, предназначенный для представления табличных данных
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

Термин/ Сокращение	Расшифровка
IMEI	Уникальный номер мобильного устройства, состоящий из 15 цифр
Fingerprint	Цифровой отпечаток (информация, собранная об удаленном устройстве для дальнейшей идентификации)
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 компьютеру
Push-уведомления	Текстовые сообщения, предназначенные для оперативной (мгновенной) доставки на устройство пользователей
QR-код	Quick response code – код быстрого реагирования, матричный код (двумерный штрихкод)
WLAN	Wireless Local Area Network — локальная сеть, построенная на основе беспроводных технологий

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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