



Руководство администратора

Ред. 1.0

Всего листов: 121

Аннотация

Данное руководство является частью эксплуатационной документации для программного продукта «МИРАМОБАЙЛ».

Содержание

Аннотация.....	2
1. Введение.....	7
1.1. Термины и сокращения.....	7
2. Общие сведения о системе	9
2.1. Назначение системы.....	9
2.2. Условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средства автоматизации в соответствии с назначением	9
2.3. Основные функции и возможности.....	10
2.4. Состав Портала.....	11
2.5. Роли администратора	12
3. Документация.....	13
4. Описание работы.....	14
4.1. Основные этапы работы	14
4.1.1. Настройка и мониторинг.....	14
4.1.2. Клиентская часть.....	14
4.2. Возможности администраторов	14
4.3. Защита информации	14
4.4. Лицензирование	15
4.5. Эксплуатация веб - портала	15
5. Назначение и условия применения.....	16
5.1. Стартовое окно.....	16
5.2. Возможные ошибки при входе	17
5.3. Первоначальная настройка	18
5.4. Выход администратора.....	19
5.5. Панель навигации	19
6. Раздел Устройства	22
6.1. Окно просмотра списка устройств	22
6.2. Поиск устройств.....	23
6.3. Перемещение устройства или группы устройств в другую группу.....	27
6.4. Команды управления работой устройства	27
6.4.1. Блокировка устройства.....	29
6.4.2. Затереть все данные.....	30
6.4.3. Смена пароля.....	31
6.4.4. Отправка сообщения.....	32
6.4.5. Обновление клиента	33
6.4.6. Запрос информации об устройстве.....	34
6.4.7. Запрос журнала безопасности	35
6.5. Применение шаблона политики к устройству или группе устройств.....	36
6.6. Экспорт списка устройств	37
6.7. Просмотр подробной информации об устройстве	39
6.7.1. Информация об устройстве или группе устройств.....	39
6.7.2. Об устройстве	40
6.7.3. SIM.....	43
6.7.4. Правила безопасности	43
6.7.5. Приложения.....	44
6.7.6. WI-FI	45
6.7.7. События.....	46
6.7.8. Координаты	49
6.8. Создание приглашения на добавление нового устройства	49
6.9. Создание группы и добавление в нее устройств	51
6.10. Редактирование правила политик безопасности на выбранном устройстве или группе устройств.....	53
6.11. Удаление устройства или групп устройств	56
6.12. Изменение списка администраторов групп у выбранной группы.....	58
6.12.1. Назначение администратора	58
6.12.2. Удаление администратора.....	60
7. Раздел Шаблоны политик	61
7.1. Главное окно раздела	61
7.2. Создание нового шаблона	62

7.3.	Создание шаблона через копирование существующего	63
7.4.	Редактирование шаблона политики	64
7.5.	Удаление шаблона политики	65
8.	Раздел Приложения.....	67
8.1.	Главное окно раздела	67
8.2.	Добавление стороннего приложения в каталог через APK файл	67
8.3.	Добавление приложения в каталог из магазина приложений	68
8.4.	Удаление приложения из каталога	69
8.5.	Поиск приложения	69
9.	Раздел Роли и права	70
9.1.	Главное окно раздела	70
9.2.	Описание ролей	71
9.3.	Редактирование прав выбранной роли	72
10.	Раздел Пользователи	73
10.1.	Главное окно раздела	74
10.2.	Просмотр списка пользователей	74
10.3.	Фильтрация списка пользователей	75
10.4.	Добавление нового пользователя	76
10.5.	Импорт новых пользователей	78
10.6.	Изменение атрибутов пользователя	79
10.7.	Удаление пользователя	80
11.	Раздел Регистрации	82
11.1.	Окно главной страницы раздела	82
11.2.	Создание приглашения на регистрацию устройства	83
11.3.	Аннулирование приглашения на регистрацию устройства	84
12.	Раздел Настройки.....	86
12.1.	Загрузка лицензии	87
12.2.	Просмотр истории лицензий для mdm - сервера	88
12.3.	Вкладка О программе	90
12.4.	Пароли сервисного режима	91
12.4.1.	Поиск пароля сервисного режима	92
12.4.2.	Удаление пароля сервисного режима	93
12.5.	Вкладка syslog - сервера	94
12.5.1.	Добавление syslog-сервера	94
12.5.2.	Удаление syslog-сервера	95
13.	Раздел Журнал	97
13.1.	Главная страница раздела Журналы	97
13.2.	Поиск события из общего списка	101
13.3.	Выгрузка журнала сервера	101
13.4.	Удаление записей событий из журнала	102
14.	Аварийные ситуации	104
Приложения.....	105	
Приложение 1: Список правил	105	
Белый список Wi-Fi точек	105	
Блокировка при смене SIM	105	
Все разрешения приложениям	105	
Возможность удаления приложений	106	
Встроенный браузер	106	
Журнал событий	106	
Запрет скриншотов	106	
Зашифровать устройство	107	
Использование Bluetooth	107	
Использование NFC	107	
Использование SMS	107	
Использование VPN	107	
Использование Wi-Fi	107	
Использование звукозаписи	108	
Использование камеры	108	
Межпрофильный буфер обмена	108	
Мобильная точка доступа	109	
Мобильные данные	109	

Настройка Proxy	109
Настройка Wi-Fi точек.....	110
Настройка почты Exchange.....	111
Осуществление звонков	112
Отладка по USB.....	112
Пароль и блокировка.....	113
Передача данных по USB.....	114
Право установки приложений.....	114
Сброс настроек.....	115
Системные приложения	116
Сотовые станции	116
Установить / удалить приложения.....	116
Хранилище данных.....	118
Частота обмена данными.....	119
Черный список приложений.....	119

История изменений

№ п/п	Дата изменения	Версия	Описание изменений	Номер релиза

1. Введение

Руководство предназначено для администраторов изделия «Программный комплекс МИРАМОБАЙЛ» (далее — комплекс). В нем содержатся сведения, необходимые для эксплуатации комплекса.

1.1. Термины и сокращения

Термины и определения приведены в таблице 1 настоящего раздела документа.

Таблица 1 – Термины и определения

Термин	Определение
«Администратор»	Пользователь системы, который может пройти аутентификацию на портале
«Администратор группы»	Пользователь с ограниченными правами администратора, который управляет устройствами и пользователями в пределах своей группы или подразделения
«Аудитор»	Пользователь системы с правами только на просмотр информации, без возможности внесения любых изменений
«Главный администратор»	Администратор системы с максимальными правами в системе. Рекомендуются использовать только для первоначальной настройки системы, назначения администраторов группы на разделы
Компания	ООО «СолидСолюшенс», владелец продукта
Поддерживаемое устройство	Устройство, на котором установлен клиент управления MDM, на которое можно назначать правила из шаблона политики и отправлять команды

Термин	Определение
Правило	Отдельное правило для выполнения определённых действий на устройстве или использования функции устройства. Может иметь настройки
Роль	Уровень прав доступа, например «Без роли» или «Администратор группы»
Устройство	Телефон или другое устройство, зарегистрированное в конкретном продукте
Шаблон политики безопасности	Набор правил с конкретными настройками, объединённый в группу, реализующую политику безопасности организации
Mobile device manager (MDM)	Система управления мобильными устройствами, обеспечивающая централизованный контроль, настройку, безопасность и мониторинг устройств организации
Корпоративное устройство (COBO)	Условное название режима управления устройством, характеризующееся определённым набором возможностей и ограничений. В этом режиме устройство управляется с приоритетом корпоративных настроек и политик, при этом личное использование ограничено или исключен
Личное устройство (BYOD)	Условное название режима управления, при котором на персональном устройстве пользователя создаётся отдельный рабочий профиль. Этот режим обеспечивает разделение рабочих и личных данных и настроек, позволяя использовать устройство как для рабочих, так и для личных задач

2. Общие сведения о системе

2.1. Назначение системы

Портал предназначен для централизованного удалённого управления мобильными устройствами в организации. Портал обеспечивает контроль, настройку и защиту мобильных устройств сотрудников, предоставляя два условных режима управления — «Личное» и «Корпоративное». Выбор режима и правила использования устройств определяются организацией в соответствии с её внутренними политиками.

Основные возможности:

- управление политиками безопасности, такими как требования к паролям, шифрование данных, блокировка устройств;
- контроль доступа к корпоративным ресурсам и приложениям;
- мониторинг состояния устройств и анализ использования;
- возможность очистки данных в случае утери или кражи устройства.

Портал реализован на базе сервера управления. Управление системой осуществляется через веб-интерфейс административной консоли Портала (далее — Портал), предоставляющей удобный доступ к настройкам и мониторингу.

2.2. Условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средства автоматизации в соответствии с назначением

Использование Системы Администратором возможно при соблюдении следующих условий:

1. Наличие доступа к Порталу.
2. Использование поддерживаемых производителями версий веб-браузеров:

- Chrome,
- Firefox,
- Safari,
- Edge.

2.3. Основные функции и возможности

Портал обеспечивает базовый набор функций, направленных на эффективное управление мобильными устройствами и пользователями в корпоративной среде. К основным возможностям относятся:

- управление устройствами:
 - создание, группировка, перемещение, удаление устройств и групп устройств;
 - отправка команд на устройства; применение шаблонов политик безопасности;
 - просмотр подробной информации, логов и истории геолокации устройств
- управление политиками безопасности:
 - создание новых шаблонов политик, копирование, редактирование, удаление; настройка правил и разрешение конфликтов правил на устройствах и группах
- управление приложениями:
 - добавление приложений в каталог через арк-файлы или по названию пакета;
 - удаление приложений; поддержка интеграции с различными магазинами приложений
- регистрация устройств:
 - создание и управление приглашениями на регистрацию устройств;
 - поддержка корпоративного (COBO) и личного (BYOD) использования;

- контроль статусов приглашений
- управление пользователями:
 - добавление новых пользователей, массовый импорт пользователей из *.csv-файлов;
 - изменение атрибутов пользователей;
 - удаление пользователей; управление ролями и правами доступа
- настройка прав и ролей:
 - редактирование прав для предустановленных ролей, включая главного администратора группы
- настройки системы:
 - загрузка лицензий; просмотр истории лицензий;
 - настройка параметров скачивания MDM-агента;
 - настройка отправки сообщений на сервер Syslog;
 - поиск пароля сервисного режима для устройств
- журналы и аудит:
 - просмотр, фильтрация, выгрузка и удаление записей журнала сервера;
 - контроль действий администраторов и пользователей; обеспечение прозрачности и безопасности работы системы
- интеграция и дополнительная функциональность:
 - отправка данных в систему дашборда;
 - поддержка мобильного клиента Android;
 - возможности интеграции с внешними системами мониторинга и управления.

2.4. Состав Портала

Портал состоит из следующих отдельно устанавливаемых программных средств:

- сервер MDM (далее — сервер);

- клиент управления (далее — клиент) — устанавливается на мобильном устройстве пользователя.

Клиент используется совместно с сервером.

Сервер является основным элементом в структуре системы. Этот компонент обеспечивает взаимодействие объектов управления, реализует функции контроля и управления работой устройств, а также осуществляет обработку, хранение и передачу информации.

Управление порталом осуществляется с помощью веб-интерфейса — консоли администратора для настройки, мониторинга и управления системой через браузер. Не требует отдельной установки, доступна через сервер.

2.5. Роли администратора

Управление порталом осуществляют сотрудники организации, обладающие правами администратора. От назначенной роли зависит уровень доступа администратора к разделам и функциям системы.

Существуют три роли администратора (привилегированного пользователя):

- «Главный администратор»;
- «Администратор»;
- «Аудитор».

Более подробную информацию о ролях администраторов и их правах смотрите в разделе [Роли и права](#).

3. Документация

«МИРАМОБАЙЛ». Руководство администратора» — описание системы «МИРАМОБАЙЛ».

«МИРАМОБАЙЛ». Руководство по установке» — описание Инструкции по установке и настройке компонентов «МИРАМОБАЙЛ».

4. Описание работы

4.1. Основные этапы работы

Настройка и мониторинг

Через консоль администратора осуществляется настройка и мониторинг всех разделов системы.

Сервер MDM обрабатывает данные, управляет устройствами и обеспечивает взаимодействие с клиентскими приложениями, установленными на мобильных устройствах пользователей.

Клиентская часть

Клиентская часть, установленная на устройствах, выполняет команды сервера, применяет политики безопасности и передает информацию о состоянии устройства.

4.2. Возможности администраторов

Администраторы могут выполнять широкий спектр задач в зависимости от уровня доступа, предоставленного их ролью:

- управление устройствами (группировка, применение политик, отправка команд, просмотр свойств и состояния устройств);
- настройка правил согласно шаблонам политики безопасности в компании (шифрование, требования к паролям, блокировка);
- управление приложениями (добавление через арк или магазины приложений), регистрацию устройств.

Система также поддерживает мониторинг, аудит действий и интеграцию с внешними системами для дополнительной функциональности.

4.3. Защита информации

В случае утери или кражи устройства комплекс позволяет удаленно очистить данные, обеспечивая защиту корпоративной информации. Все

действия фиксируются в журналах сервера, что гарантирует прозрачность и возможность анализа активности.

Таким образом, портал предоставляет организациям гибкий инструмент для управления мобильными устройствами, обеспечивая баланс между безопасностью, удобством и эффективностью работы сотрудников.

4.4. Лицензирование

Лицензия предоставляется потребителю в момент приобретения права на использование портала «МИРАМОБАЙЛ» или предоставления временного права на ознакомление с его возможностями. Использование комплекса регулируется рядом лицензионных ограничений. Лицензируются следующие параметры:

- количество мобильных устройств, зарегистрированных на сервере.

Ограничения на использование портала «МИРАМОБАЙЛ» определяются приобретёнными лицензиями.

4.5. Эксплуатация веб - портала

Для работы администратору необходимо иметь логин и пароль доступа к консоли управления.

5. Назначение и условия применения

Первоначальная настройка портала предназначена для конфигурации системы после развёртывания, обеспечивая безопасный доступ и управление. После развёртывания комплекса будет создан пользователь с ролью «Главный администратор» с логином и паролем. Учётные данные используются для старта процесса, но их следует изменить для повышения безопасности.

Условия применения:

- доступ к portalу через поддерживаемый веб-браузер;
- наличие прав для выполнения действий, как указано в разделе [Роли и права](#).

5.1. Стартовое окно

Стартовое окно отображается без аутентификации и служит для входа в систему.

Окно содержит следующие поля:

- для ввода логина и пароля;
- сообщения о статусе (например, приглашение ко входу).

Для входа в систему выполните следующие действия:

1. Откройте портал в веб-браузере.
2. В адресную строку веб-браузера введите адрес Портала и нажмите клавишу **Enter**. Откроется страница ввода логина и пароля (см. рисунок 1).
3. Введите свой логин в поле Логин.
4. Введите пароль в поле Пароль.
5. Нажмите кнопку **Войти** или **Enter** для продолжения. После успешного входа появится основное окно консоли управления.

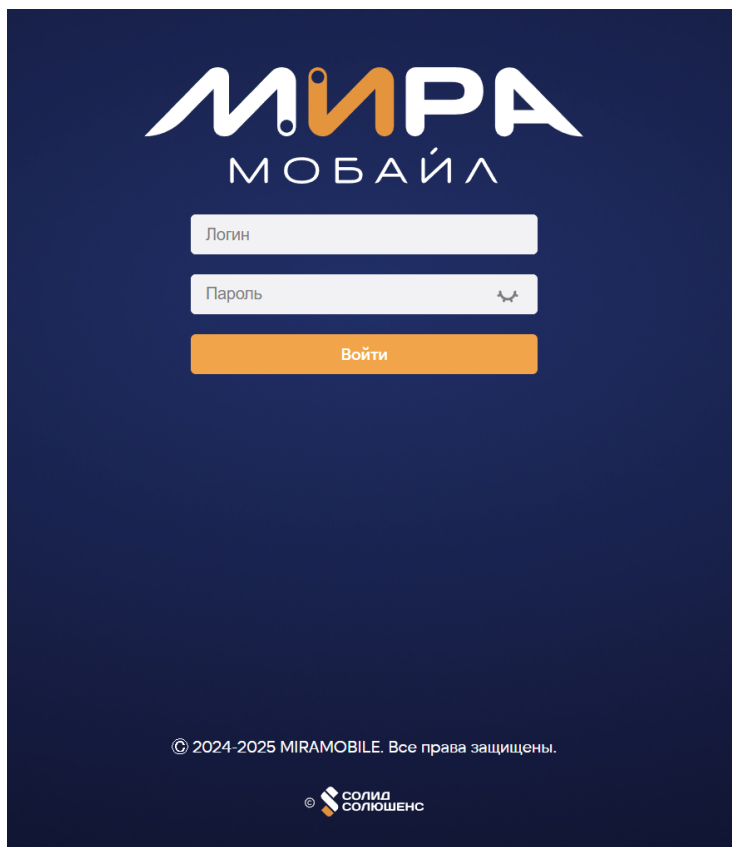


Рисунок 1 – Страница ввода логина и пароля

Примечание – Если окно не загружается, проверьте подключение к сети, так как это может указывать на технические проблемы.

5.2. Возможные ошибки при входе

Попытка входа администратора может быть неудачной, к чему приводит ряд событий, таких как неверный ввод данных, истечение сессии или отсутствие прав. При этом на экран выводятся сообщения, описывающие характер события для устранения проблемы.

Если пользователь ввёл неверный логин или пароль, система отобразит сообщение «Неверные данные», требуя повторного ввода (см. рисунок 2).

Если сессия истекла из-за длительного бездействия, появится предупреждение о необходимости повторной аутентификации.

Если отсутствуют права, система покажет «Доступ запрещен», с рекомендацией проверить роль.

Выполните следующие действия:

1. Откройте стартовое окно.

2. Введите логин и пароль.
3. Нажмите кнопку входа.



Рисунок 2 – Страница ошибки при вводе логина или пароля

5.3. Первоначальная настройка

После аутентификации выполните первоначальную настройку для полной конфигурации системы.

Выполните следующие действия:

1. Зарегистрируйтесь в роли «Главный администратор».
2. Измените логин и пароль в разделе **Пользователи**, чтобы использовать надежные учётные данные.
3. Создайте пользователей с ролями администратора и (или) администратора группы.
4. Добавьте обычных пользователей через [Импорт новых пользователей](#).
5. Добавьте устройства в систему путем отправки приглашений.

Примечание – Все действия требуют проверки прав доступа. Если права отсутствуют, система отобразит сообщение об ошибке.

При входе администратора по умолчанию открывается основное окно раздела **Устройства**.

5.4. Выход администратора

Выход доступен из любого окна и завершает сессию, обеспечивая безопасность после завершения работы.

Выполните следующие действия:

1. Найдите кнопку **Выйти из профиля** (см. рисунок 3).
2. Нажмите на кнопку для выхода.

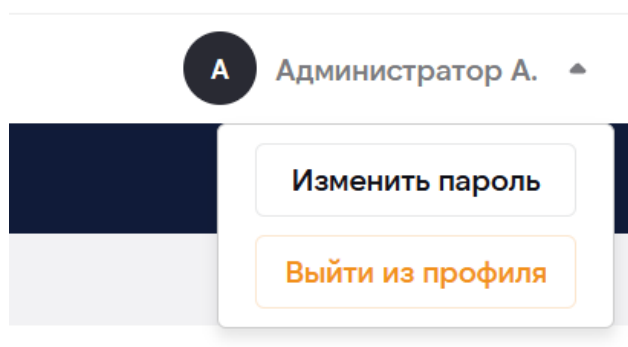


Рисунок 3 – Выход администратора

5.5. Панель навигации

В левой части главного окна расположена панель навигации, на которой отображается список разделов панели администратора. Для более компактного переключения внешнего вида панели навигации используется кнопка ✕, для обратного переключения ≡ (см. рисунок 4).

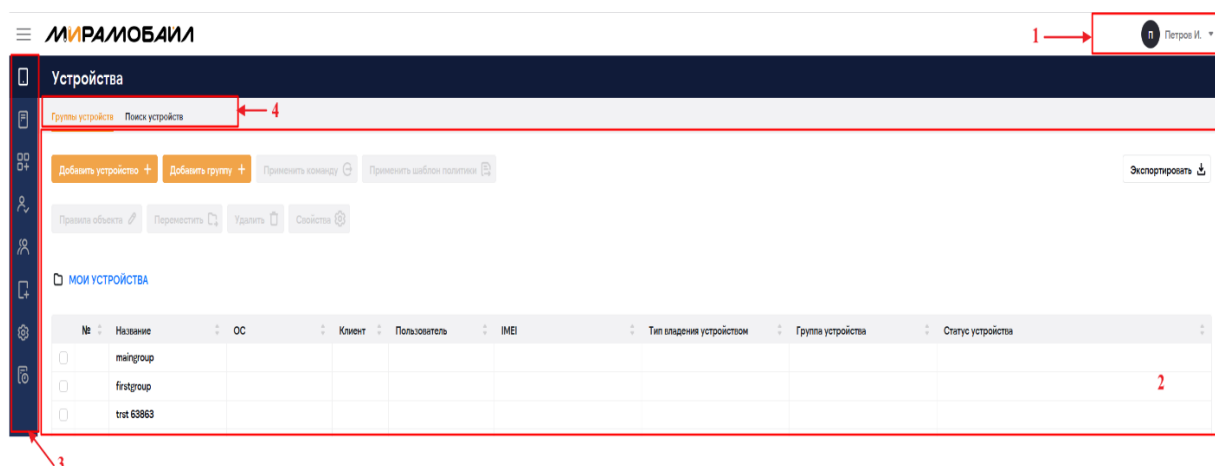


Рисунок 4 – Окно панели администратора

Обозначение позиций окна панели администратора и ее состав представлен в таблице 2.

Таблица 2 – Обозначение и состав панели администратора

	Обозначение	Описание
①	Меню для смены пароля и выхода из учётной записи	Обеспечивает доступ к функциям смены пароля и выхода из текущей учётной записи
②	Область отображения информации раздела	Основная область, где отображается содержимое выбранного раздела панели администратора
③	Панель навигации	Содержит список разделов и позволяет переключаться между ними
④	Панель инструментов	Содержит кнопки и элементы управления для выполнения операций в текущем разделе

В таблице 3 представлены разделы панели навигации и условное обозначение.

Таблица 3 – Разделы панели навигации

Значок	Название раздела	Описание
	Устройства	Раздел предназначен для управления работой мобильных устройств пользователей
	Шаблоны политик	Раздел предназначен для управления политиками безопасности
	Приложения	Раздел предназначен для управления приложениями, которые добавляются в политики для управления их работой на устройстве

Значок	Название раздела	Описание
	Роли и права	Раздел предназначен для просмотра доступных ролей привилегированных пользователей и редактирования прав администратора группы.
	Пользователи	Раздел предназначен для управления учетными записями пользователей
	Регистрация	Раздел предназначен для управления запросами на регистрацию устройства пользователя
	Настройки	Раздел предназначен для загрузки лицензий, просмотра версий компонентов системы и паролей сервисного режима
	Журнал	Раздел предназначен для просмотра и экспорта событий, регистрируемых комплексом

6. Раздел Устройства

Раздел предназначен для централизованного управления и мониторинга устройств, зарегистрированных в системе. Он позволяет пользователям с различными ролями эффективно работать с устройствами и группами устройств в рамках своих полномочий.

Примечание – Все действия в разделе выполняются пользователями с одной из следующих ролей:

- «Главный администратор» — имеет полный доступ и может выполнять все действия;
- «Администратор группы» — может выполнять все действия в пределах назначенных ему групп устройств;
- «Аудитор» — имеет доступ только для просмотра информации, изменения недоступны.

6.1. Окно просмотра списка устройств

Раздел **Устройства** имеет следующий вид (см. рисунок 4).

Информация об устройствах и их дочерних группах представлена в виде таблицы со следующими столбцами:

- **№ п/п** – порядковый номер устройства;
- **Название** – название устройства или группы устройств;
- **ОС** – операционная система устройства;
- **Клиент** – версия клиента на устройстве;
- **Пользователь** – на кого зарегистрировано устройство;
- **IMEI** – IMEI устройства (не отображается для личных устройств);
- **Тип владения устройством** – категория владения устройством;
- **Группа устройства** – название группы, к которой относится устройство;
- **Статус устройства** – текущее состояние устройства в системе.

Список возможностей:

- Просмотр списка устройств;
- Добавление устройства (через приглашение);
- Добавление группы устройств;
- Удаление выделенных устройств или группы;
- Перемещение устройства или группы;
- Применение шаблона политики;
- Отправка команды.
- Экспорт списка устройств;
- Переход к поиску устройств.

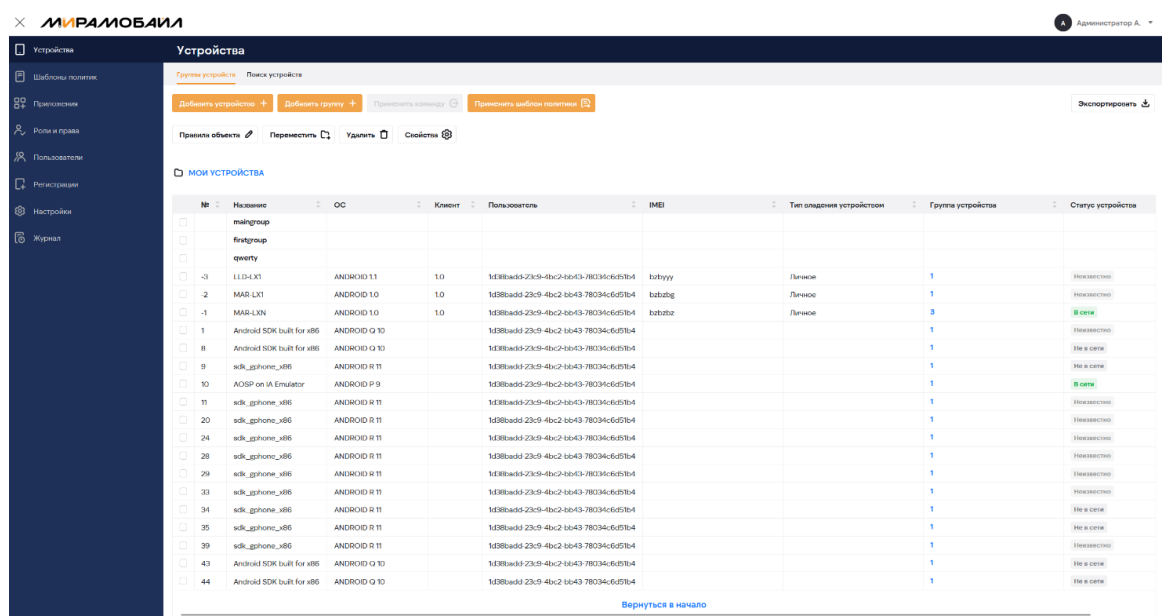


Рисунок 5 – Главное окно раздела Устройства

6.2. Поиск устройств

Для нахождения нужного устройства из общего списка выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Переключитесь на вкладку **Поиск устройств** (см. рисунок 5).

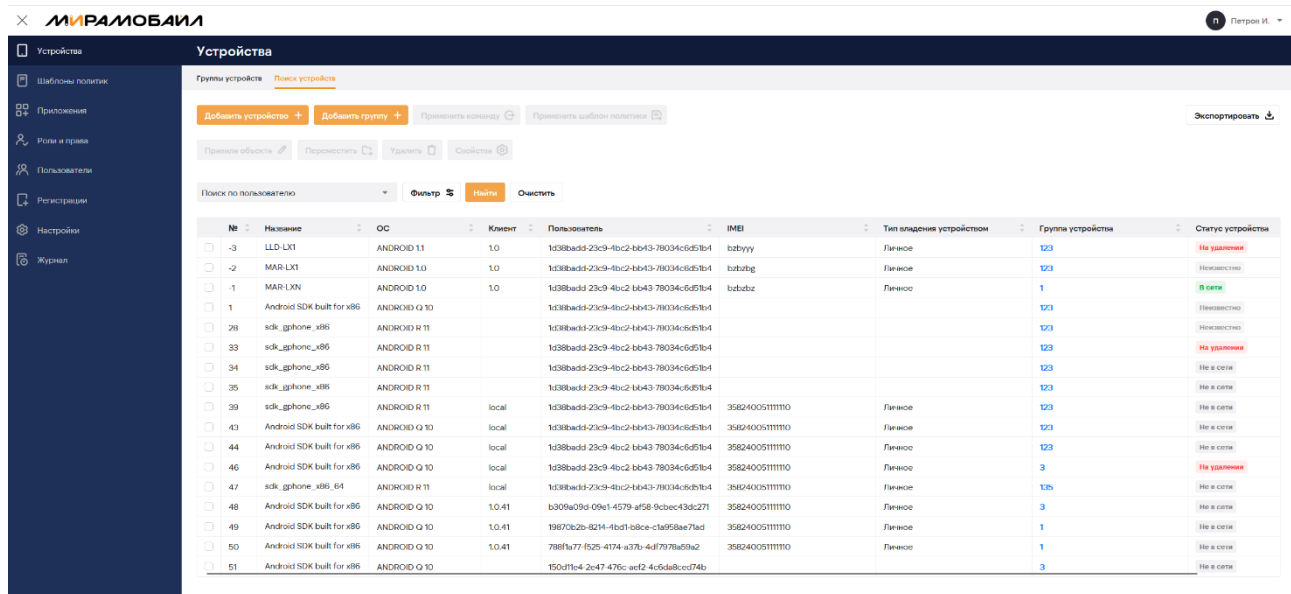


Рисунок 6 – Окно поиска устройств

- Нажмите кнопку **Фильтр**. Откроется форма поиска (см. рисунок 6).
- Выберите/заполните необходимые критерии (см. в таблице 2) и нажмите кнопку **Найти**. На экране появится список устройств, соответствующих выбранным критериям (см. рисунок 7).

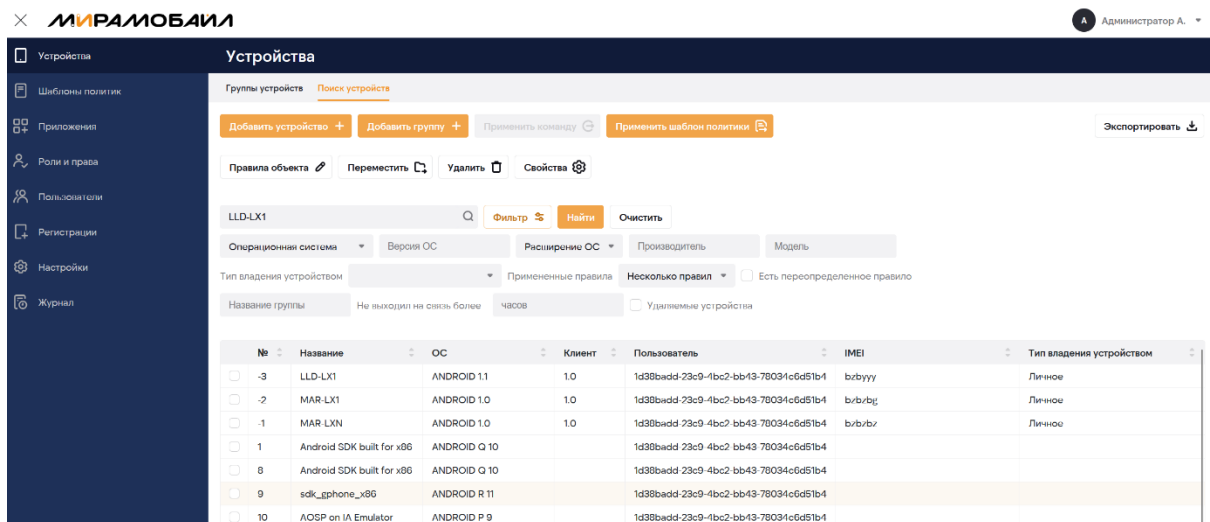


Рисунок 7 – Критерии фильтра по поиску устройств

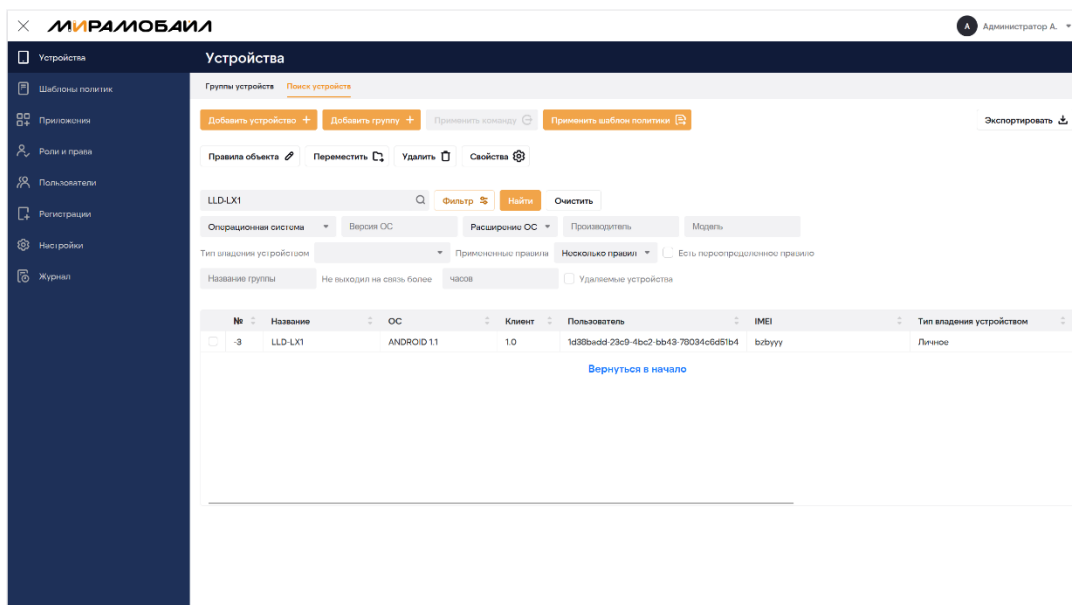


Рисунок 8 – Список найденных устройств

5. Для очистки формы поиска используйте кнопку **Очистить**.
6. Для возврата в раздел **Устройства** нажмите вкладку **Группы устройств**.

Таблица 4 – Критерии поиска устройств

Наименование критерия	Описание влияния на поиск
Операционная система	Фильтрует по ОС (например, Android), ограничивая список совместимыми устройствами
Версия ОС	Позволяет указать конкретную версию операционной системы
Расширение ОС	Уточняет поиск по установленным расширениям операционной системы, например «KNOX»
Производитель	Фильтрует устройства по производителю
Модель	Позволяет указать конкретную модель устройства

Наименование критерия	Описание влияния на поиск
Тип владения устройством	Отображает устройства в зависимости от типа владения («Личное», «Корпоративное»)
Применённые правила	Показывает устройства, к которым применены определённые правила
Название группы	Фильтрует устройства по принадлежности к определённой группе
Не выходил на связь более (в часах)	Отображает устройства, которые не выходили на связь в течение указанного времени
Удаляемые устройства	При выборе отображаются только устройства с активной командой удаления

Примечания:

Фильтрация по правилам

Можно выбрать одно или несколько правил. В этом случае будут показаны устройства, к которым применены все выбранные правила.

Если не выбрано ни одно правило, отображаются все устройства.

Поиск устройств без применённых правил

Чтобы найти устройства, к которым не применено ни одно правило, используйте опцию «На устройстве нет применённых правил».

Переопределённые правила

Если выбран признак «Только те, к которым применено переопределение правил», отображаются только устройства с переопределёнными правилами.

Особенности совместного выбора фильтров

Если одновременно выбраны опция «На устройстве нет применённых правил» и признак переопределения, список устройств будет пустым.

6.3. Перемещение устройства или группы устройств в другую группу

Чтобы переместить устройство или группу устройств в другую группу и обновить связанные правила, выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите устройство или группу в окне списка (см. рисунок 8).
3. Нажмите кнопку .
4. Выберите целевую группу из доступного списка.
5. В правом нижнем углу нажмите кнопку **Создать**. Устройство будет перенесено в выбранную группу.

Примечания:

1. После перемещения к устройствам применяются правила новой группы.
2. Действие переопределённых правил сохраняется.
3. Система автоматически применяет активный набор правил к целевой группе для сохранения целостности настроек.

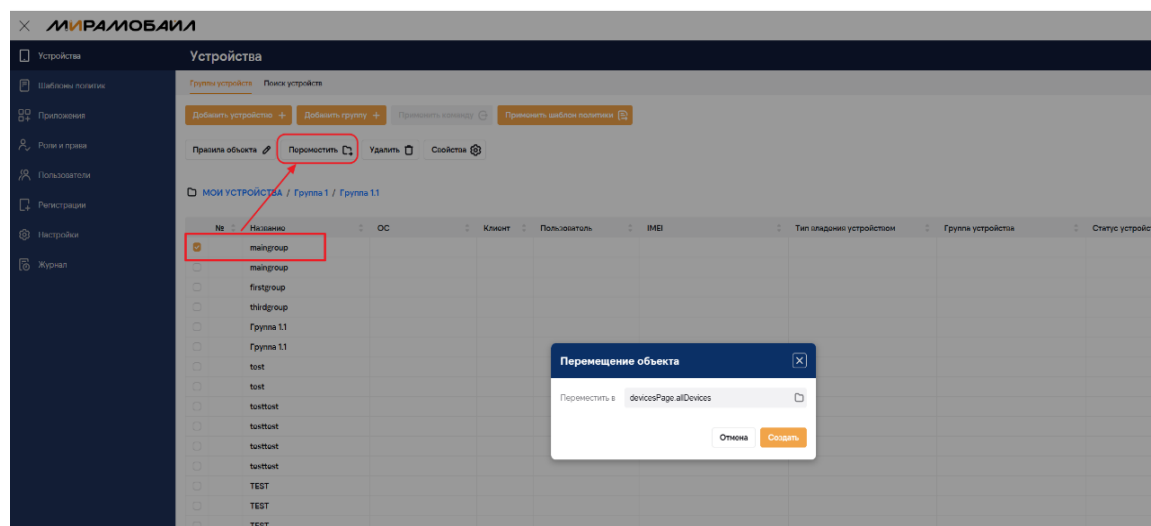


Рисунок 9 – Перемещение устройств

6.4. Команды управления работой устройства

Примечание – Подробное описание списка команд представлен в таблице 5 и рисунке 9.

Таблица 5 – Список команд на устройства

Команда	Параметры	Влияние
Блокировать устройство	Выбор устройств	Устройство переходит в заблокированное состояние, ограничивая доступ пользователя до разблокировки
Затереть все данные	clearInternalStorage (стереть внутреннее хранилище); clearExternalStorage (стереть внешнее хранилище)	При clearInternalStorage == true — очистка клиентского приложения (сброс до заводских настроек в корпоративном режиме). При clearExternalStorage == true — дополнительно очищается внешнее хранилище. При clearInternalStorage == false — в KNOX_CONTAINER очищается только контейнер, иначе команда игнорируется
Сменить пароль	Новый пароль; установка одноразового пароля (да/нет)	При установке одноразового пароля после ввода верного пароля пользователю будет предложено ввести новый пароль
Отправить сообщение	Тема сообщения; текст сообщения; тип сообщения (Информация, Предупреждение, Ошибка)	Сообщение отображается в виде push-уведомления и сохраняется в журнале на устройстве
Обновить клиент	Подтверждение или отмена запроса	Запускает процесс обновления MDM-клиента на устройстве
Запрос информации об устройстве	Подтверждение или отмена запроса	Запрашивает актуальную информацию о состоянии устройства
Запрос журнала безопасности	Подтверждение или отмена запроса	Запрашивает журнал безопасности устройства для анализа событий и инцидентов

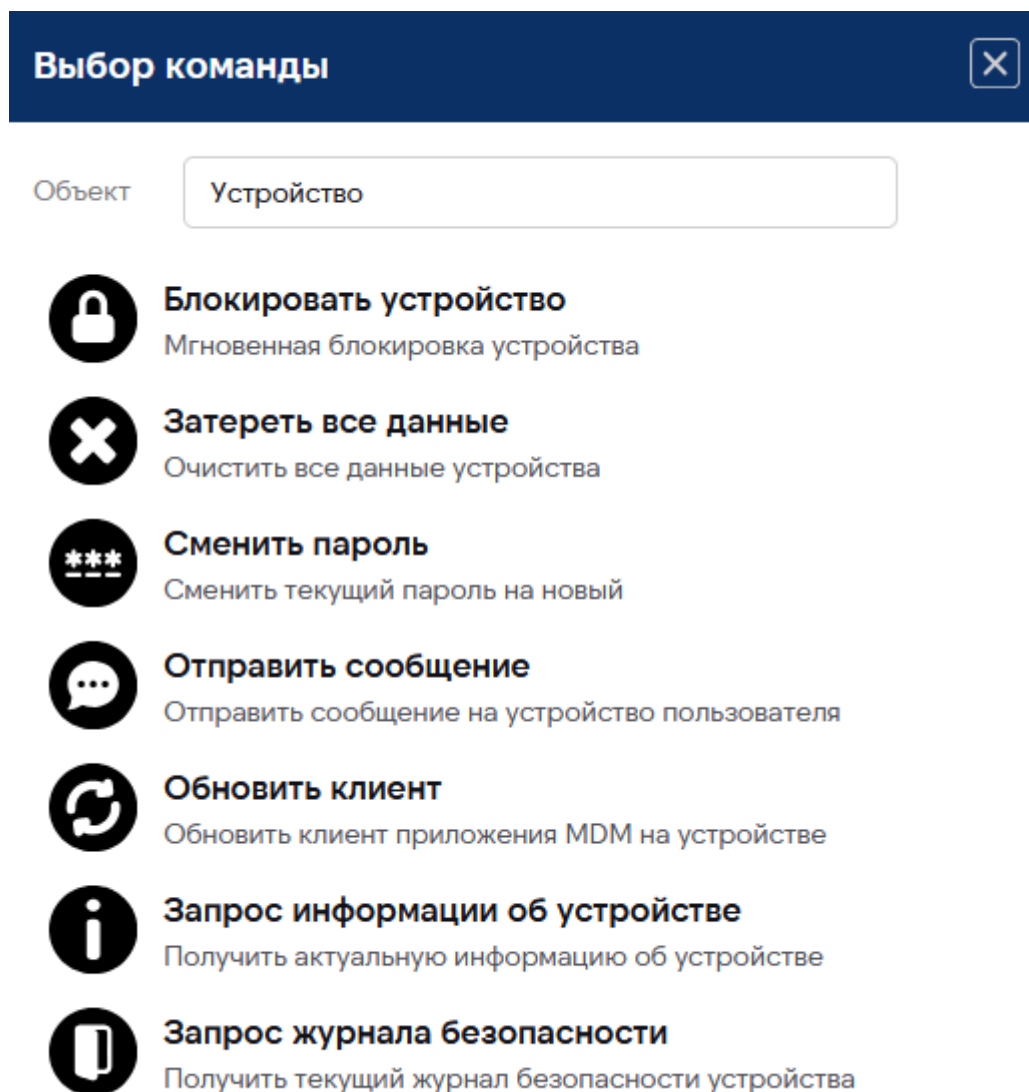


Рисунок 10 – Список команд управления

Блокировка устройства

Чтобы выполнить блокировку устройства выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите нужную команду, нажав на её название один раз. Появится сообщение об отправке команды.
5. Нажмите кнопку **Выполнить** для завершения процесса (см. рисунок 10). Появится сообщение. Для отмены действия нажмите кнопку **Отмена**.

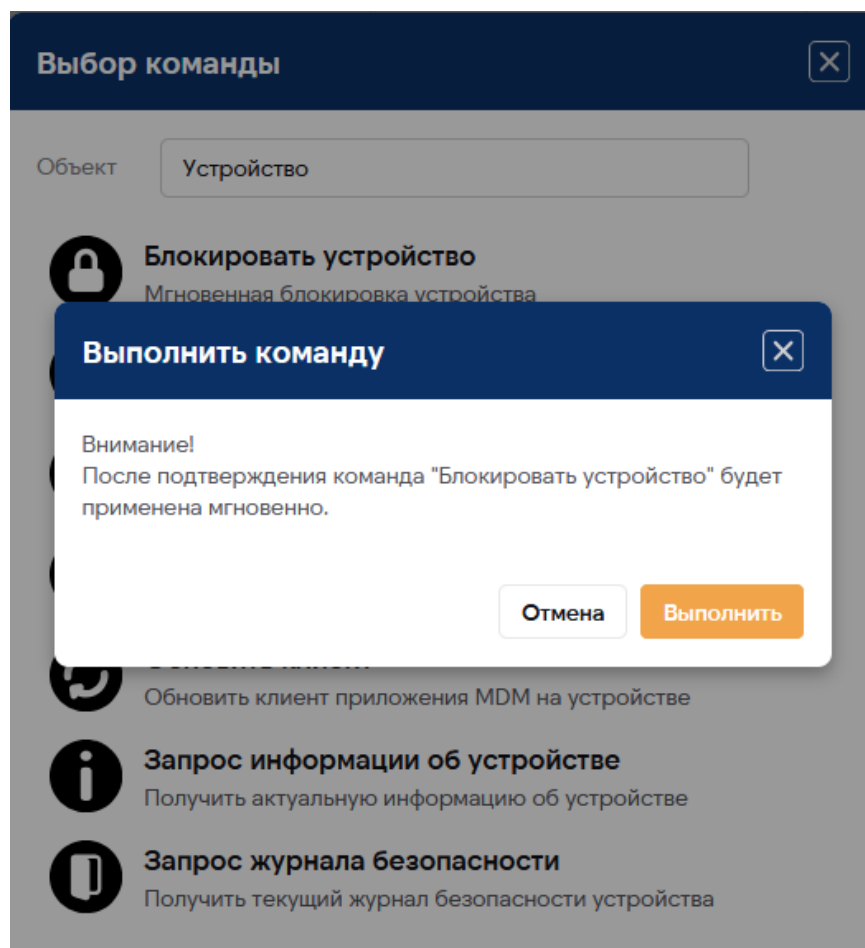


Рисунок 11 – Сообщение о блокировании устройства

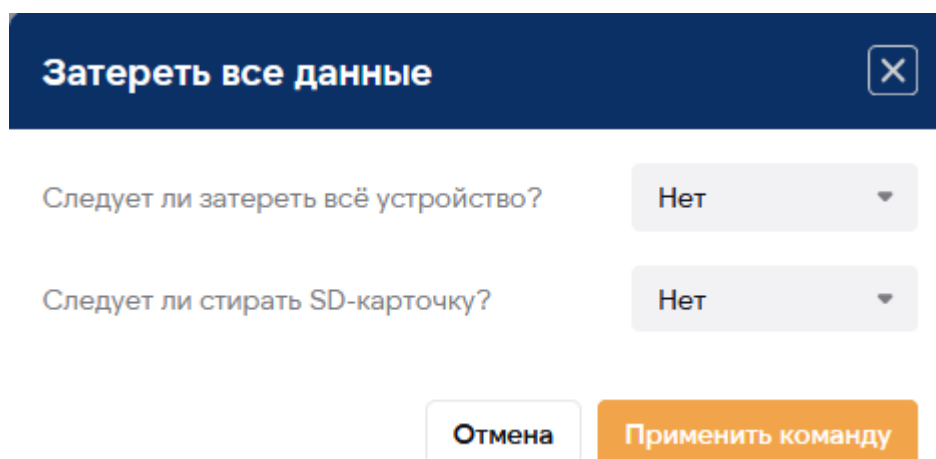
Затереть все данные

Команда «Затереть все данные» удалит клиентское приложение и, в зависимости от настроек и наличия/отсутствия KNOX контейнера, удалит внешние данные и KNOX контейнер.

Чтобы затереть все данные выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Затереть все данные** и нажмите на нее. На экране появится модальное окно.
5. Ответьте на вопросы (см. рисунок 11).

6. Нажмите кнопку **Применить команду** для завершения процесса. Для отмены действия нажмите кнопку **Отмена**.



Затереть все данные [X]

Следует ли затереть всё устройство? Нет ▾

Следует ли стирать SD-карточку? Нет ▾

Отмена Применить команду

Рисунок 12 – Запрос затереть данные

Смена пароля

Чтобы сменить пароль выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Сменить пароль** и нажмите на нее. На экране появится модальное окно.
5. Ответьте на вопросы.
6. Нажмите кнопку **Применить команду** для завершения процесса (см. рисунок 13). Для отмены действия нажмите кнопку **Отмена**.

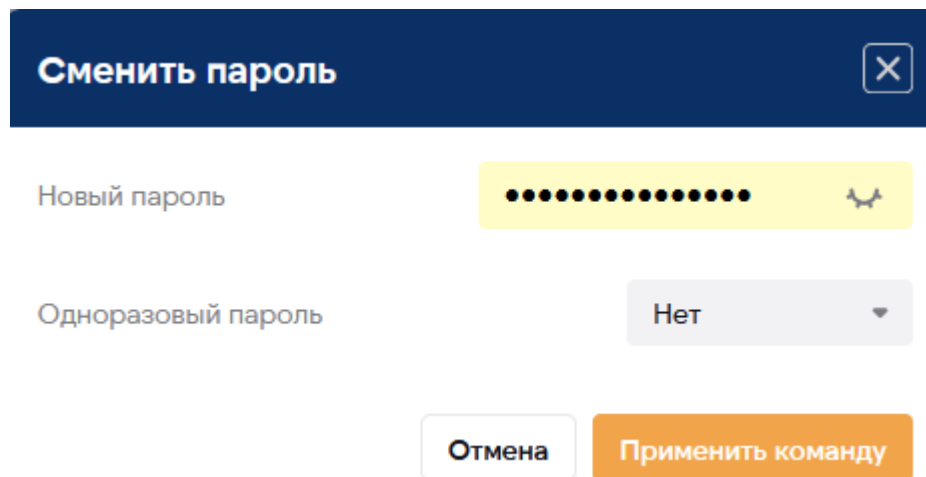
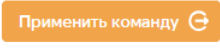


Рисунок 13 – Запрос на смену пароля

Отправка сообщения

Чтобы отправить сообщение выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Отправить сообщение** и нажмите на нее. На экране появится модальное окно.
5. В соответствующих полях выберите/введите:
 - Тип сообщения;
 - Заголовок;
 - Текст.
6. Нажмите кнопку **Применить команду** для завершения процесса (см. рисунок 13). Для отмены действия нажмите кнопку **Отмена**.

Отправить административное сообщение

Тип сообщения: Информация

Заголовок

Введите текст сообщения

Информация

Предупреждение

Ошибка

Отмена Применить команду

Рисунок 14 – Запрос на отправки сообщения

Обновление клиента

Чтобы обновить клиент выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Обновить клиент** и нажмите на нее. На экране появится модальное окно.
5. Нажмите кнопку **Выполнить** для завершения процесса (см. рисунок 13). Появится сообщение. Для отмены действия нажмите кнопку **Отмена**.

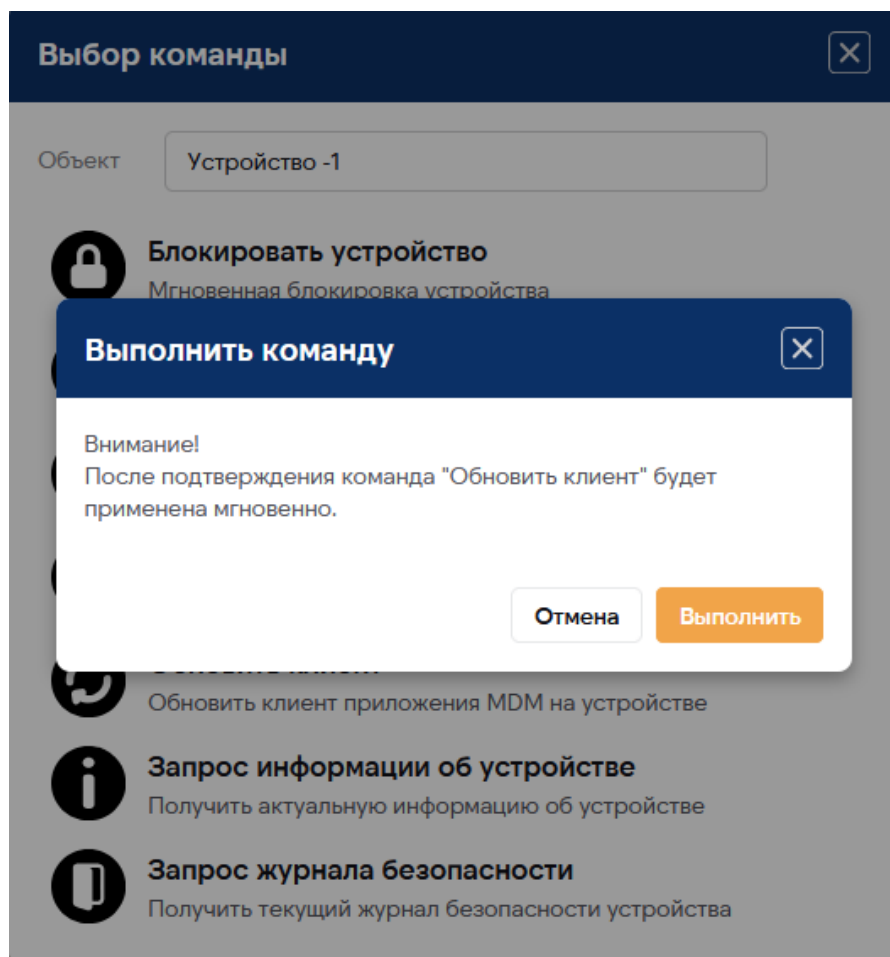


Рисунок 15 – Запрос на обновление клиента

Запрос информации об устройстве

Чтобы запросить информацию об устройстве выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Запрос информации об устройстве** и нажмите на нее. На экране появится модальное окно.
5. Нажмите кнопку **Выполнить** для завершения процесса (см. рисунок 14). Появится сообщение. Для отмены действия нажмите кнопку **Отмена**.

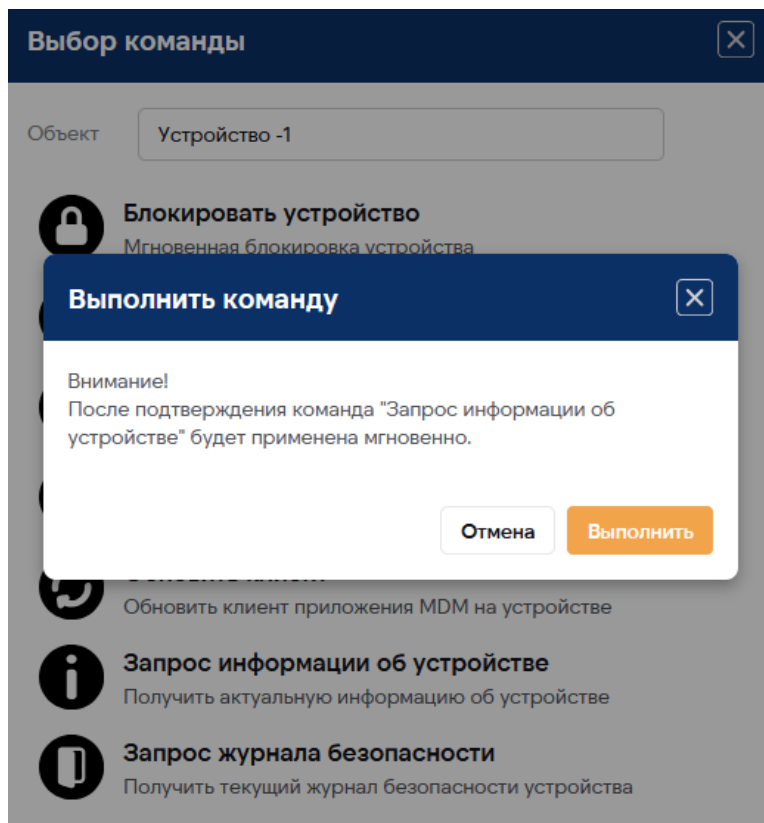
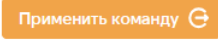


Рисунок 16 – Запрос информации об устройстве

Запрос журнала безопасности

Чтобы запросить журнал безопасности выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите в списке нужное устройство.
3. Нажмите кнопку . Откроется модальное окно.
4. В модальном окне выберите команду **Запрос журнала безопасности** и нажмите на нее. На экране появится модальное окно.
5. Нажмите кнопку **Выполнить** для завершения процесса (см. рисунок 15). Появится сообщение. Для отмены действия нажмите кнопку **Отмена**.

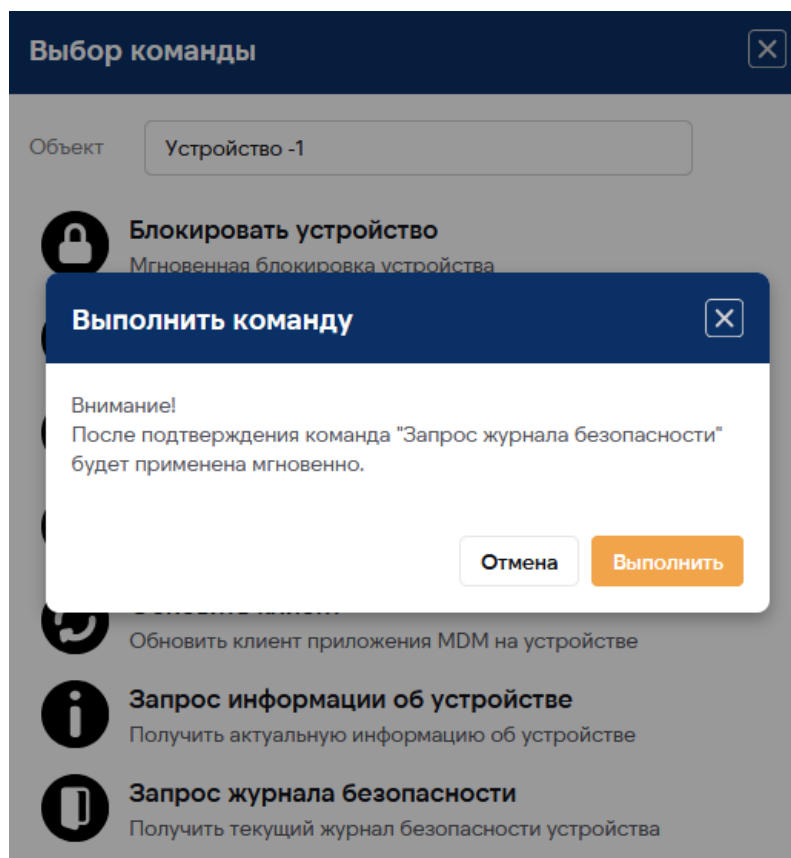
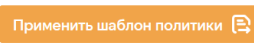


Рисунок 17 – Запрос журнала безопасности

6.5. Применение шаблона политики к устройству или группе устройств

Чтобы применить шаблон политики к устройству или группе устройств и обновить настройки, выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите устройство или группу устройств.
3. Нажмите кнопку . Появится модальное окно (см. рисунок 16).
4. В модальном окне в поле **Название шаблона политики** введите название шаблона или выберите из списка.
5. Нажмите кнопку **Найти**.
6. Нажмите кнопку **Назначить**. Система назначит правила из шаблона.

Для очистки формы поиска нажмите кнопку **Очистить**. Для отмены действия нажмите кнопку **Отмена**.

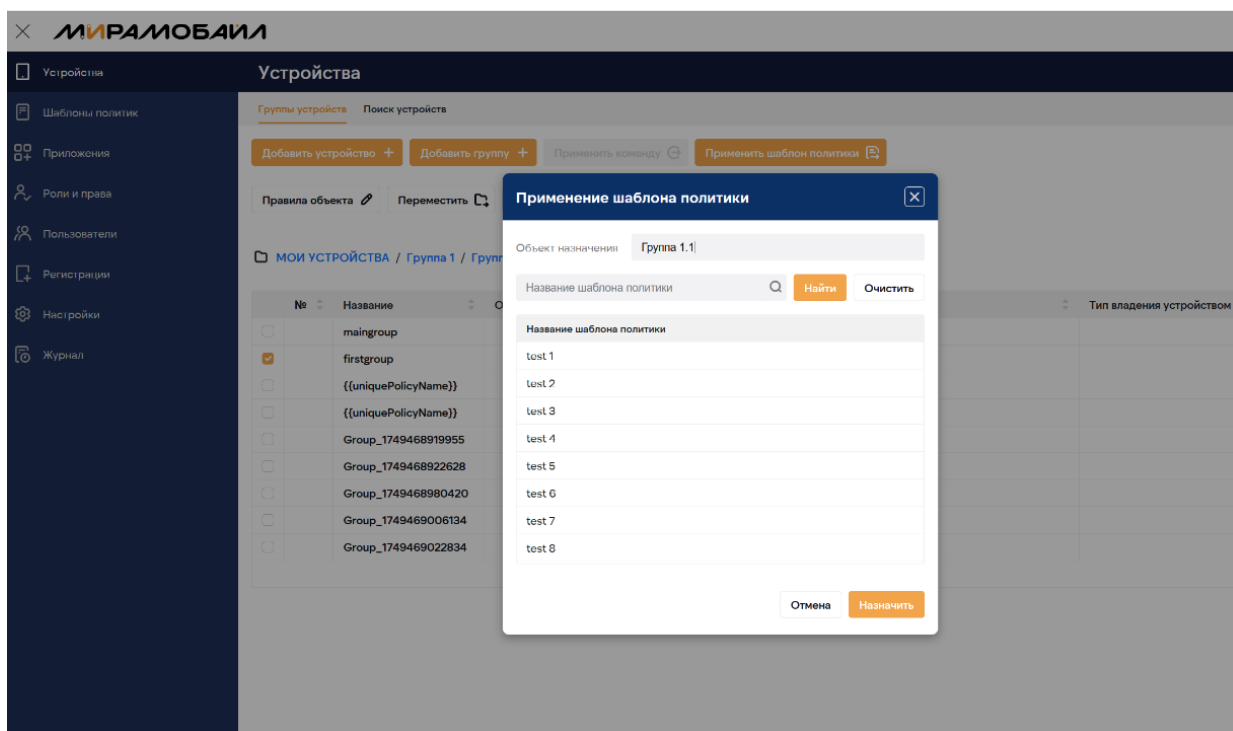


Рисунок 18 – Применение шаблона политики

Примечание – При назначении шаблона политики на устройство или группу действует механизм определения приоритетных правил и разрешения конфликтов между ними.

6.6. Экспорт списка устройств

Чтобы экспортировать список актуальных устройств для анализа или отчётности выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. В правом верхнем углу интерфейса нажмите кнопку

Экспортировать

Система сгенерирует *.csv-файл с разделителем в виде символа ';'. «Администратор» может открыть файл для просмотра или сохранить его на своём ПК.

Основные сведения об устройстве представлены в таблице 4.

Таблица 6 – Основные сведения об устройстве

Данные	Описание
Идентификатор	Уникальный идентификатор устройства в БД
UDID	Уникальный идентификатор устройства
Владелец	Идентификатор владельца устройства
Группа	Группа, в которой расположено устройство
Версия OS	Версия операционной системы
Расширение OS	Дополнительные данные OS
Версия клиента	Версия MDM-клиента
IMEI	IMEI устройства
Тип владения устройством	Корпоративное или личное
Статус устройства:	Текущий статус устройства (онлайн/офлайн)
Дата последней синхронизации с устройством	Дата и время последнего успешного обмена данными с устройством;

Данные	Описание
Пиктограмма статуса	Графический индикатор состояния подключения устройства (например, онлайн, офлайн, ошибка);
Время отсутствия в сети	Если устройство офлайн, отображается, как долго оно не было в сети (в часах/минутках);
Последние координаты	Последние известные географические координаты устройства (широта, долгота);
Уровень заряда батареи	Текущий процент заряда батареи устройства

Примечание – При экспорте из окна просмотра групп устройств файл содержит список устройств, доступных текущему пользователю в выбранной группе и всех её подгруппах. При экспорте из окна поиска устройств файл включает все устройства, соответствующие установленным пользователем фильтрам с учётом его роли и доступных групп устройств.

6.7. Просмотр подробной информации об устройстве

Информация об устройстве или группе устройств

«Администратор» может получить актуальную информацию о мобильном устройстве пользователя. Для этого выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите устройство в окне списка.

3. Нажмите кнопку . Откроется информационная панель с подробными сведениями об устройстве (см. рисунок 17). По умолчанию отображается вкладка **Об устройстве**.

В информационной панели доступны следующие данные:

- ФИО пользователя устройства;
- должность пользователя;
- e-mail;
- текущий статус подключения устройства к сети (в сети, не в сети);
- координаты устройства;
- уровень заряда аккумулятора;
- IP-адрес.

Для получения дополнительной информации используйте вкладки: **Об устройстве, SIM, Правила безопасности, Приложения, Wi-Fi, События, Координаты**.

Примечание – Отображение информации внутри вкладок происходит только при наличии у администратора прав на их просмотр. Детали см. в разделе [Роли и права](#).

Об устройстве

На вкладке **Об устройстве** отображается подробная информация, включающая следующие разделы (см. рисунок 17, таблицу 5).

Свойства устройства

Пользователь

Информация о пользователе устройства

ФИО:

Петров Иван Иванович

Должность:

Администратор

E-mail:

admin@mira-mobile.ru

Статус устройства

Информация получена 30.06.2025, 10:59:11

Текущий статус:

Не в сети

Координаты:

37.421998333333335 -122.084

Аккумулятор:

100%

IP-адрес:

ipv4 : 10.0.2.15 ipv6 : FE80::9022:EFF:FE35:AE56

Об устройстве

SIM

Правила безопасности

Приложения

Wi-Fi

События

Координаты

Сведения об устройстве

Системная информация об устройстве и его характеристики

UDID:

658dc2f1-dc2b-ca38-b315-66c5ba673255

Принадлежит к группе:

Группа 1

Платформа:

ANDROID

Версия mdm-клиента:

local

Версия ОС:

R 11

ROOT-доступ для mdm-admin:

Тип владения:

Личное

Шифрование памяти:

Производитель:

Google

Запрос пароля:

Модель:

sdk_gphone_x86

Пароль:

Серийный номер:

EMULATOR35X5X10X0

IMEI:

358240051111110

MAC-адрес Wi-Fi:

—

MAC-адрес BT:

—

Заккрыть

Рисунок 19 – Вкладка Об устройстве

Таблица 7 – Сведения об устройстве

Характеристика	Описание / Пример
UDID устройства	Уникальный идентификатор устройства
Пиктограмма ОС устройства	Иконка или логотип операционной системы
Версия ОС	Текущая версия операционной системы

РУКОВОДСТВО АДМИНИСТРАТОРА

41

Характеристика	Описание / Пример
Тип владения устройства	Корпоративное или личное
Производитель устройства	Samsung
Серийный номер устройства	R43FDS331FAA
IMEI устройства	Международный идентификатор мобильного оборудования
Mac-адрес Wi-Fi	MAC-адрес Wi-Fi адаптера
Mac-адрес Bluetooth	MAC-адрес Bluetooth адаптера
Группа устройства	Название группы, в которую входит устройство
Версия MDM-клиента	Текущая версия установленного клиента MDM
Root-доступ для MDM-admin	Наличие root-доступа для администратора MDM (да/нет)
Шифрование памяти	Статус шифрования памяти (включено/выключено)
Запрос пароля	Требуется ли запрос пароля при доступе (включено/выключено)
Кнох	Статус Samsung Кнох (активирован/не активирован)

Характеристика	Описание / Пример
Пароль для удаления MDM-клиента	Наличие пароля для удаления клиента MDM

SIM

На вкладке **SIM** отображается информация о SIM-картах, установленных в устройстве пользователя. Может содержать произвольное количество сим-карт (таблицу 8).

Таблица 8 – Характеристики Sim – карт

Характеристика	Пример
IMSI	89701201915301009638
Номер телефона	+79991112233
Текущий Оператор связи	Beeline
Страна текущего подключения	Россия
Текущая сотовая сеть	
Домашняя страна подключения	Россия
Домашняя сотовая сеть	Россия

Правила безопасности

Для каждого правила отображается экземпляр, назначенный на данное устройство, а также активный экземпляр, если они отличаются.

По каждому правилу отображаются следующие данные (см. рисунок 12):

- Название правила;
- Объект, на который правило назначено непосредственно;
- Визуальный признак активности — указывает, что правило является активным;
- Визуальный признак суперприоритета — обозначает, что правило имеет статус «суперприоритетное»;
- Настройки правила — параметры и условия, определяющие поведение правила.

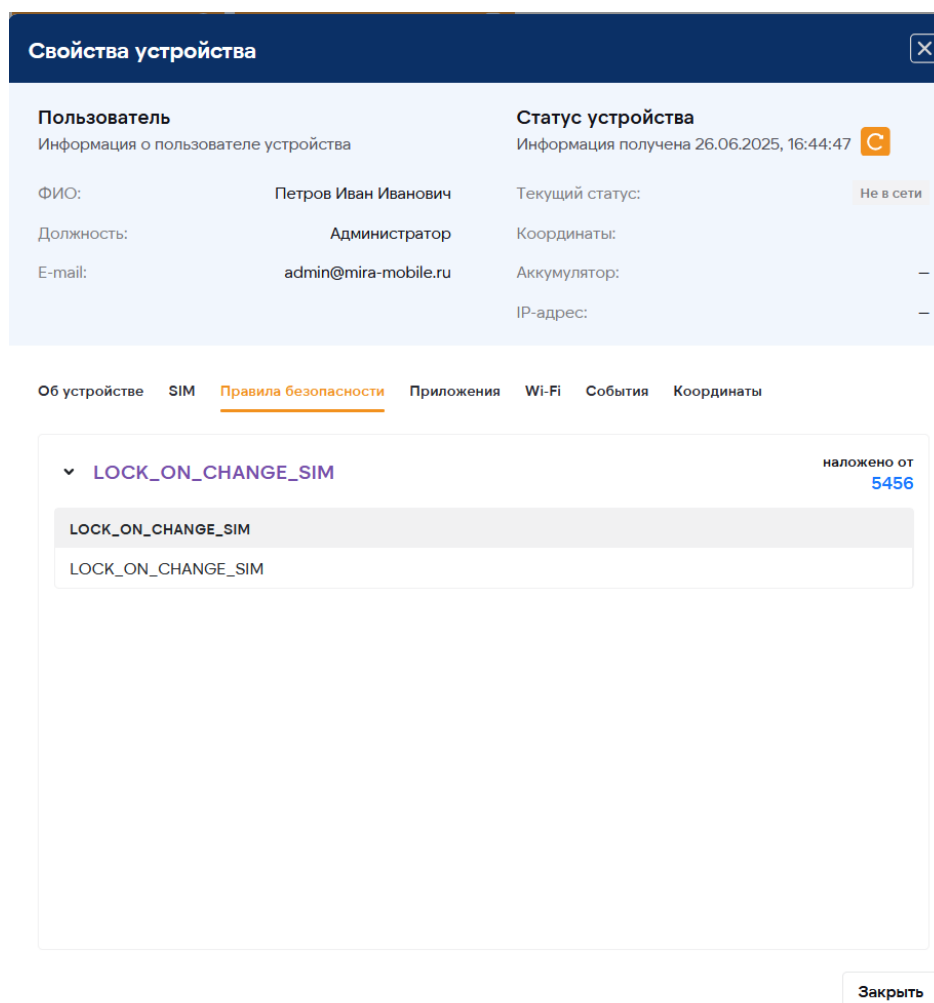


Рисунок 20 – Вкладка Правила безопасности

Приложения

На вкладке **Приложения** приведен актуальный список установленных на устройстве приложений. Отображаются все приложения, установленные на

устройстве, в том числе те, которые «Администратор» установил, применив соответствующую политику.

Свойства устройства

Пользователь

Информация о пользователе устройства

ФИО:

Петров Иван Иванович

Должность:

Администратор

E-mail:

admin@mira-mobile.ru

Статус устройства

Информация получена 30.06.2025, 10:59:11

Текущий статус:

Не в сети

Координаты:

37.42199833333335 -122.084

Аккумулятор:

100%

IP-адрес:

ipv4 : 10.0.2.15 ipv6 : FE80::9022:EFF:FE35:AE56

Об устройстве

SIM

Правила безопасности

Приложения

Wi-Fi

События

Координаты

Название	Пакет
Tethering	com.google.android.networkstack.tetherir
com.android.cts.priv.ctsshim	com.android.cts.priv.ctsshim
YouTube	com.google.android.youtube
Corner cutout	com.android.internal.display.cutout.emula
Android Services Library	com.google.android.ext.services
Double cutout	com.android.internal.display.cutout.emula
Phone and Messaging Storage	com.android.providers.telephony
Dynamic System Updates	com.android.dynsystem
Pebble	com.android.theme.icon.pebble
Google	com.google.android.googlequicksearchbo
Call Broadcast Service	com.google.android.callbroadcastservice

Заккрыть

Рисунок 21 – Вкладка Приложения

WI-FI

На вкладке **Wi-Fi** в табличном виде отображён список используемых точек доступа Wi-Fi. Представлены только сохраненные на устройстве Wi-Fi сети. Для каждой сети указываются (см. рисунок 13):

- SSID (имя сети);
- механизм (Тип) аутентификации.

РУКОВОДСТВО АДМИНИСТРАТОРА

45

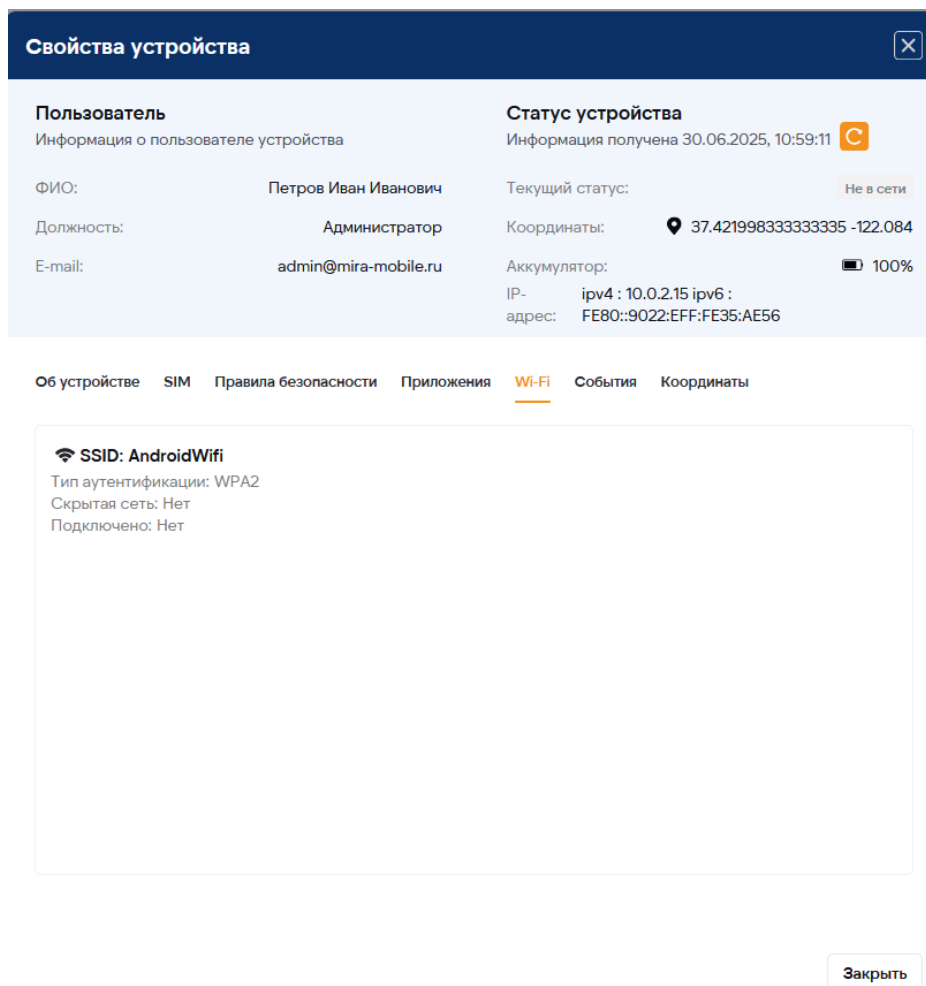


Рисунок 22 – Вкладка Wi-Fi

События

На вкладке **События** в табличном виде отображается информация о событиях безопасности, произошедших на устройстве (см. рисунок 14, таблица 7).

Свойства устройства

Пользователь

Информация о пользователе устройства

ФИО:

Петров Иван Иванович

Должность:

Администратор

E-mail:

admin@mira-mobile.ru

Статус устройства

Информация получена 26.06.2025, 16:44:47

Текущий статус:

Не в сети

Координаты:

—

Аккумулятор:

—

IP-адрес:

—

Об устройстве

SIM

Правила безопасности

Приложения

Wi-Fi

События

Координаты

Временной интервал отображения событий

От

До

Найти

Очистить

Сгенерирован сервисный пароль для устройства с uuid: 464a575b-9f9d-7edd-f214-cbaa0af93034}

11:01 | 02.07.2025

Статус: AGENT_PASSWORD_CHANGED

{"ucid":"111bf80d-b70d-4ad9-92b1-98150eb11002","status":"SUCCESS"}

11:30 | 30.06.2025

Статус: COMMAND_APPLIED

{"ucid":"106bf80d-b70d-4ad9-92b1-98150eb11002","status":"SUCCESS"}

11:28 | 30.06.2025

Статус: COMMAND_APPLIED

Устройство отключено

11:26 | 30.06.2025

Статус: DEVICE_DISCONNECTED

Устройство подключено

11:26 | 30.06.2025

Статус: DEVICE_CONNECTED

Заккрыть

Рисунок 23 – Вкладка События

Для поиска события устройства в заданном временном интервале выполните следующие действия:

1. Выберите начальную и конечную даты в выпадающем календаре.

Выбрать

2. Нажмите кнопку .
3. Нажмите кнопку **Найти**. На экране отобразится список событий устройств, соответствующих выбранным датам (см. рисунок 16). Для сброса выбранных дат и очистки результатов поиска используйте кнопку **Очистить**.

РУКОВОДСТВО АДМИНИСТРАТОРА

47

Свойства устройства

✕

Пользователь

Информация о пользователе устройства

ФИО:Петров Иван Иванович

Должность:Администратор

E-mail:admin@mira-mobile.ru

Статус устройства

Информация получена — С

Текущий статус:В сети

Координаты:—

Аккумулятор:—

IP-адрес:0.0.0.0

Об устройстве

SIM

Правила безопасности

Приложения

Wi-Fi

События

Координаты

Временной интервал отображения событий

02.06.2025

02.07.2025

Найти

Очистить

{"ucid":"111bf80d-b70d-4ad9-92b1-98150eb11002","status":"SUCCESS"}

Статус: COMMAND_APPLIED

11:30 | 30.06.2025

{"ucid":"106bf80d-b70d-4ad9-92b1-98150eb11002","status":"SUCCESS"}

Статус: COMMAND_APPLIED

11:28 | 30.06.2025

Устройство отключено

Статус: DEVICE_DISCONNECTED

11:26 | 30.06.2025

Устройство подключено

Статус: DEVICE_CONNECTED

11:26 | 30.06.2025

com.google.android.contactkeys

Статус: INSTALL_APP

11:26 | 30.06.2025

Устройство отключено

11:26 | 30.06.2025

Закреть

Рисунок 24 – Поиск события устройства за определённый период

Таблица 9 – Информация о событиях безопасности на устройстве

Тип события	Описание события	Отображаемые параметры
Отправка правила безопасности	Фиксация факта отправки правила безопасности на устройство	Дата и время отправки; Название правила; Статус применения правила; Просмотр настроек правила
Назначение команды	Назначение и выполнение команды на устройстве	- Название команды (например, «Заблокировать устройство») - Статус выполнения команды (например, «START_APP», «INTERNET_ON», «COMMAND_APPLIED»)

Тип события	Описание события	Отображаемые параметры
Фильтрация по дате	Отбор событий за выбранный период	Начальная дата; Конечная дата
Очистка журнала событий	Удаление всех событий из журнала устройства	Подтверждение действия (да/нет)

Координаты

Вкладка **Координаты** содержит список всех координат, которые были получены с данного устройства, от недавно полученных к давно полученным. По каждой координате:

- полученные координаты;
- дата-время получения координат.

6.8. Создание приглашения на добавление нового устройства

Чтобы создать приглашение и управлять им выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Нажмите кнопку . Откроется форма приглашения пользователя на регистрацию.
3. В открывшейся форме выберите одного или несколько пользователей для которых создаётся приглашение.
4. Выберите тип владения устройством (например, «Личное»), укажите дату и время окончания срока действия приглашения (см. рисунок 26).
5. Выберите группу устройств, в которую будет добавлено новое устройство после регистрации.
6. Выберите способ отправки приглашения:
 - отправить приглашение пользователям: система отправит QR-код по электронной почте каждому выбранному пользователю;

- скачать QR-код: если выбран один пользователь, скачайте QR-код в формате *.pdf. Файл будет содержать ссылку для скачивания приложения, пароль и другие необходимые данные.

7. Подтвердите действие, нажав кнопку **Отправить** или **Скачать**.

Система обработает запрос и сообщит о статусе в разделе **Журнал**.

Примечание – Скачанный файл формата *.pdf содержит QR-код с инструкциями для скачивания приложения и подключения (см. рисунок 27).

Откройте его в удобном месте и следуйте указаниям для регистрации устройства.

Приглашение на регистрацию

ФИО Подразделение Должность **Найти** Очистить

☐ Нет зарегистрированных устройств ☐ Еще не приглашен

	Имя пользователя	Должность	Подразделение	Телефон
☐	Имя1 Отчество1 Пользак1			
☐	Пользак2			
☐	Александр Александрович Александр	test	test	79992029988
☒	Иван Николаевич Корепин	Всея менеджер	проектный офис	79627279901
☐	Андрей Иванов			
☐	Дарья Петрова	DevOps		
☐	Морозов	Тестировщик	Отдел тестирования	
☐	qwe qwe qwe	qwe	qwe	79627279901

Тип владения устройством: ☒ Личное ☐ Корпоративное

Конечная папка размещения устройства **Мои устройства**

Дата окончания срока действия приглашения **Дата окончания** **Время окончания** 11:00

Отправить **Скачать**

Рисунок 25 – Форма приглашения на регистрацию



Скачайте приложение по ссылке: <https://mdm-developer.ru/mdm-core/api/v1/mobile-applications/distribution?registrationCode=433849>. Далее следуйте инструкциям приложения. Пароль: 433849

Рисунок 26 – Пример QR-кода с приглашением и паролем

6.9. Создание группы и добавление в нее устройств

Чтобы создать группу устройств выполните следующие действия (см. рисунок 15):

1. Перейдите в раздел **Устройства**.
2. Откройте окно со списком устройств.
3. Нажмите кнопку .
4. В открывшемся окне введите название новой группы.
5. Выберите место создания группы, нажав на иконку . Откроется модальное окно по выбору групп для размещения устройства.
6. Для быстрого поиска нужной группы воспользуйтесь строкой поиска: введя название группы и нажав кнопку **Найти**. Результаты поиска отобразятся в окне.
7. Выберите нужную группу и нажмите кнопку **Выбрать**.

8. После выбора места размещения в правом нижнем углу окна нажмите кнопку **Создать**. Диалоговое окно закроется, а в списке устройств появится созданная группа.

Для отмены действий нажмите кнопку **Отмена**.

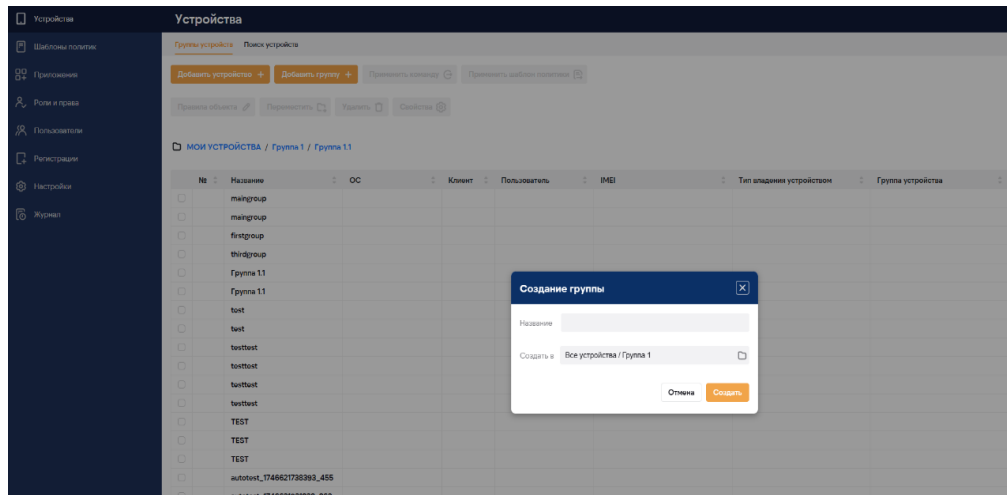


Рисунок 27 – Создание группы устройств

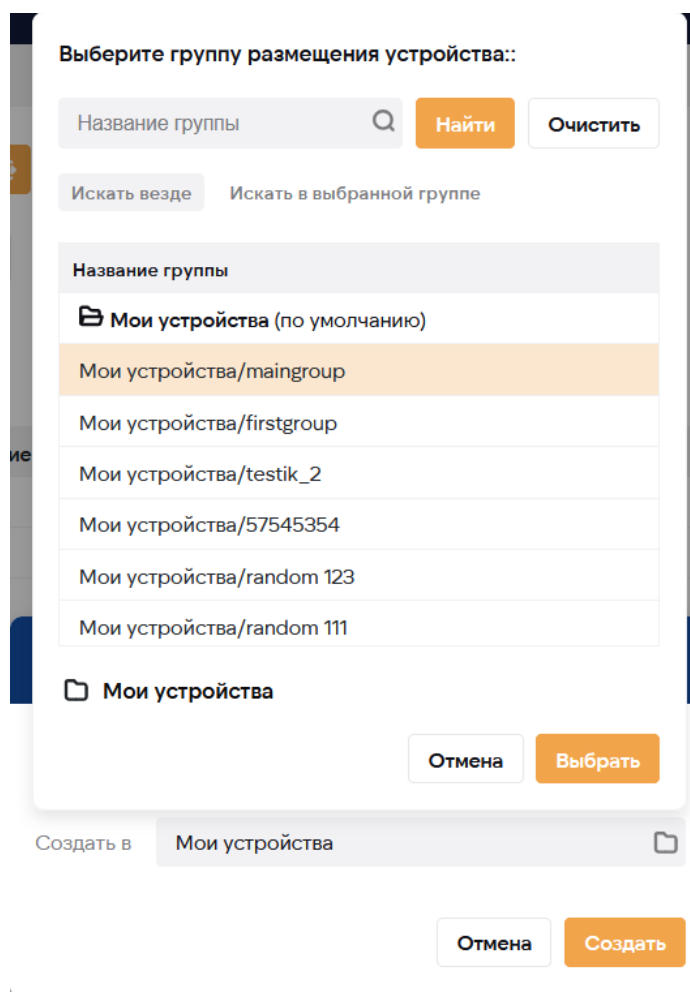


Рисунок 28 – Выбор группы устройств

6.10. Редактирование правила политик безопасности на выбранном устройстве или группе устройств

Чтобы редактировать правила политик безопасности на устройстве или группе устройств, выполните следующие действия (см. рисунок 17):

1. Перейдите в раздел **Устройства**.
2. Выберите устройство или группу.
3. Нажмите кнопку . Откроется форма редактора правил.
4. Измените настройки, активировав переключатель.
5. В правом нижнем углу нажмите кнопку **Применить**.

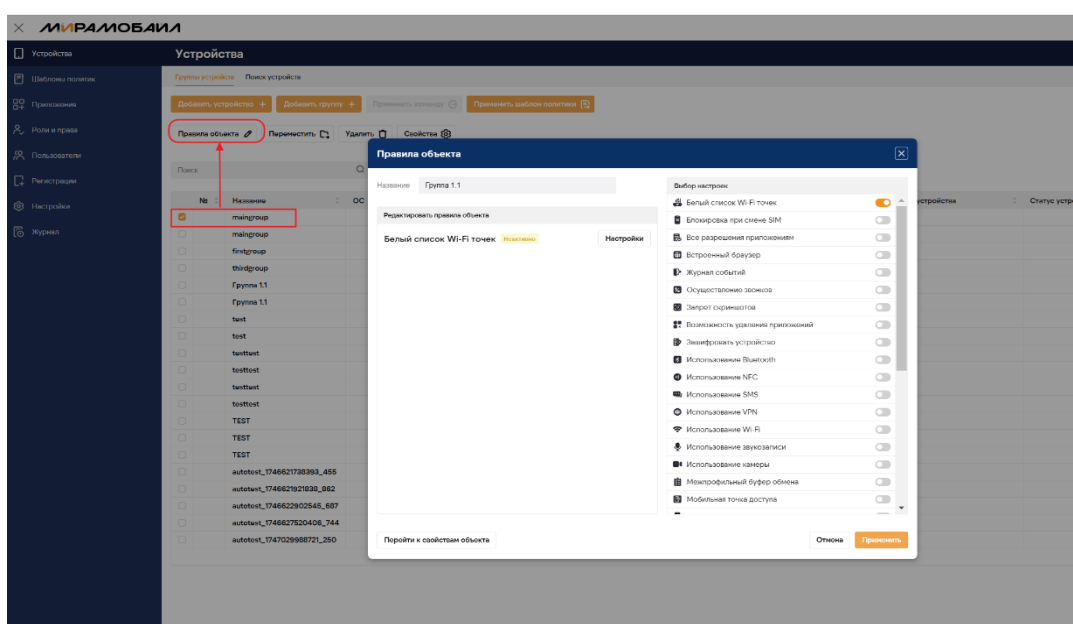


Рисунок 29 – Редактирование правила политик безопасности

В таблице 10 приведён список политик и платформ, на которых они применяются.

Таблица 10 – Список политик и платформ

Пиктограмма	Политика	Используется на платформе
	Пароль и блокировка	Android, Android (BYOD)

Пиктограмма	Политика	Используется на платформе
	Журнал событий	Android, Android (BYOD)
	Установить/удалить приложения	Android, Android (BYOD)
	Возможность удаления приложения	Android, Android (BYOD)
	Все разрешения приложениям	
	Черный список приложений	Android, Android (BYOD)
	Использование Bluetooth	Android
	Использование звукозаписи	Android
	Использование камеры	Android, Android (BYOD)
	Использование Wi-Fi	Android
	Настройка Wi-Fi точек	Android
	Белый список Wi-Fi точек	Android

Пиктограмма	Политика	Используется на платформе
	Настройка Proxy	Android
	Настройка почты Exchange	Android (только для Samsung-устройств)
	Зашифровать устройство	Android
	Сотовые станции	Android
	Использование NFC	Android
	Использование VPN	Android
	Отладка по USB	Android
	Передача данных по USB	Android
	Сброс настроек	Android
	Запрет осуществления звонков	Android
	Встроенный браузер	Android

Пиктограмма	Политика	Используется на платформе
	Мобильные данные	Android
	Хранилище данных	Android
	Использование SMS	Android
	Мобильная точка доступа	Android
	Частота обмена данными	Android
	Блокировка при смене SIM-карты	Android
	Системные приложения	Android, Android (BYOD)
	Межпрофильный буфер обмена	Android, Android (BYOD)
	Право установки приложений	Android, Android (BYOD)
	Запрет скриншотов	Android, Android (BYOD)

6.11. Удаление устройства или групп устройств

Чтобы удалить устройство или группу устройств из системы выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите устройство или группу устройств в окне списка (см. рисунок 18).
3. Нажмите кнопку . Откроется модальное окно подтверждения удаления объекта с возможностью выбора:
 - для продолжения подтвердите удаление;
 - для отмены действия нажмите кнопку **Отмена**.
4. После подтверждения:
 - если выбрана группа устройств, будут удалены только пустые группы, в которых отсутствуют устройства. Если в группе есть хотя бы одно устройство, удаление не будет выполнено, и система выдаст ошибку;
 - на выбранное устройство будет отправлена служебная команда на удаление клиентского приложения;
 - после успешного выполнения команды и получения подтверждения от устройства сервер удалит устройство из системы.
5. После удаления всех устройств из группы, пустые группы будут удалены автоматически.

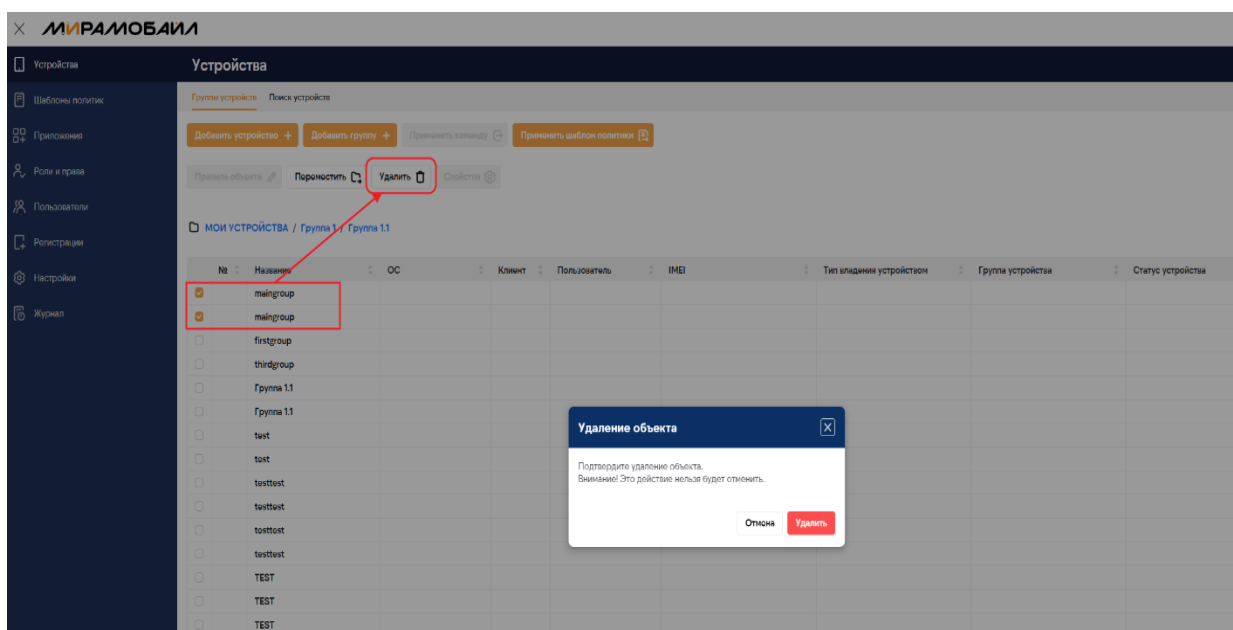
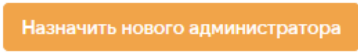
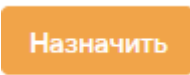


Рисунок 30 – Удаление устройства

6.12. Изменение списка администраторов групп у выбранной группы

Назначение администратора

Чтобы назначить нового администратора групп и управлять доступом выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите группу, для которой необходимо назначить нового администратора.
3. Нажмите кнопку . Откроется окно редактора.
4. Перейдите на вкладку **Администраторы** (см. рисунок 28).
5. Нажмите кнопку . Откроется модальное окно со списком администраторов (см. рисунок 29).
6. В списке выберите нужного пользователя и нажмите кнопку . Для отмены действия нажмите кнопку **Отмена**.

Примечание – для быстрого поиска администратора воспользуйтесь формой поиска (см. рисунок 29). Введите данные пользователя и нажмите

кнопку .

Свойства группы

✕

Название

третья

Количество устройств: 12

Путь

/firstgroup/123/qwerty/5456/третья

Правила безопасности

Администраторы

Назначить нового администратора

Удалить

Логин	Имя пользователя	E-mail	Телефон
ivanov	ИвановАндрей	ivanov@mail.ru	
kek	ПетроваДарья	user1@mail.ru	

Посмотреть все назначенные правила

Отмена

Применить

Рисунок 31 – Модальное окно со списком администраторов

Свойства группы

Название

maingroup

Количество устройств: 5

Путь

/maingroup

Назначение администратора

Объект назначения

maingroup

Данные пользователя

Найти

Очистить

	Логин	Имя пользователя	E-mail	Телефон
☐	alex	АлександрАлександрАлександрович	alexandr@mail.com	79992029988
☐	test123	testtesttest	test@mail.com	79028887722

Отмена

Назначить

Посмотреть все назначенные правила

Отмена

Применить

Рисунок 32 – Назначение администраторов

Удаление администратора

Чтобы удалить администратора групп выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите группу, для которой необходимо изменить список администраторов.
3. Нажмите кнопку . Откроется окно редактора.
4. Перейдите на вкладку **Администраторы** (см. рисунок 28).

5. Нажмите кнопку . Произойдет автоматическое удаление администратора. Для отмены действия нажмите кнопку **Отмена**.

7. Раздел Шаблоны политик

Раздел предназначен для создания и управления стандартными наборами правил и настроек, которые применяются к устройствам или их группам с целью унификации управления поведением и обеспечением безопасности. Использование шаблонов упрощает администрирование, позволяя быстро и последовательно внедрять согласованные политики по всей организации. При этом изменения в шаблонах не затрагивают уже назначенные устройства, что обеспечивает стабильность их текущей конфигурации.

Шаблоны политик — конечный набор правил и настроек, применяемых к устройствам или группам устройств для управления их поведением и безопасностью.

Шаблоны позволяют стандартизировать и упростить настройку правил, обеспечивая единообразное применение настроек в организации.

Изменения в шаблоне не влияют на устройства, которым он уже назначен.

«Администратор» может создавать, редактировать, удалять шаблоны для управления настройками и безопасностью устройств.

7.1. Главное окно раздела

Окно отображает список шаблонов с полями (см. рисунок 20):

- **Название шаблона;**
- **Дата создания;**
- **Дата редактирования;**
- **Автор редактирования;**
- **Описание.**

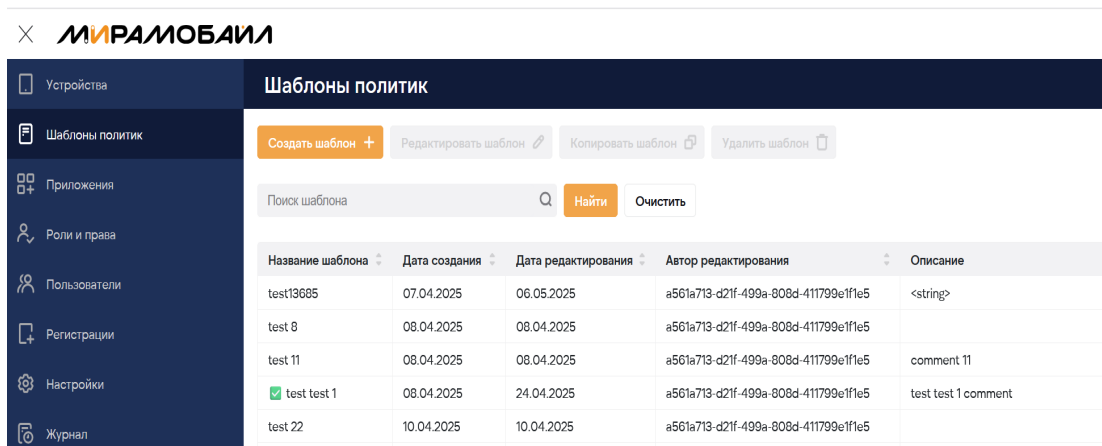


Рисунок 33 – Главное окно раздела Шаблоны политик

7.2. Создание нового шаблона

Окно создания включает поля для ввода названия (обязательное), комментария и списка правил. После добавления правил система проверяет уникальность названия.

Для создания нового шаблона выполните следующие действия:

1. Перейдите в раздел **Шаблоны политик**.

Нажмите кнопку **Создать шаблон** в главном окне. Появится модальное окно со списком правил в правой части, которые могут быть добавлены в шаблон с помощью активации переключателя при выборе настроек (см. рисунок 21).

2. В соответствующих полях введите название, при необходимости добавьте комментарий.
3. Настройте параметры политики. Набор параметров зависит от выбранного правила.
4. После добавления в группу всех нужных политик в правом нижнем углу модального окна нажмите кнопку **Применить**. Окно закроется и

созданный шаблон появится в списке шаблонов политики.

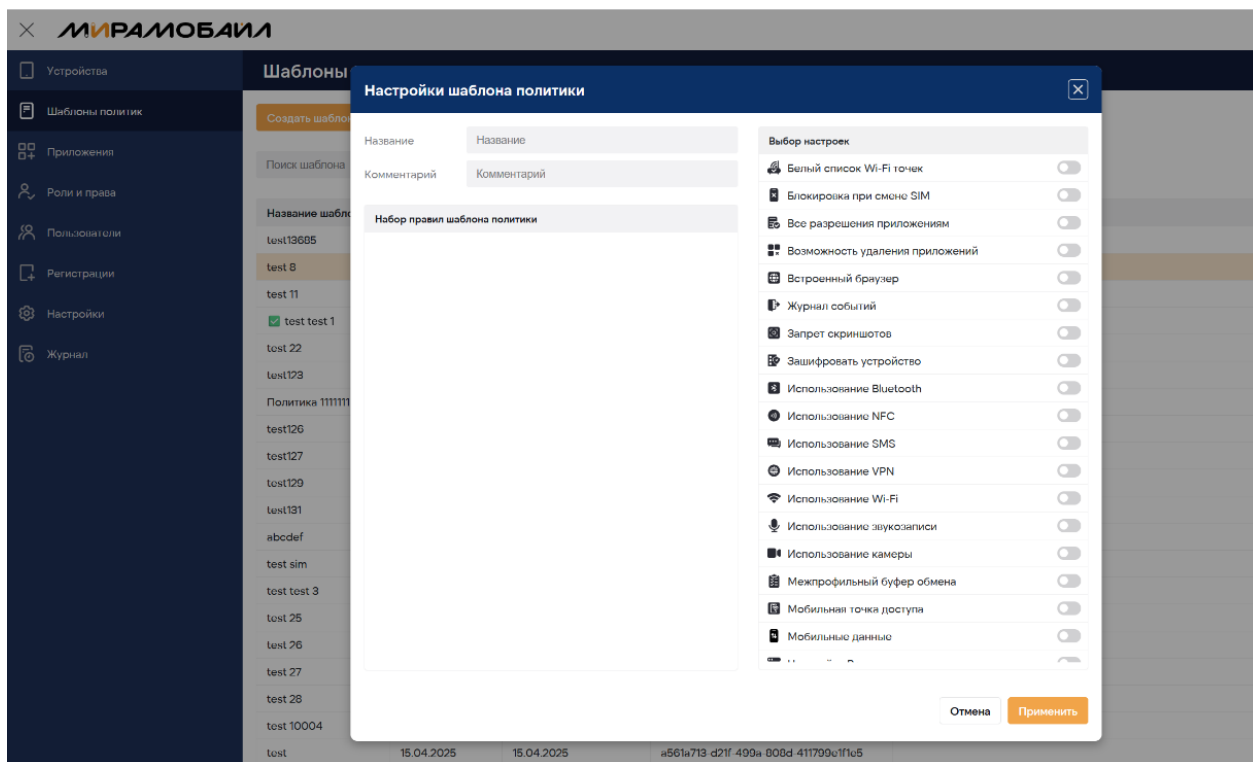


Рисунок 34 – Создание нового шаблона

7.3. Создание шаблона через копирование существующего

Для копирования шаблона политики выполните следующие действия:

1. Перейдите в раздел **Шаблоны политик**.
2. Выберите существующий шаблон в главном окне.
3. Нажмите кнопку . Система создаст копию шаблона политики с добавлением «Копия» к названию, включая правила и параметры правил и автоматически откроет «копию» для редактирования (см. рисунок 22).
4. Внесите необходимые изменения правил во скопированный шаблон, и, при необходимости, измените название шаблона.
5. Для сохранения изменений нажмите на кнопку **Применить**.
6. Для отмены изменений нажмите кнопку **Отмена**.

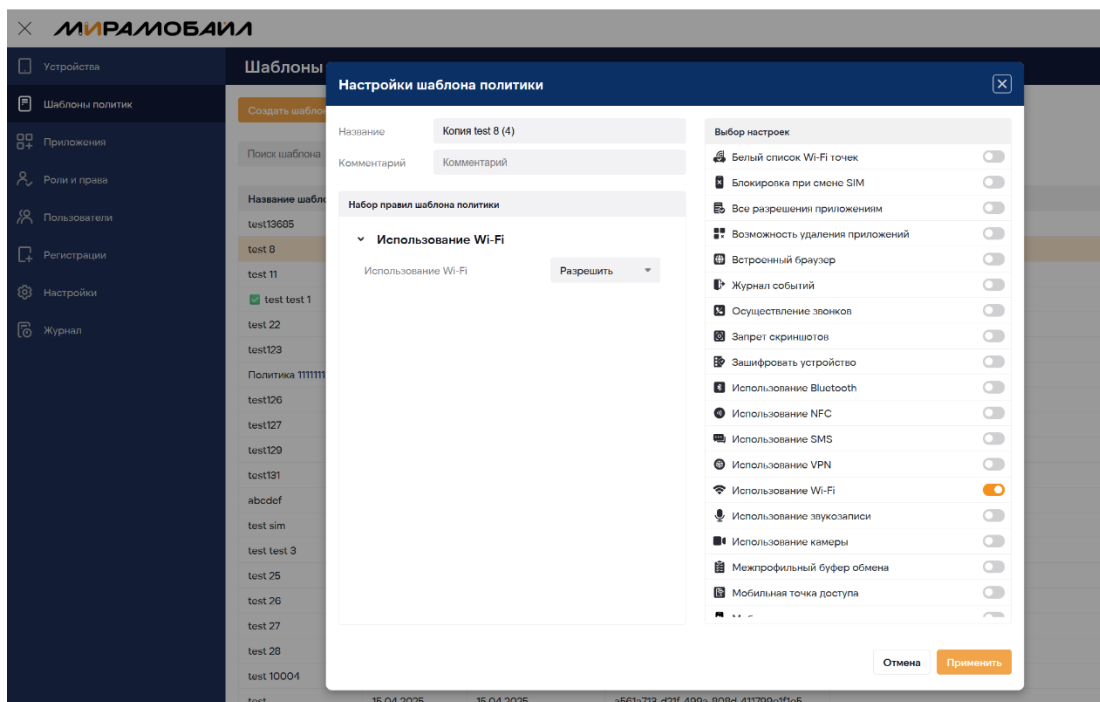


Рисунок 35 – Создание шаблона через копию существующего

7.4. Редактирование шаблона политики

Для редактирования шаблона политики выполните следующие действия:

1. Перейдите в раздел **Шаблоны политик**.
2. Выберите нужный шаблон.
3. Нажмите кнопку . Откроется модальное окно с настройками (см. рисунок 23).
4. В модально мокне измените параметры шаблона политик, добавляя или отключая настройки с помощью переключателя. Добавленные правила шаблона политик отобразятся в левой части окна. Для подробного просмотра списка правил шаблона политик (см. [Приложение.](#)).
5. После внесения изменений в правом нижнем углу модального окна нажмите кнопку **Применить**. Модальное окно закроется, изменения будут сохранены. Для отмены действия нажмите кнопку **Отмена**.

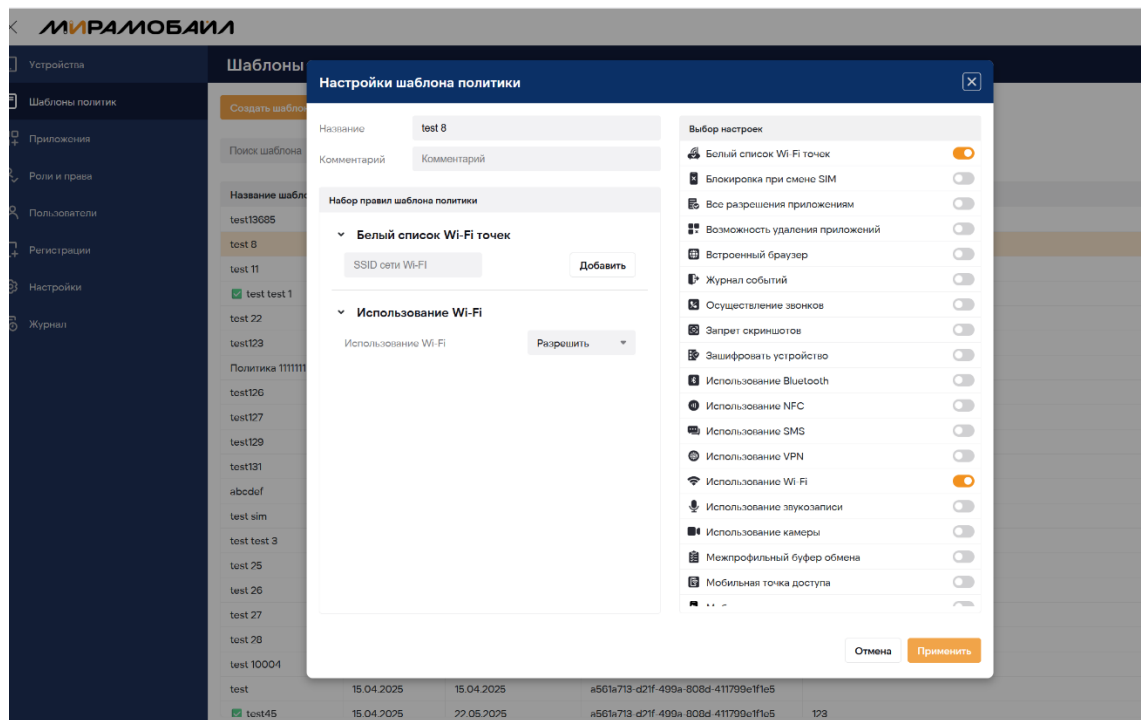


Рисунок 36 – Редактирование шаблона политик

7.5. Удаление шаблона политики

Для удаления шаблона политики выполните следующие действия:

1. Перейдите в раздел **Шаблоны политик**.
2. Выберите шаблон в главном окне.
3. Нажмите кнопку  **Удалить шаблон**. Появится модальное окно (см. рисунок 24).
4. Подтвердите удаление, нажав кнопку **Удалить**. Система удалит шаблон.

Для отмены действия нажмите кнопку **Отмена**.

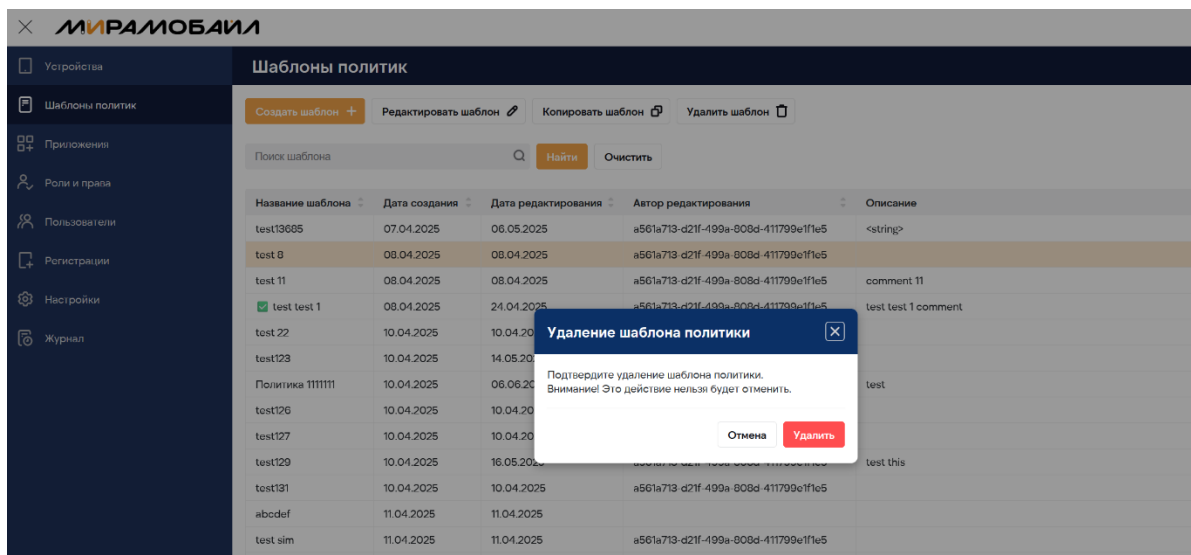


Рисунок 37 – Удаление шаблона политики

8. Раздел Приложения

Раздел предназначен для управления каталогом приложений, обеспечивая централизованное добавление и хранение программного обеспечения. Система позволяет создавать каталог приложений, которые впоследствии могут быть установлены на устройствах или группах устройств. В каталог можно добавлять приложения как из магазинов (Google Play, App Gallery, RuStore, GetApps), так и загружая арк-файл.

8.1. Главное окно раздела

Окно отображает список приложений с полями (см. рисунок 25):

- Приложение;
- Пакет;
- Версия пакета;
- Кол-во устройств;
- ОС;
- Способ загрузки;
- Дата загрузки;
- Пользователь.

Приложение	Пакет	Версия пакета	Кол-во устройств	ОС	Способ загрузки	Дата загрузки	Пользователь
apps_uploading_error				ANDROID	INTERNAL	2025-07-03T10:46:04.226929Z	00000000-0000-0000-0000-000000000000
apps_uploading_error				ANDROID	EXTERNAL_FILE	2025-07-07T08:21:50.116276Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4
apps_uploading_error				ANDROID	EXTERNAL_FILE	2025-07-07T14:20:34.643135Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4
apps_uploading_error				ANDROID	EXTERNAL_FILE	2025-07-08T09:46:22.816002Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4
	test.test			ANDROID	EXTERNAL	2025-07-08T10:15:28.629019Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4
apps_uploading_error				ANDROID	EXTERNAL_FILE	2025-07-08T10:53:47.719206Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4
HW	com.helloworld.app	1.0		ANDROID	EXTERNAL_FILE	2025-07-08T12:25:52.713709Z	1d38badd-23c9-4bc2-bb43-78034c6d51b4

Рисунок 38 – Главное окно раздела Приложения

8.2. Добавление стороннего приложения в каталог через APK файл

Для добавления стороннего приложения на Android - устройства с помощью загрузки арк-файла выполните следующие действия:

1. Перейдите в раздел **Приложения**.

2. Нажмите кнопку .
3. В появившемся окне для нажмите кнопку **Открыть** для выбора арк-файла.
4. Выберите нужный арк-файл и подтвердите загрузку.
5. Дождитесь завершения загрузки приложения на сервер. Приложение появится в списке доступных приложений.

8.3. Добавление приложения в каталог из магазина приложений

Поддерживаемые магазины для установки приложений:

- Google Play;
- App Gallery;
- RuStore;
- GetApps.

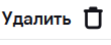
Для добавления приложения на Android - устройства выполните следующие действия:

1. Перейдите в раздел **Приложения**.
2. Нажмите кнопку .
3. В появившемся окне введите имя пакета приложения.
4. Нажмите кнопку **Добавить**. Приложение появится в списке.
5. В главном окне раздела в поле **Приложение** отобразится его название, полученное из арк-файла.
6. При установке на устройстве пользователя откроется диалог установки из доступного на устройстве магазина приложений (Google Play, App Gallery, RuStore, GetApps).

Примечание – Система не требует наличия конкретного магазина. Установка осуществляется с помощью любого из поддерживаемых магазинов, установленных на устройстве. При наличии нескольких магазинов приложений, пользователю предоставят выбрать любое из имеющихся.

8.4. Удаление приложения из каталога

Для удаления приложения выполните следующие действия:

1. Перейдите в раздел **Приложения**.
2. Выберите в списке нужное приложение.
3. Нажмите кнопку . Откроется модальное окно подтверждения удаления приложения (см. рисунок 26).
4. Нажмите кнопку **Удалить**. Для отмены действия нажмите кнопку **Отмена**.

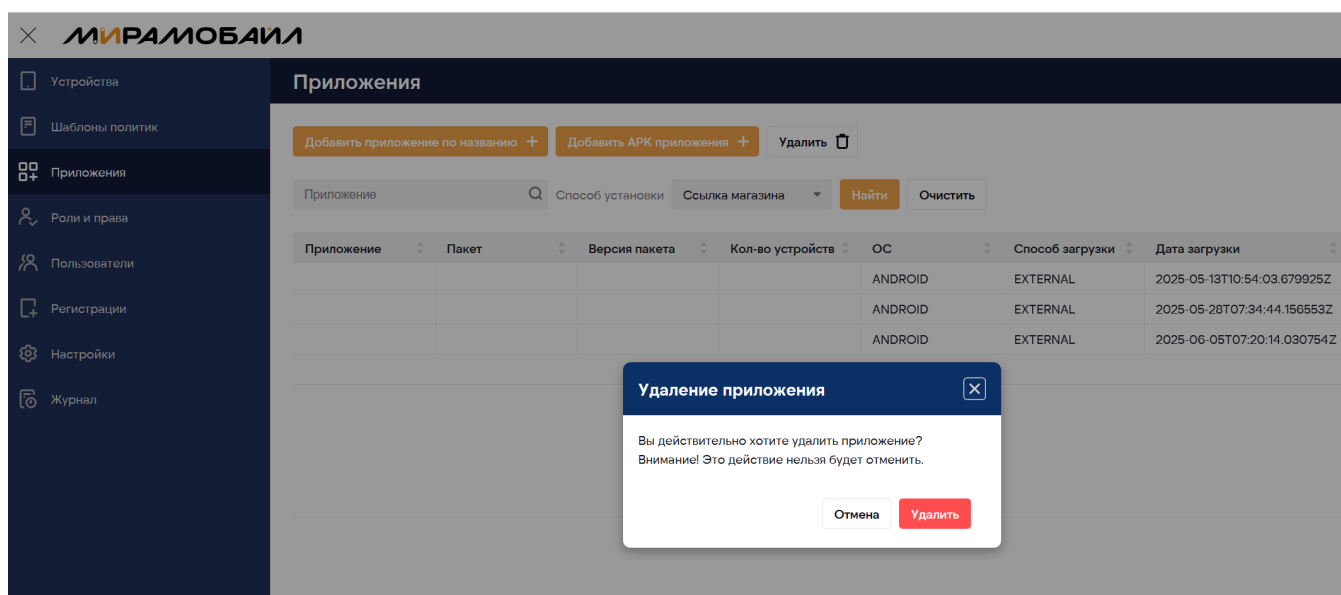


Рисунок 39 – Удаление приложения

8.5. Поиск приложения

Для нахождения нужного приложения из общего списка выполните следующие действия:

1. Перейдите в раздел **Приложения**.
2. Выберите способ установки по критериям (файл арк или ссылка магазина).
3. Нажмите кнопку **Найти**. На экране появится список приложений, соответствующих выбранным критериям.
4. Для очистки формы поиска используйте кнопку **Очистить**.

9. Раздел Роли и права

Раздел предназначен для централизованного управления доступом пользователей к функциональным возможностям системы. Он обеспечивает настройку и распределение уровней прав между администраторами и другими пользователями, позволяя гибко контролировать, кто и какие действия может выполнять в ключевых разделах комплекса — от управления устройствами и политиками до загрузки приложений и ведения журнала сервера, что гарантирует безопасность и структурированность администрирования, минимизируя риски несанкционированных изменений.

9.1. Главное окно раздела

Управление комплексом осуществляет «Главный администратор» комплекса, обладающий разными уровнями доступа к разделам и функциям.

Администратору с данной ролью доступны права на редактирование следующих разделов (см. рисунок 27):

- **Устройства;**
- **Шаблон политики;**
- **Загрузка приложений;**
- **Регистрация;**
- **Пользователи;**
- **Роли и права;**
- **Настройки;**
- **Журнал сервера.**

В перечисленных разделах администратор обладает максимальными правами: создание, редактирование, чтение, удаление всех элементов (см. таблицу 10).

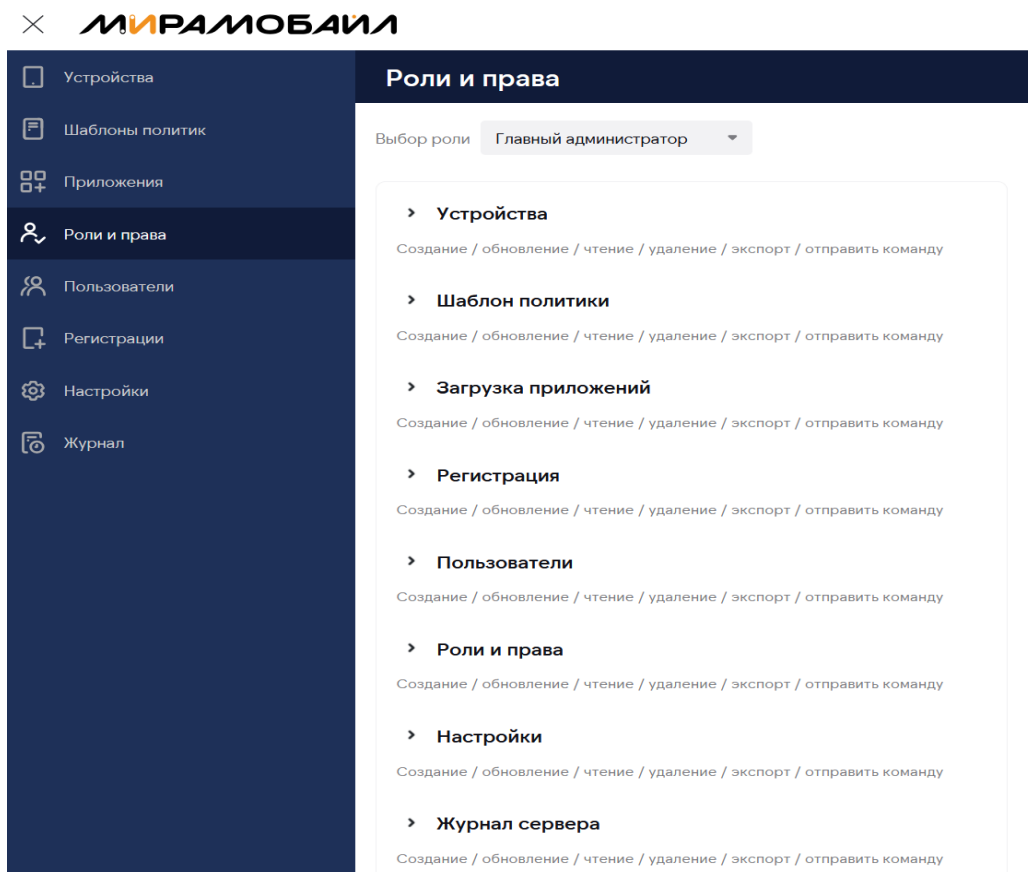


Рисунок 40 – Главное окно раздела Роли и Права

9.2. Описание ролей

Список ролей пользователей и ограничения описаны в таблице 10.

Таблица 11 – Основные роли пользователей и их права в системе

Роль	Функции	Ограничения
«Главный администратор»	Полный CRUD-доступ ко всем объектам и разделам системы (Устройства, Пользователи, Шаблоны политик, Роли и права, Настройки, Журнал и др.)	Максимальные права без ограничений; нельзя изменять собственные права; нет возможности создавать или удалять роли и права
«Аудитор»	Просмотр журнала сервера с полным доступом к событиям	Только чтение, без прав на создание или редактирование; разделы: Устройства, Пользователи, Шаблоны политик и др. скрыты в интерфейсе
«Администратор группы»	CRUD-доступ к устройствам, шаблонам политик и приложениям в пределах назначенной группы и вложенных структур; просмотр всех пользователей; создание, редактирование и удаление пользователей с ролью «Без роли»; просмотр назначенных прав (без изменения)	Управление ограничено назначенными группами и их вложенными структурами; нет прав на управление пользователями с ролями, отличными от «Без роли»; нет возможности создавать или изменять роли и права

Примечание – Настройки прав установлены по умолчанию после установки продукта. В процессе эксплуатации их можно корректировать в рамках предусмотренных системой возможностей. Создание или удаление ролей и прав в системе не предусмотрено.

9.3. Редактирование прав выбранной роли

Для редактирования прав для выбранной роли выполните следующие действия:

1. Выберите роль в главном окне.
2. Выберите роль из выпадающего списка ролей. Появится список разделов для редактирования прав с выбранной ролью.
3. Активируйте нужные переключатели (CRUD - создание, чтение, обновление, удаление для объектов). Изменения вступят в силу сразу.

Примечание – Изменять права можно только для тех ролей, у которых это предусмотрено.

10. Раздел Пользователи

Раздел предназначен для управления учётными записями пользователей системы, обеспечивая создание, редактирование, просмотр и удаление профилей с учётом ролей и атрибутов. Он служит основой для контроля доступа и разграничения прав в системе, позволяя задавать обязательные и необязательные параметры пользователей, а также устанавливать соответствующие роли, которые определяют уровень их полномочий.

Совет

При заполнении атрибутов пользователя соблюдайте следующие правила:

- для обязательного поля **Фамилия** используйте непустую строку (пробел допустим).
- в поле **e-mail** обязательно должен присутствовать символ «@», разделяющий строку на две непустые части; в левой части не допускается пробел; обе части могут содержать печатные символы из различных алфавитов;
- логин доступен для ввода только при роли, отличной от «Без роли», и должен быть непустым, может содержать произвольные символы;
- поля **Пароль** и **Подтверждение пароля** доступны при роли, отличной от «Без роли», должны быть непустыми, совпадать и содержать хотя бы один символ из латинского алфавита в нижнем регистре (a-z);
- атрибуты **Имя**, **Отчество**, **Должность**, **Подразделение**, **Телефон** и **Комментарий** являются необязательными и могут содержать произвольные строки;
- при выборе роли пользователя учитывайте, что она не может быть изменена при редактировании. Возможен выбор из всех ролей системы, включая «Без роли»;
- для роли «Администратор группы» на этапе создания отображается список управляемых групп (пустой и без возможности редактирования); название группы доступно для редактирования только при создании пользователя с этой ролью.

10.1. Главное окно раздела

Интерфейс отображает список пользователей с полями в табличном виде (см. рисунок 37):

- **ФИО** (Фамилия, Имя, Отчество);
- **Логин**;
- **Почта (e-mail)**;
- **Должность**;
- **Подразделение**;
- **Роль**.

ФИО	Логин	Почта	Должность	Подразделение	Роль
Иван Иванович Петров	admin	admin@mira-mobile.ru	Администратор	qwe	super_admins
Имя1 Отчество1 Пользаак1	admin1	admin1@mail.ru			auditors
Пользаак2	admin2	admin2@mail.ru			auditors
Иван Николаевич Корепин	ivankorepin	ivan.korepin@osinit.com	Всея менеджер	проектный офис	
Андрей Иванов	ivanov	ivanov@mail.ru			auditors
Дарья Петрова	kek	user1@mail.ru	DevOps		
Морозов	moroz	test@mail.ru	Тестировщик	Отдел тестирования	
qwe qwe qwe	qwerty123	qwe@aysdasd.com		qwe	group_admins
дима дима2 дима3	sosockol	chel@mail.ru	работяга	галера	
null null test	testtes1t	1asdwe@mail.com	test	test	

Рисунок 41 – Главное окно раздела Пользователи

Доступны фильтры и кнопки для действий.

Для навигации выполните следующие действия:

1. Перейдите на вкладку **Пользователи**.
2. Используйте кнопку  для поиска по ФИО, роли, должности или подразделения.
3. Выберите пользователя для просмотра, добавления, импорта, редактирования или удаления.

10.2. Просмотр списка пользователей

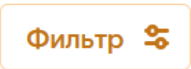
Для просмотра списка пользователей выполните следующие действия:

1. Перейдите на вкладку **Пользователи**. Система отобразит список всех зарегистрированных пользователей в соответствии с правами администратора в табличном виде (см. рисунок 32).

10.3. Фильтрация списка пользователей

Для фильтрации списка пользователей выполните следующие действия:

1. Перейдите на вкладку **Пользователи**. Система отобразит список всех зарегистрированных пользователей в соответствии с правами администратора в табличном виде (см. рисунок 27).

2. Нажмите кнопку . Появится форма поиска пользователя с дополнительными полями поиска.

3. Выберите/заполните необходимые критерии поиска (см. таблицу 11).

4. Нажмите кнопку **Найти**. На экране появится список пользователей, соответствующих выбранным критериям (см. рисунок 7). Для очистки содержимого в поле **Логин** используйте кнопку **Очистить**.

Таблица 12 – Критерии поиска пользователей

Наименование критерия	Описание влияния на поиск
Логин	Фильтрует пользователей по уникальному идентификатору в системе, что помогает быстро находить конкретного пользователя
Должность	Позволяет отобрать пользователей по занимаемой должности, что удобно для поиска сотрудников с определёнными обязанностями
Организационная единица	Фильтрует пользователей по подразделению или отделу, что облегчает поиск в больших организациях с несколькими филиалами
Роль	Позволяет выбрать пользователей по назначенной роли, что упрощает управление правами и доступом в системе

10.4. Добавление нового пользователя

Для добавления нового пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи**.
2. Нажмите кнопку **Добавить пользователя +**. Появится форма ввода данных о новом пользователе.
3. В отрывшейся форме заполните следующие поля (см. рисунок 29, таблица 11).
4. В правом нижнем углу нажмите кнопку **Применить**. Пользователь будет зарегистрирован, его имя появится в списке пользователей. Для отмены действия нажмите кнопку **Отмена** без сохранения внесённых изменений.

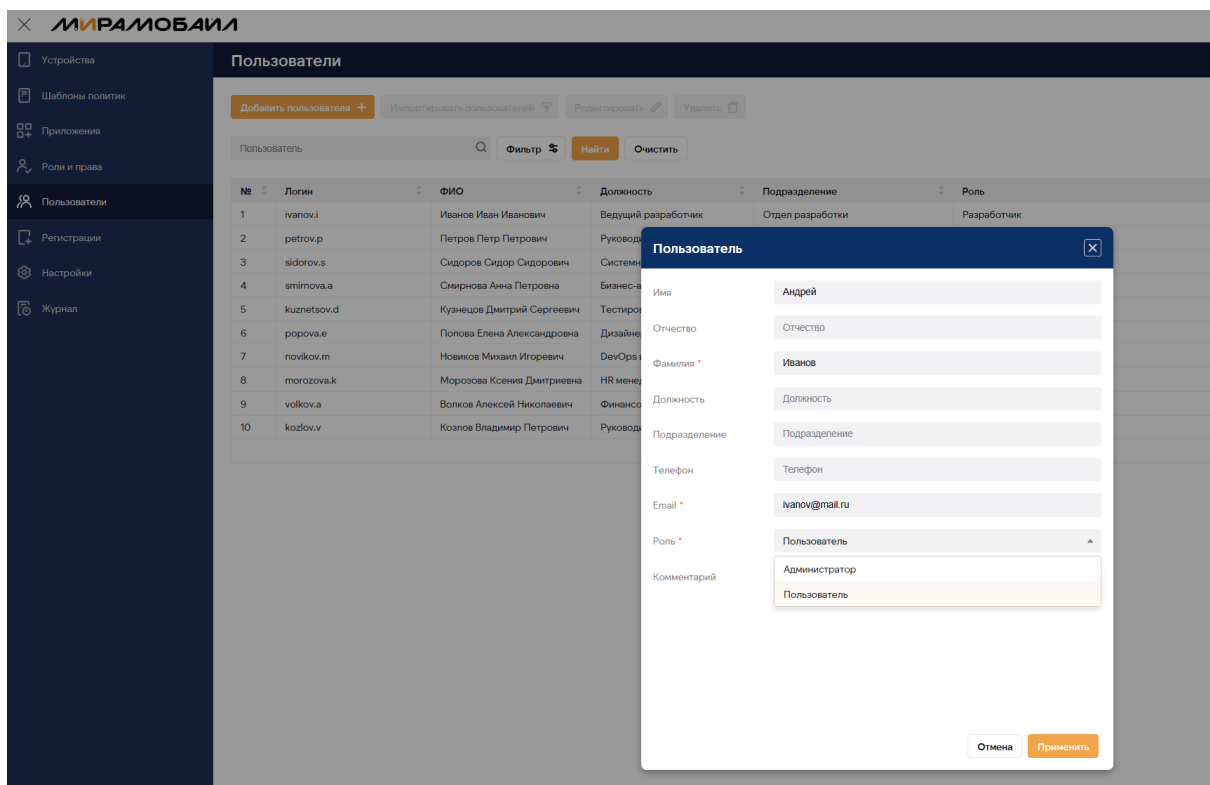


Рисунок 42 – Добавление нового пользователя

Таблица 13 – Параметры для регистрации пользователя

Поле	Обязательное поле	Описание	Пример заполнения
Имя		Имя пользователя	Иван
Отчество		Отчество пользователя	Сергеевич
Фамилия	✓	Фамилия пользователя	Иванов
Должность		Должность пользователя	Системный администратор
Подразделение		Подразделение или отдел пользователя	IT-отдел
Е-mail	✓	Электронная почта пользователя	ivanov@domain.ru
Телефон		Контактный телефон пользователя	+7 (999) 123-45-67
Роль	✓	Назначенная роль пользователя в системе	Администратор
Логин	✓	Уникальный идентификатор пользователя в системе	ivanov
Пароль	✓	Пароль для входа в систему	****
Повторить пароль	✓	Повтор пароля для подтверждения	****

Поле	Обязательное поле	Описание	Пример заполнения
Комментарий		Дополнительная информация или примечание	Новый сотрудник

10.5. Импорт новых пользователей

Функция позволяет импортировать сразу несколько пользователей из *.csv-файла. Для этого выполните следующие действия:

1. Перейдите в раздел **Пользователи**.
2. Нажмите кнопку **Импортировать пользователей**. Появится окно ввода параметров импорта.
3. Выберите *.csv-файл, в котором содержится информация о пользователях.
4. Выберите кодировку файла («utf8», «Cp1251», «koi8_r») и разделитель, который в нем используется.
5. Установите соответствие полей *.csv-файла и полей формы регистрации. Как и в случае с регистрацией одного пользователя обязательно должны быть заполнены поля **e-mail** и **Фамилия**.
6. Выберите роль пользователя.
7. Для создания привилегированного пользователя задайте логин, пароль и подтверждение пароля для входа в систему.
8. Нажмите кнопку **Ввод**. Пользователи будут зарегистрированы, их имена появятся в списке пользователей.

Если при импорте обнаружатся ошибки, например, дублирование адресов e-mail или несоответствие значений атрибутов, система уведомит администратора и предложит варианты действий: пропустить, заменить или остановить импорт.

Администратор может задать действие по умолчанию для всех конфликтов, чтобы ускорить процесс.

10.6. Изменение атрибутов пользователя

Для изменения атрибутов созданного пользователя выполните следующие действия:

1. Перейдите в раздел **Пользователи** (см. рисунок 30).

2. Выберите пользователя в списке и нажмите кнопку

Редактировать 

Откроется форма редактирования.

3. Вы можете изменить следующие атрибуты:

- Имя;
- Отчество;
- Фамилия – обязательное поле для заполнения;
- Должность;
- Подразделение;
- Телефон;
- E-mail – обязательное поле для заполнения;
- Логин – если он был введён при создании пользователя, его также можно изменить;
- Комментарий.

Примечание – атрибут **Роль** при редактировании изменить нельзя. Если роль пользователя — «Администратор группы»:

- отображается список групп, находящихся под его управлением;
 - при создании роль должна быть пустой и не подлежит редактированию.
4. Нажмите кнопку **Применить**. Подтвердите изменения после проверки корректности введённых данных системой.

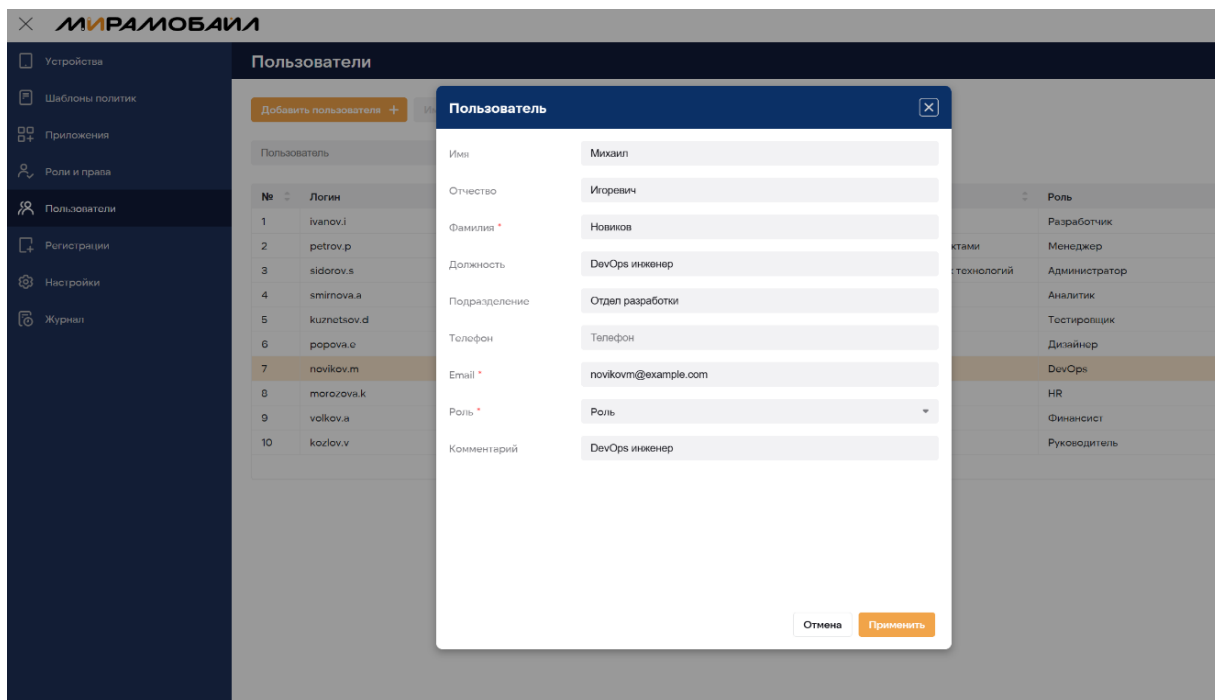


Рисунок 43 – Изменение атрибутов пользователей

10.7. Удаление пользователя

Для удаления пользователя выполните следующие действия:

1. Перейдите в раздел **Пользователи**.
2. Выберите пользователя для удаления.
3. Нажмите кнопку **Удалить** (см. рисунок 31). Для отмены действия нажмите кнопку **Отмена**. Подтвердите действие в окне подтверждения. Система проверит отсутствие у пользователя зарегистрированные устройства.

Примечание – Удаление пользователя, который является владельцем другого пользователя, может привести к ошибкам: роль меняется на «Без роли», но удаление не завершается. Удаление пользователя, который создал приглашения, назначил политики или загрузил приложения, может привести к сбросу роли до «Без роли» без полного удаления.

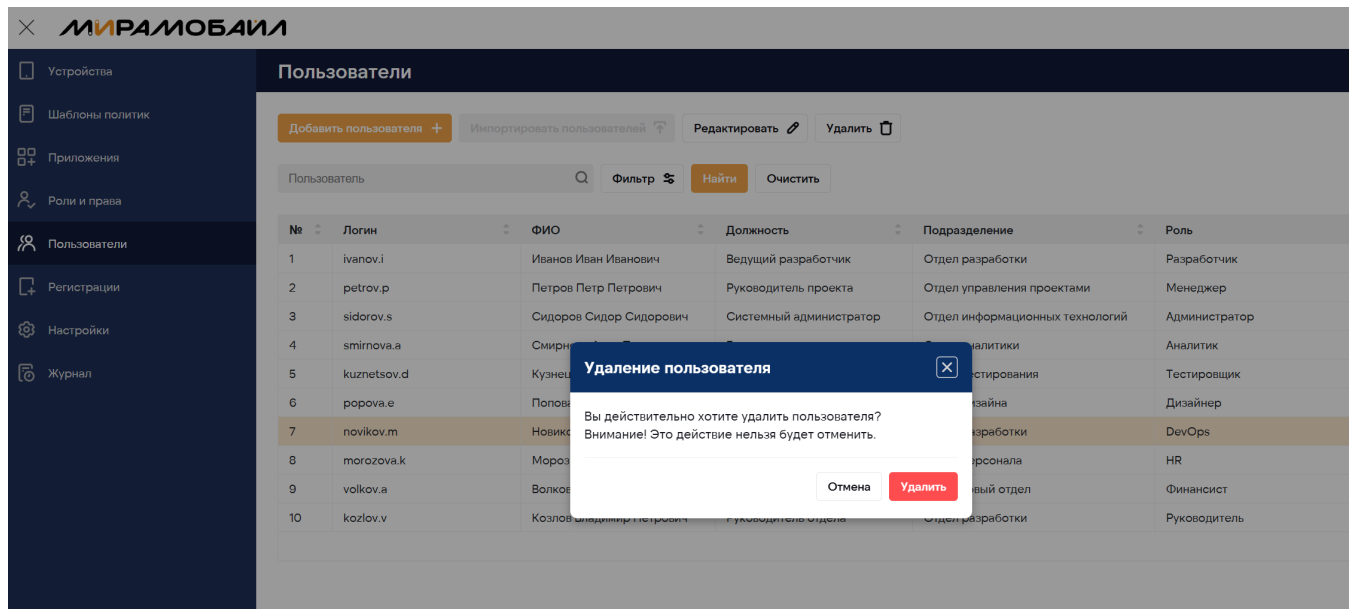


Рисунок 44 – Удаление пользователя

11. Раздел Регистрации

Раздел предназначен для эффективного управления процессом приглашения новых пользователей к регистрации в системе. В разделе доступны следующие возможности:

- создание нового приглашения на регистрацию: позволяет быстро сформировать индивидуальное приглашение для пользователя, указав необходимые данные. После создания приглашения пользователь получает ссылку или уведомление для самостоятельной регистрации;
- удаление (аннулирование) приглашения: обеспечивает удаление одного или нескольких выбранных приглашений из списка — например, если они утратили актуальность или были созданы по ошибке;
- удобный поиск: реализован поиск по фамилии пользователя, его должности, подразделению, что значительно облегчает работу с большим количеством приглашений и позволяет быстро находить нужные записи.

11.1. Окно главной страницы раздела

Окно отображает список приглашений по пользователям, доступным администратору (см. рисунок 32):

- **Имя** пользователя;
- **ФИО** пользователя;
- **Должность**;
- **Подразделение**;
- **Телефон**;
- **e-mail**;
- **Время окончания**.

Доступны действия: создание нового приглашения, удаление существующего, фильтрация по фамилии пользователя и переход в раздел **Устройства**.

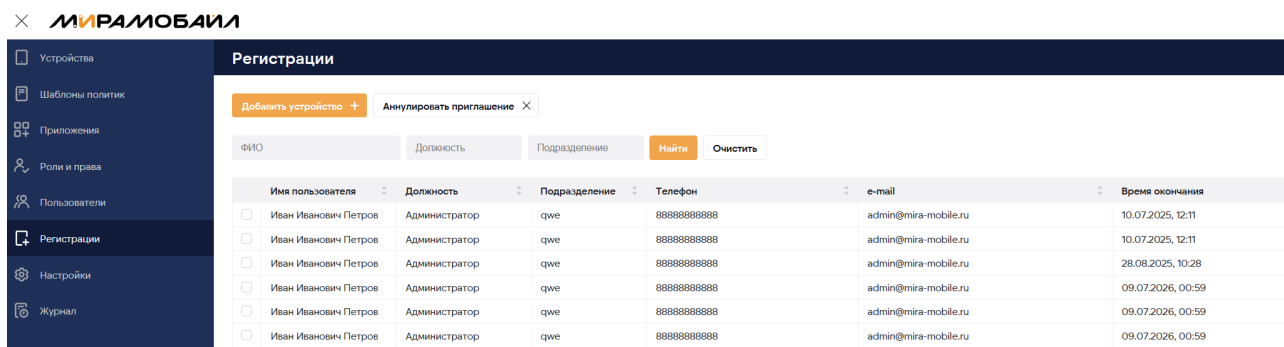


Рисунок 45 – Главное окно раздела Регистрации

11.2. Создание приглашения на регистрацию устройства

Для создания приглашения пользователя на регистрацию устройства выполните следующие действия:

1. Перейдите в раздел **Регистрации**.
2. Нажмите кнопку **Добавить устройство +**. Откроется модальное окно приглашения на регистрацию.
3. Выберите в списке пользователя/пользователей отметив чек-боксы напротив нужных записей. При необходимости можно воспользоваться фильтрацией по следующим параметрам:
 - ФИО пользователя;
 - Подразделение;
 - Должность.

Укажите время действия запроса на регистрацию в полях:

- Дата окончания срока действия приглашения;
- Время окончания.

4. Выберите тип владения устройством. Доступны два варианта использования для Android - устройств:

- корпоративное (COBO) — корпоративное устройство, предназначенное для рабочих задач. Реализуется, как правило,

установкой на сброшенное устройство в специальном режиме управления;

- личное (BYOD) — персональное устройство пользователя, используемое как для личных целей, так и для рабочих задач. Для реализации создаётся рабочий профиль на личном устройстве пользователя.

5. Выберите вариант отправки запроса на регистрацию. Доступны следующие варианты отправки:

- Отправить пользователям - выбранным для регистрации пользователям QR-код будет отправлен на e-mail, указанный при создании пользователя;
- Скачать - на ПК администратора будет загружен файл с QR-кодами для регистрации выбранных пользователей и краткой информацией о них;
- Отправить себе - QR-коды для регистрации выбранных пользователей будут отправлены на e-mail администратору, который создал запрос на регистрацию.

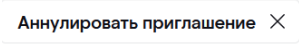
6. После выбора любого из доступных вариантов в списке запросов на регистрацию появятся новые записи с указанием срока окончания действия запроса.

Примечание – Отправить запрос на регистрацию можно также из раздела **Устройства**. Для этого необходимо нажать кнопку  на вкладке **Группы устройств**, в результате чего откроется то же самое модальное окно, что и при нажатии кнопки  в разделе **Регистрация**.

11.3. Аннулирование приглашения на регистрацию устройства

Для аннулирования приглашения на регистрацию устройства выполните следующие действия:

1. Перейдите в раздел **Регистрации**.
2. Выберите в списке запрос на регистрацию устройства.

3. Нажмите кнопку . Приглашение аннулируется автоматически.
4. Приходит оповещение в раздел **Устройства**, о том, что устройство успешно отозвано.

12. Раздел Настройки

Раздел предназначен для настройки параметров работы. В разделе содержится информация об используемой лицензии, списке паролей сервисного режима, предоставляется возможность загрузки лицензии.

Раздел содержит следующие вкладки (см. рисунок 33, таблица 12):

- **Лицензии;**
- **О программе;**
- **Пароли сервисного режима;**
- **Syslog - сервера.**

Чтобы ознакомиться с интерфейсом и выбрать группу для работы, выполните следующие действия:

1. Перейдите в раздел **Настройки**.
2. Выберите нужную вкладку для детального просмотра, например, **Лицензии** для управления лицензиями.
3. Используйте интерфейс для запуска действий, как указано в подразделах.

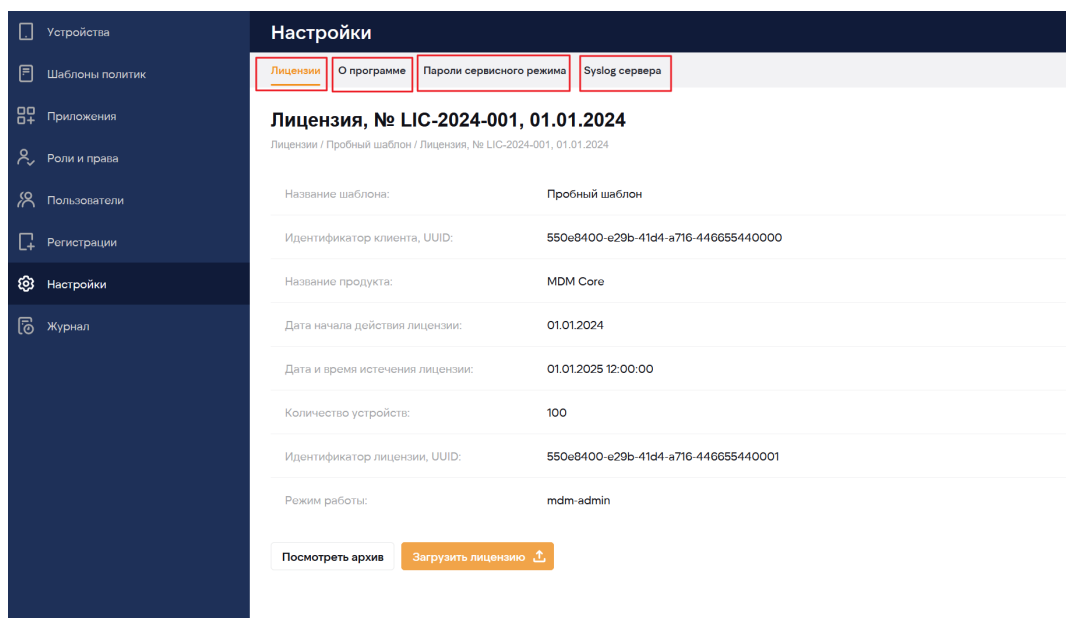


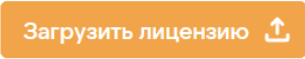
Рисунок 46 – Главное окно раздела Настройки

Таблица 14 – Описание вкладок

Вкладка	Назначение	Доступные действия
Лицензии	Просмотр информации о лицензии, загрузка новой лицензии	Просмотр, загрузка
О программе	Отображение сведений о версии и производителе программного обеспечения	Просмотр
Пароли сервисного режима	Управление списком паролей для сервисного режима	Просмотр, редактирование
Syslog-сервера	Настройка параметров и списка серверов для передачи системных журналов (Syslog)	Просмотр, редактирование, загрузка

12.1. Загрузка лицензии

Чтобы обновить или загрузить новую лицензию для системы, выполните следующие действия (см. рисунок 47):

1. Перейдите на вкладку **Лицензии** на главной странице.
2. Нажмите кнопку . Появится стандартный диалог работы с файлами с указанием Периода действия лицензии и количеством устройств.
3. Нажмите кнопку **Загрузка**.
4. Выберите файл с лицензией, расположенный на вашем ПК с расширением (*.lic) и нажмите кнопку **Открыть**. Система автоматически обновит лицензию.

Для отмены действия нажмите кнопку **Отмена**.

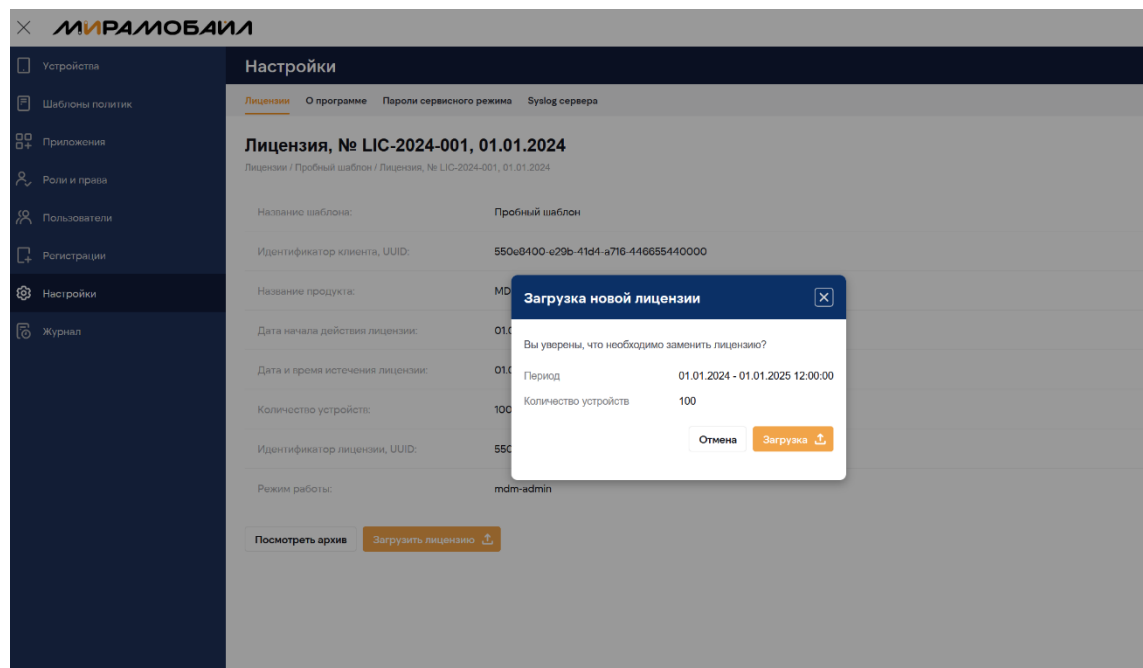


Рисунок 47 – Загрузка лицензий

12.2. Просмотр истории лицензий для mdm - сервера

Чтобы проанализировать историю лицензий и проверить изменения, выполните следующие действия:

1. Откройте вкладку **Лицензии**.

2. Нажмите кнопку **Посмотреть архив**. Система отобразит в табличном виде список лицензий, содержащий параметры (см. рисунок 48, таблица 15):

Для выхода из режима просмотра лицензий нажмите кнопку **<**.

Лицензии						
О программе Пароли сервисного режима Syslog сервера						
< Архив лицензий						
Идентификатор, №	Дата создания	Дата начала	Дата окончания	Количество устройств	Режим работы MDM-admin	
af43ca9f-aa5c-4f82-8562-d577bd7209e0	11.06.2025	16.06.2025	11.06.2026	701	Online	
5ea9a073-7ffe-478b-b190-35a1d36a46f0	12.05.2025	17.05.2025	12.05.2026	519	Online	

Рисунок 48 – Архив лицензий

Таблица 15 – Параметры лицензий

Параметр	Описание	Пример
Идентификатор, №	Уникальный номер лицензии	97d0ae21-ac73-4c12-8dae-f966b2d82f68
Дата создания	Дата создания лицензии	11.06.2025
Дата начала	Дата начала лицензионного периода в данной лицензии	16.06.2025
Дата окончания	Дата окончания лицензионного периода в данной лицензии	11.06.2026
Количество устройств	Ограничение на количество устройств по данной лицензии	701
Режим работы MDM-admin	Режим работы MDM - ONLINE или ISOLATION	ONLINE

Примечание – Атрибут лицензии «Режим работы MDM» может принимать два значения:

- ONLINE - для ситуации, когда MDM имеет возможность обращаться к серверам SOLID для актуализации лицензионного статуса, проверок ограничений лицензии
- ISOLATION - для ситуации, когда MDM не имеет возможности обращаться к серверам SOLID, все проверки производит самостоятельно

12.3. Вкладка О программе

Вкладка **О программе** отображает ключевую информацию о продукте и его компонентах (см. рисунок 36, таблица 14):

- список используемых компонентов системы с их версиями;
- копирайт приложения;
- версии MDM Server и MDM Клиент;
- ссылка для загрузки MDM агента в формате APK;
- контакт технической поддержки (Саппорт).

В настройках группы можно вручную изменить URL для загрузки MDM агента, указав нужную ссылку.

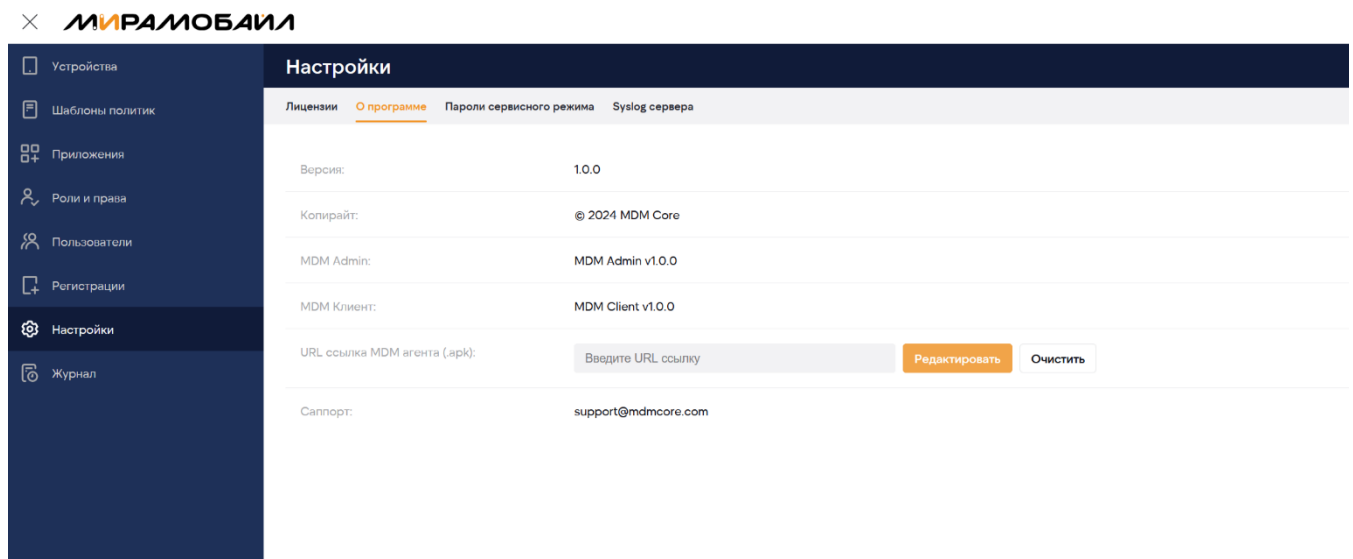


Рисунок 49 – Вкладка О программе

Таблица 16 – Основные сведения о программе и компонентах MDM

Поле	Как оформить	Комментарии
Версия	Текущая версия программного продукта (например, «1.0.0»)	Указывайте точную версию, желательно с датой выпуска
Копирайт	Информация об авторских правах (например, «© 2025 MDM Core»)	Используйте символ © и указывайте год и владельца

Поле	Как оформить	Комментарии
Администратор MDM	Версия административного модуля (например, «MDM Admin v1.0.0»)	Можно добавить дату сборки или релиза
MDM Клиент	Версия клиентского приложения (например, «MDM Client v1.0.0»)	Аналогично — версия и дата
URL-адрес агента MDM (.apk)	Прямая ссылка для скачивания APK-файла агента MDM	Укажите корректный URL, желательно с кнопкой для копирования или скачивания
Саппорт	Контактная информация службы поддержки (электронная почта, телефон, чат)	Добавьте несколько способов связи, часы работы

Для редактирования поля URL-адрес агента MDM (.apk) нажмите на кнопку **Редактировать**.

Для очистки формы поиска URL-адреса используйте кнопку **Очистить**.

12.4. Пароли сервисного режима

На вкладке **Пароли сервисного режима** отображен список всех известных паролей сервисного режима. Для каждого устройства в списке создаётся отдельная запись, содержащая (см. рисунок 37):

- UUID устройства;
- автоматически сгенерированный пароль сервисного режима;
- дату создания пароля.

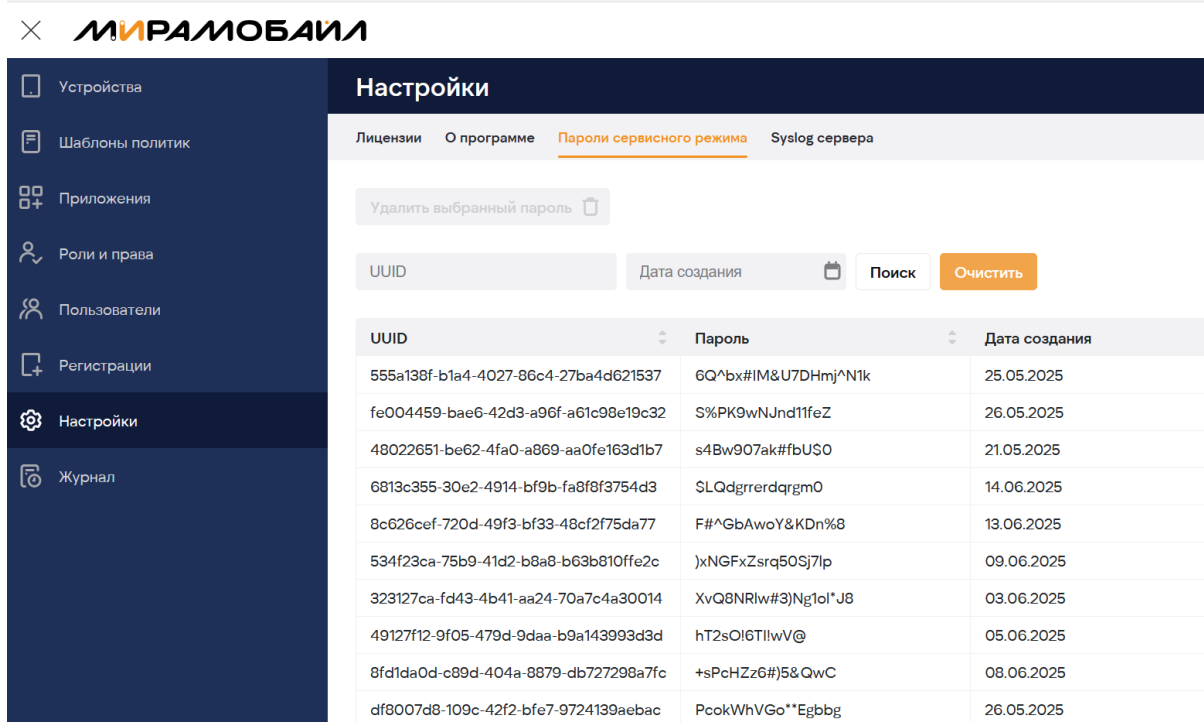


Рисунок 50 – Вкладка Пароли сервисного режима

Примечание – В системе не осуществляется проверка наличия устройства — возможно, устройство уже было удалено, однако пароль остается в списке. Если устройство с одним и тем же UUID регистрировалось несколько раз, пароль будет одинаковым. Если UUID устройства менялся, пароль будет соответствовать текущему UUID устройства.

Интерфейс предоставляет пользователю следующие возможности:

- фильтрация списка по UUID устройства (поиск введенной подстроки с начала UUID);
- фильтрация по точной дате создания пароля;
- очистка всех установленных фильтров;
- удаление выбранного пароля сервисного режима из списка.

Поиск пароля сервисного режима

Чтобы найти пароль сервисного режима и получить доступ к определённому устройству, выполните следующие действия:

1. Откройте вкладку **Пароли сервисного режима** на главной странице.
2. Введите параметры фильтрации (см. рисунок 38):

- UUID устройства;
- Дату создания.

3. Нажмите кнопку **Поиск**. Система отобразит пароль.

Для удаления параметров поиска нажмите кнопку **Очистить**.

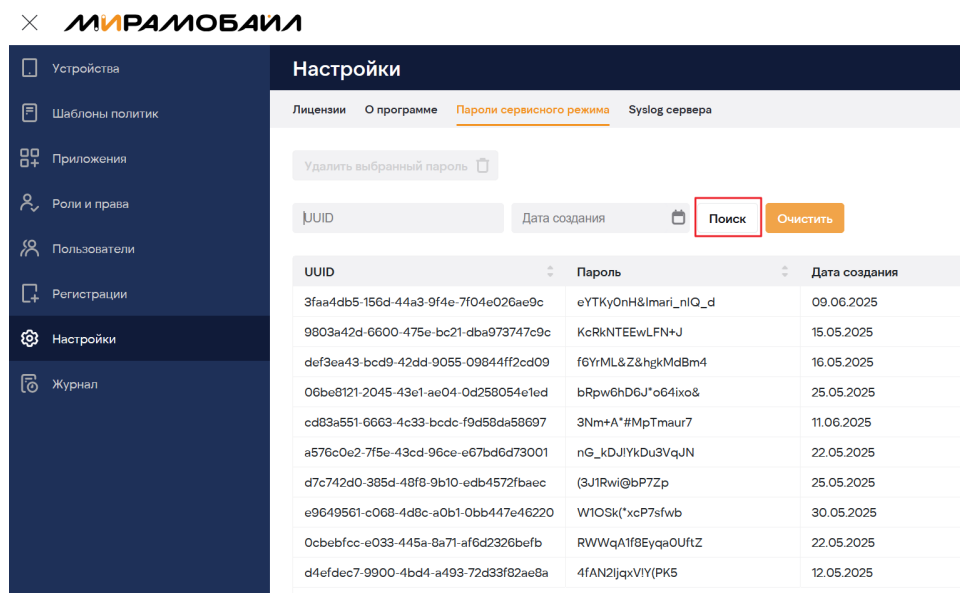


Рисунок 51 – Поиск пароля сервисного режима

Удаление пароля сервисного режима

Чтобы удалить пароль сервисного режима выполните следующие действия:

1. Откройте вкладку **Пароли сервисного режима** на главной странице.
2. Выберите устройство для которого требуется удалить пароль.
3. Нажмите кнопку . Появится модальное окно с сообщением (см. рисунок 39).
4. Нажмите кнопку **Удалить**.

Для отмены действия нажмите кнопку **Отмена**.

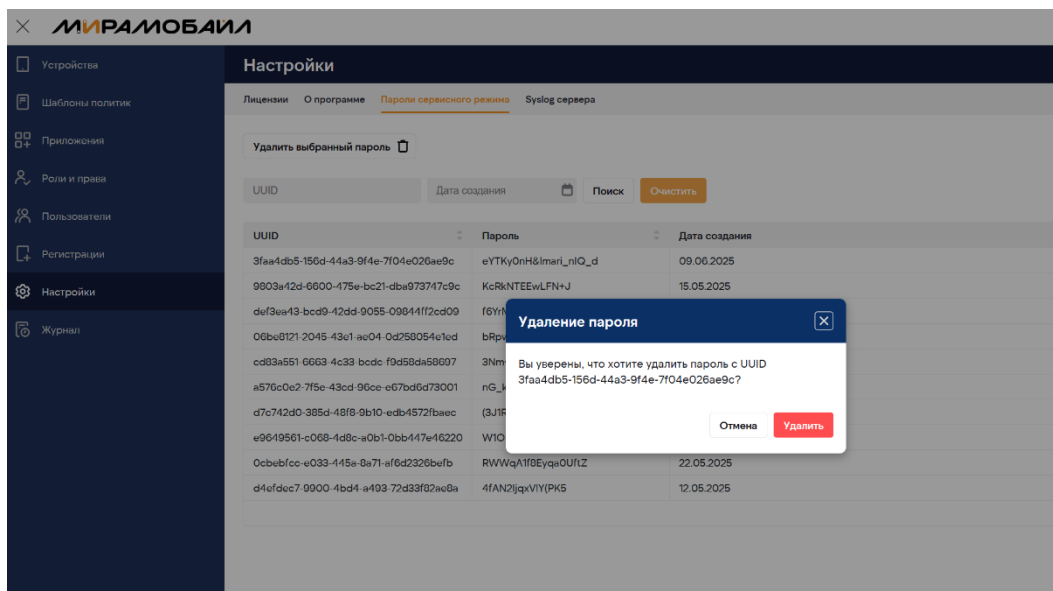


Рисунок 52 – Удаление пароля сервисного режима

12.5. Вкладка syslog - сервера

На вкладке **syslog сервер** отображен список настроенных серверов для приёма syslog-сообщений. Для каждого сервера отображаются следующие параметры: название, IP-адрес, порт, используемый протокол и минимальный уровень severity level для сообщений, при котором сообщения будут отправляться на данный сервер.

Добавление syslog-сервера

Чтобы добавить syslog - сервер выполните следующие действия (см. рисунок 53):

1. Перейдите на вкладку **syslog сервер**.
2. Нажмите кнопку **Добавить сервер +**. Отобразится окно.
3. Заполните поля формы:
 - Название сервера;
 - IP-адрес сервера;
 - Порт сервера;
 - Протокол (TCP/UDP);

- Минимальный уровень значения severity, которые будут отображены для отправки.
4. Нажмите кнопку **Применить изменения** для сохранения настроек.

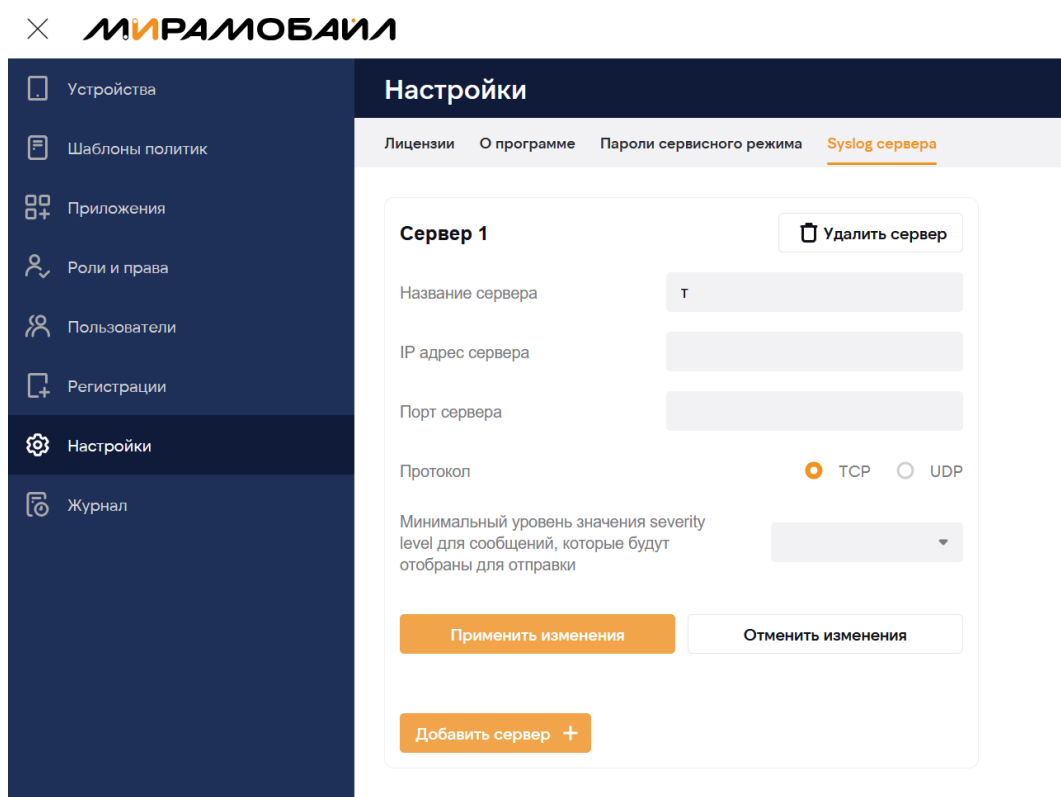


Рисунок 53 – Добавление syslog - сервера

Удаление syslog-сервера

Для удаления syslog - сервера выполните следующие действия:

1. Выберите нужный сервер в списке и нажмите кнопку  **Удалить сервер**.
2. Появится модальное окно (см. рисунок 41).
2. Нажмите кнопку **Удалить** для подтверждения удаления. Для отмены действия нажмите кнопку **Отмена**.

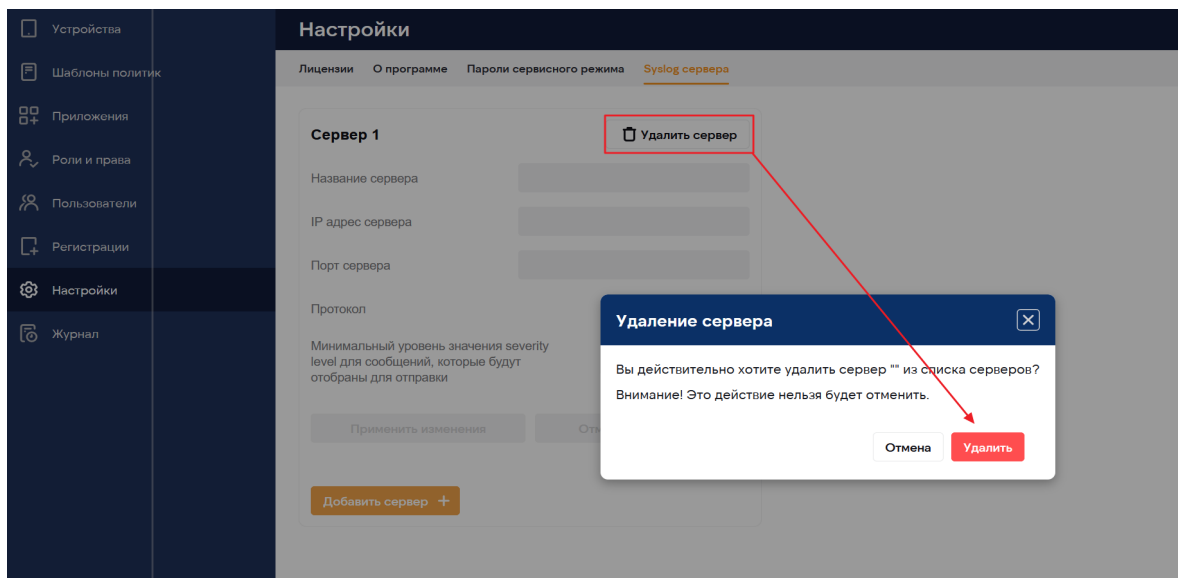


Рисунок 54 – Удаление syslog – сервера

13. Раздел Журнал

Раздел предназначен для централизованного ведения и анализа событий, происходящих в системе. Он позволяет администраторам контролировать и отслеживать все важные действия и изменения, фиксируемые системой, обеспечивая прозрачность и безопасность работы.

«Администратор» может:

- просматривать полный список событий, отсортированных в хронологическом порядке от более поздних к более ранним;
- анализировать события по следующим параметрам: важность, тип, дата и время, пользователь, инициировавший событие, а также связанное устройство;
- использовать фильтры для быстрого поиска нужных записей по типу события, пользователю, дате, ID устройства, тексту и важности события;
- выгружать журнал событий для внешнего анализа;
- удалять все записи журнала при необходимости.

Примечание – Все действия в разделе — поиск событий, просмотр, выгрузка и удаление всех записей журнала — выполняются пользователями, прошедшими аутентификацию в системе и обладающими соответствующими правами доступа.

13.1. Главная страница раздела Журналы

Окно отображает список событий, отсортированных по времени от более поздних к более ранним в хронологическом порядке. Для каждого события фиксируются:

- **Событие;**
- **Важность** (Критическое, Информация, Предупреждение) (см. рисунок 51, таблица 15);
- **Время события/дата;**

- Тип события;
- Пользователь;
- ID пользователя, инициирующего событие.
- ID устройства.

Доступны фильтры по атрибутам:

- Тип события;
- Пользователь;
- Дата события;
- ID устройства,
- Текст события;
- Важность события.

Дополнительно доступны функции:

- Сброс используемых фильтров;
- Выгрузка журнала сервера;
- Удаление журнала сервера.

Событие	Важность	Время события / дата	Тип события	Пользователь	ID пользователя	ID устройства
Сгенерирован сервисный пароль для устройства.	INFO	14:47 19.06.2025	AGENT_PASSWORD_CHANGED			8a93286f-d040-4830-200b-fbd38ff6cc00
Сгенерирован сервисный пароль для устройства.	INFO	17:06 23.06.2025	AGENT_PASSWORD_CHANGED			95ae8906-532d-c5a3-ae2-16a048e65866
Сгенерирован сервисный пароль для устройства.	INFO	11:46 24.06.2025	AGENT_PASSWORD_CHANGED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	12:24 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	12:24 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	12:24 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	15:47 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	15:47 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство отключено	INFO	16:03 25.06.2025	DEVICE_DISCONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	16:15 25.06.2025	DEVICE_CONNECTED			6176bfb8-e7b5-27c4-ab43-26b6c46d0882
Устройство подключено	INFO	16:30 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	16:30 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	16:43 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство отключено	INFO	16:45 25.06.2025	DEVICE_DISCONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	16:50 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство отключено	INFO	16:55 25.06.2025	DEVICE_DISCONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство подключено	INFO	16:55 25.06.2025	DEVICE_CONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a
Устройство отключено	INFO	17:32 25.06.2025	DEVICE_DISCONNECTED			e4a1a1e6-3946-8648-85de-c8e870ad95a

Рисунок 55 – Главное окно раздела Журнал

Таблица 17 – Регистрация событий в журнале сервера (успешные и неуспешные)

Важность события	Тип события	Текст события	Когда записывается
Информация	auth request	Приглашения на регистрацию отправлены:	При успешной отправке приглашения на регистрацию
Критическое событие	auth request	Ошибка при отправке приглашений на регистрацию:	При возникновении ошибок в процессе отправки приглашения на регистрацию
Информация	user import	Импортировано {X} пользователей из {Y}	При импорте пользователей
Предупреждение	Device authorization	The device is not registered in system	При попытке подключения неавторизованного устройства
Информация	Device authorization	The device has been authorized successfully	При успешной авторизации устройства
Информация	Device connected	The device has been connected successfully	При успешном подключении устройства к серверу
Информация	Device connected	The device has been disconnected successfully	При отключении устройства от сервера
Информация	Apply policy template	Лог применения шаблона политики безопасности в формате XML	При успешном применении шаблона политики
Предупреждение	Change rules on device / device group	%Administrator.login% changed rules on {device %Device.UDID%. device group %DeviceGroup.Name%} %Change.List%	Изменение напрямую назначенных на устройство или группу устройств правил безопасности
Предупреждение	The rule was set as mandatory	%Administrator.login% has changed the "mandatory" attribute on the rule %Rule.name% that is assigned to the {device %Device.UDID% device group %DeviceGroup.Name%}	Администратор изменил признак «суперприоритетное» на определенном правиле устройства или группы устройств
Предупреждение	Service Password was erased	%Administrator.login% erased service password for device %Device.Name%	Администратор удаляет пароль сервисного режима для устройства

Важность события	Тип события	Текст события	Когда записывается
Предупреждение	Service Password was changed	%Administrator.login% has generated new service password for device %Device.Name%	Администратор запросил генерацию нового пароля сервисного режима для устройства
Предупреждение	Unknown UDID	DeviceLocationJournal	-
Предупреждение	login failed	The user 'user_name' has not been registered in system. Host: 'host'	При попытке авторизации в консоли администратора незарегистрированного пользователя
Предупреждение	login failed	Invalid 'user.e_mail' user password. Host: 'host'	При вводе неправильного пароля во время авторизации в консоли администратора
Информация	login	User with id - 'userId' and email - 'user.e_mail', logged on successfully. Host: 'host'	При успешной авторизации пользователя в консоли администратора
Информация	logoff	User with id - 'userId' and email - 'user.e_mail', logged out. Host: 'host'	При выходе пользователя из консоли администратора
Предупреждение	log cleared	The log has been cleared by 'user.e_mail'	При очистке журнала сервера администратором
Информация	user edit	The user 'user.e_mail' phone number has been changed by 'user.e_mail'	При смене номера телефона пользователя
Информация	policy delete	The policy template 'название шаблона политики' has been deleted by 'user.e_mail'	При удалении шаблона политики
Информация	policy add	The policy template 'название шаблона политики' has been added by 'user.e_mail'	При добавлении шаблона политики
Информация	policy edit	The policy template 'название шаблона политики' has been modified by 'user.e_mail'	При изменении шаблона политики
Информация	password	The user 'user.e_mail' password has been changed successfully	При успешной смене пароля пользователем
Информация	user add	The user 'user.e_mail' has been added by 'user.e_mail'	При создании нового пользователя
Информация	Email changed	The user email 'старый email' changed to 'новый email'	При изменении email-адреса пользователя
Информация	user edit	The user 'user.e_mail' data have been modified by 'user.e_mail'	При изменении данных пользователя

Важность события	Тип события	Текст события	Когда записывается
Информация	user delete	The user 'user.e_mail' has been deleted by 'user.e_mail'	При удалении пользователя

13.2. Поиск события из общего списка

Чтобы ознакомиться с журналом и применить фильтры для поиска нужных записей, выполните следующие действия:

1. Перейдите в раздел **Журналы**.
 2. Нажмите кнопку . Появится форма заполнения журнала событий со следующими критериями:
 - Тип события;
 - Важность события;
 - Пользователь;
 - Текст события;
 - ID устройства;
 - Дата события от;
 - Дата события до.
 3. Нажмите кнопку **Найти**. Появится найденный список событий.
- Для удаления параметров поиска нажмите кнопку **Очистить**.
- Для возврата к хронологическому типу записей обновите страницу.

13.3. Выгрузка журнала сервера

Чтобы выгрузить события сервера в виде файла выполните следующие действия:

1. Откройте раздел **Журнал** (см. рисунок 43).
2. Выберите один из критериев события.
3. Нажмите кнопку  в верхнем левом углу. Автоматически начнётся скачивание журнала в формате *.csv (см. таблицу 16).

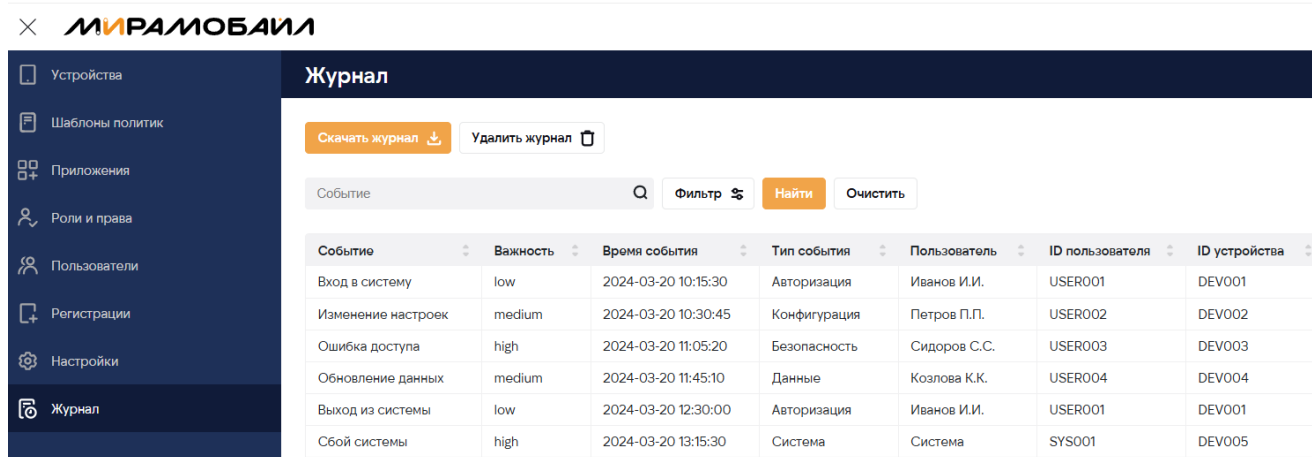


Рисунок 56 – Выгрузка журнала

Таблица 18 – Формат файла экспорта журналов сервера

Формат	Описание	Содержимое файла
csv - файл	Разделитель — точка с запятой	Таблица с атрибутами и экранированными символами

13.4. Удаление записей событий из журнала

Чтобы очистить записи журнала выполните следующие действия:

1. Откройте раздел **Журнал** (см. рисунок 44).
2. Выберите Тип события.
3. Нажмите кнопку . Появится модальное окно.
4. Нажмите кнопку **Удалить**. Система удалит все записи журналов. Для отмены действия нажмите кнопку **Отмена**.

Если администратор отклонит удаление, система вернётся к предыдущему интерфейсу без изменений.

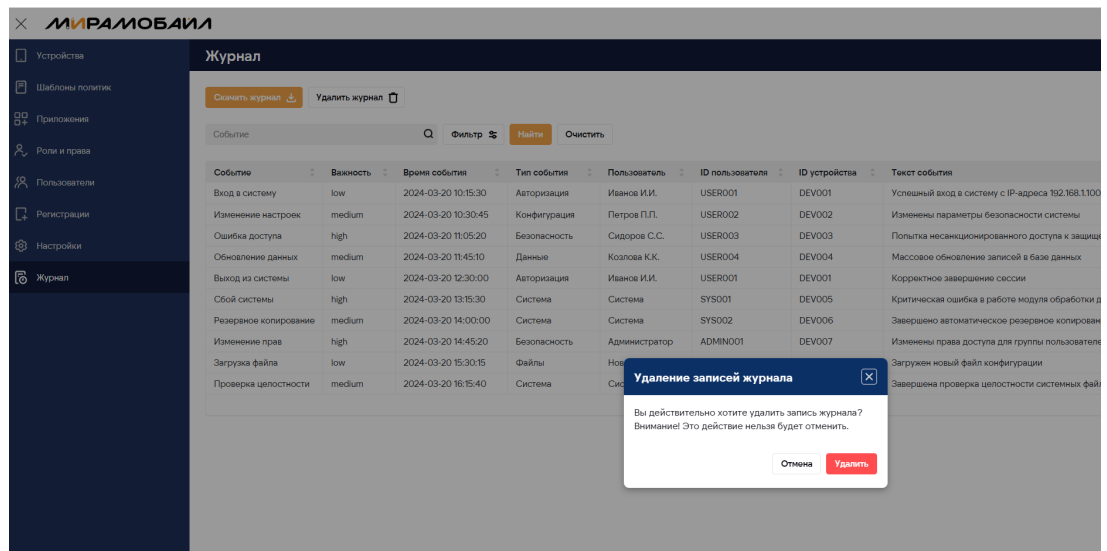


Рисунок 57 – Удаление записи журнала

14. Аварийные ситуации

При возникновении сбоев в аппаратном обеспечении, включая аварийное отключение электропитания, программный комплекс автоматически восстанавливает свою работоспособность после устранения сбоев и корректного перезапуска аппаратного обеспечения (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом). Программное обеспечение комплекса обеспечивает корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях комплекс выдает пользователю соответствующие аварийные сообщения, после чего возвращается в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Приложения

Приложение 1: Список правил

Белый список Wi-Fi точек

Данное правило устанавливает для устройств список точек доступа Wi-Fi, к которым разрешено подключение. Подключение к точкам вне списка будет заблокировано.

Для добавления в список Wi-Fi-точки необходимо внести SSID точки доступа.

Блокировка при смене SIM

Данное правило настраивает автоматическую блокировку устройства при смене SIM-карты. Если SIM-карта будет заменена, устройству будет отправлена команда «Блокировать устройство», что предотвращает несанкционированное использование.

Для активации данной функции необходимо установить параметр «Блокировка устройства при смене SIM-карты» в значение «Запретить». По умолчанию эта настройка включена («Запретить»).

Все разрешения приложениям

Данное правило управляет автоматическим предоставлением разрешений приложениям на устройстве.

Если параметр установлен в значение «Разрешить», все приложения автоматически получают все запрашиваемые разрешения без необходимости дополнительного подтверждения пользователя. Это упрощает работу приложений и ускоряет их установку.

Если параметр установлен в значение «Запретить», приложениям автоматически отзываются все ранее запрошенные разрешения, что может ограничить их функциональность или привести к некорректной работе.

Возможность удаления приложений

Данное правило позволяет или запрещает пользователю самостоятельное удаление приложений.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Встроенный браузер

Данное правило ограничивает использование браузеров на устройстве.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Журнал событий

Данное правило устанавливает срок хранения записей в журнале событий устройства и позволяет осуществлять отправку журналов событий.

Под сроком хранения записей журнала понимается период времени, в течение которого будут сохраняться события в журнале. Если период хранения не установлен, то события не удаляются, политика не отображается на устройстве.

По умолчанию параметр находится в режиме «Не установлен».

Доступные варианты настройки срока хранения:

- «Не установлен»;
- 1 день;
- 3 дня;
- 1 неделя.

Запрет скриншотов

Данное правило позволяет управлять правом пользователя осуществлять снимок или запись экрана.

Для настройки необходимо установить параметр «Запрет скриншотов» в значение «Запретить» или «Разрешить». По умолчанию параметр не задан.

Зашифровать устройство

Данное правило обязывает пользователя зашифровать все данные на мобильном устройстве.

Использование Bluetooth

Данное правило разрешает или запрещает использование Bluetooth на устройстве.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование NFC

Данное правило регулирует использование технологии NFC на устройстве пользователя.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование SMS

Данное правило ограничивает доступ пользователю к приложению для отправки SMS-сообщений, в том числе и установленных в Кнох-контейнере. Кроме того, блокируется получение входящих смс.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование VPN

Данное правило ограничивает использование VPN на устройстве.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование Wi-Fi

Данное правило разрешает или запрещает использование на устройстве пользователя технологии Wi-Fi, а также регламентирует ее принудительное включение.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование звукозаписи

Данное правило позволяет администратору управлять микрофоном мобильного устройства пользователя. Если включен запрет на использование микрофона, то им будет невозможно пользоваться из сторонних приложений.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Использование камеры

Данное правило позволяет заблокировать доступ пользователю к камере мобильного устройства из приложения «**Камера**» и из сторонних приложений, в том числе установленных в Кнох-контейнере. При попытке разрешить доступ к камере с помощью настроек в разделе **Журнал** будет зарегистрировано соответствующее событие.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Межпрофильный буфер обмена

Данное правило настраивает возможность вставки данных из рабочего профиля в личный профиль устройства (но не наоборот). Это обеспечивает контроль за обменом информации между профилями и повышает безопасность данных.

Для активации функции необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Мобильная точка доступа

Данное правило ограничивает использование на устройстве мобильной точки доступа.

Для активации функции необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Мобильные данные

Данное правило ограничивает передачу данных с использованием протоколов 3G/4G.

Для активации функции необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Настройка Proxy

Данное правило устанавливает настройки глобального HTTP-proxy для всех точек доступа Wi-Fi. Если для какой-то из точек доступа HTTP-proxy был настроен ранее, он не будет заменен. Если какая-то из точек доступа, открытая для подключения, будет удалена пользователем, при следующей попытке подключения к сети она будет автоматически восстановлена, и HTTP-трафик будет проходить с использованием заданного Proxy-сервера.

Параметры настройки:

- Включить глобальный прокси - выбор «Да» или «Нет». Значение по умолчанию - «Нет»;
- Адрес;
- Порт;
- Имя;
- Пароль.

Настройка Wi-Fi точек

Данное правило добавляет конкретные точки доступа Wi-Fi на устройстве или изменяет их настройки, а также позволяет удалить настройки указанных точек доступа Wi-Fi.

Для добавления **Wi-Fi** точки выполните следующие действия:

1. Откройте раздел настройки Wi-Fi точек в приложении или панели администратора (в зависимости от интерфейса).
2. В списке Wi-Fi точек нажмите кнопку **Добавить**. По умолчанию список пустой.
3. Заполните обязательные и дополнительные поля для новой точки (см. таблицу ...).
4. Проверьте введенные данные.
5. Сохраните изменения — новая Wi-Fi точка будет добавлена в список.

Рисунок 58 – Добавление Wi-Fi точки

Поле	Описание	Тип	Обязательность	Значение по умолчанию
SSID сети Wi-Fi	Идентификатор Wi-Fi сети (название сети)	Текстовое	Обязательное	Пустое
Действие	Выберите действие с точкой: добавить или удалить	Выпадающий список («Добавить», «Удалить»)	Обязательное	«Добавить»
Пароль	Пароль для подключения к Wi-Fi сети	Текстовое	Необязательное	Пустое
Адрес Proxy	Адрес прокси-сервера, если используется	Текстовое	Необязательное	Пустое
Порт Proxy	Порт прокси-сервера	Текстовое	Необязательное	Пустое
Тип авторизации	Тип шифрования Wi-Fi сети (без шифрования, WEP, WPA)	Выпадающий список («Нет», «WEP», «WPA»)	Необязательное	«Нет»

Настройка почты Exchange

Данное правило применяется для устройств с (установленной) ОС Android производства Samsung и определяет настройки почтового клиента, установленного на устройстве.

После применения правила на устройство пользователя поступят сообщение об обновлении настроек почтового аккаунта Exchange и предложение о настройке учетной записи пользователя.

Правило состоит из следующих обязательных параметров:

- домен;
- адрес сервера.

Примечание – Также в правиле безопасности передаются следующие параметры, которые зависят от владельца системы:

- почтовый адрес. Берётся из учётной записи владельца устройства,
- атрибут «easUser» берётся как часть почтового адреса от начала до символа @.

Осуществление звонков

Данное правило управляет возможностью пользователя использовать функции звонков из приложения «Телефон» и из сторонних приложений, включая установленные в Knox-контейнере.

Для разрешения или запрета функции необходимо установить параметр **Осуществление звонков** в значение «Разрешить» или «Запретить». По умолчанию функция отключена («Запретить»).

Используется на платформе Android, включая устройства с поддержкой Samsung Knox, где возможно дополнительное управление звонками через корпоративные политики.

Отладка по USB

Данное правило ограничивает отладку устройства по USB.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Пароль и блокировка

Данное правило устанавливает минимальные требования к паролям и определяет порядок блокировки устройства пользователя. Пользователь имеет возможность использовать более стойкий пароль, чем предписано политикой.

Информация об обновлении парольной политики отображается в журнале на устройстве пользователя. Текущие значения парольной политики на устройстве приводятся в разделе **Настройки → Пароли сервисного режима**.

Политика паролей состоит из следующих параметров (см. рисунок 59):

- Тайм-аут экрана — период неактивности пользователя, по истечении которого экран будет выключен и заблокирован;
- Срок действия пароля — период действия пароля на устройстве. По истечении срока действия необходимо сменить пароль;
- Тип пароля — символьный или цифровой;
- Длина истории пароля — новый пароль проверяется на совпадение с указанным числом предыдущих паролей;
- Количество ошибок пароля — количество ошибок ввода пароля перед принудительной блокировкой устройства (по умолчанию 5 шт).

Рисунок 59 – Политика Пароль и блокировка

Передача данных по USB

Данное правило ограничивает передачу с устройства данных по USB. При применении этого правила при подключении устройства по USB передача файлов будет недоступна.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Право установки приложений

Данное правило безопасности управляет правом пользователя самостоятельно устанавливать приложения на устройство, включая возможность установки из неизвестных источников.

Для настройки правила безопасности необходимо задать следующие параметры (см. рисунок 60):

- Право установки приложений — установите значение «Разрешить» или «Запретить», чтобы включить или отключить возможность установки приложений пользователем;
- Установка приложений из неизвестных источников — установите значение «Разрешить» или «Запретить», чтобы разрешить или запретить установку приложений вне официальных магазинов (например, из сторонних источников).

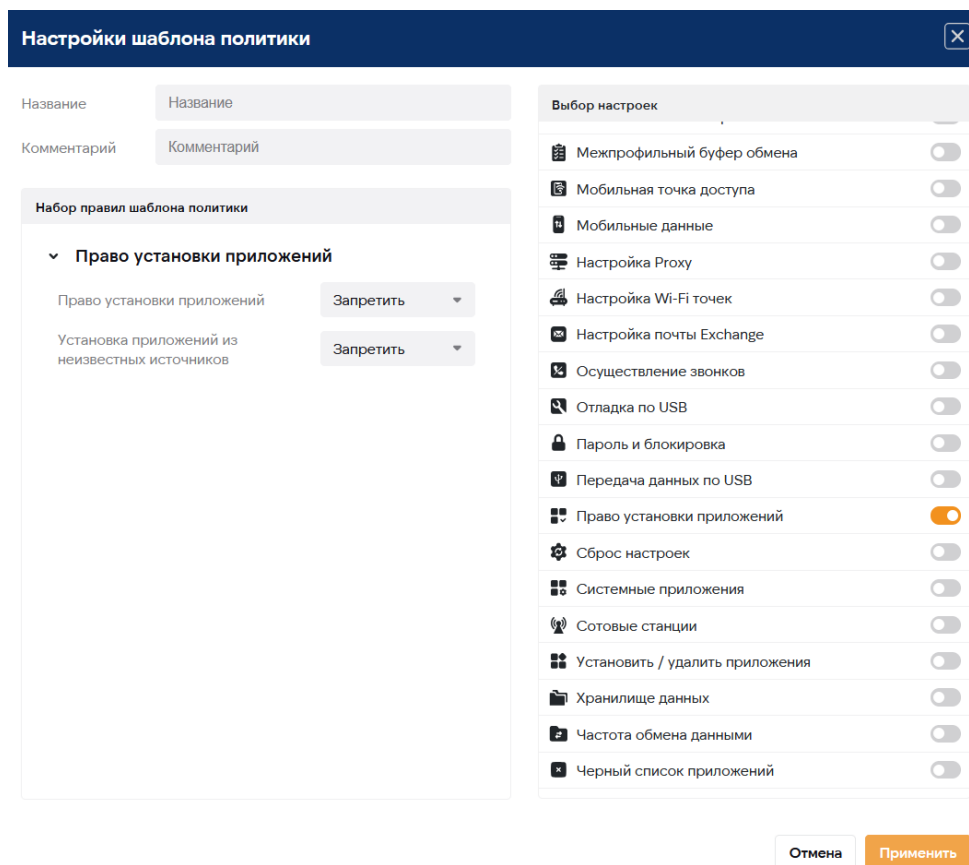


Рисунок 60 – Политика Право установки приложений

Сброс настроек

Данное правило ограничивает возможность сброса устройства к заводским настройкам. При попытке выполнить сброс настроек в журнале безопасности будет зарегистрировано соответствующее событие.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Системные приложения

Данная политика позволяет включить отображение всех доступных системных приложений для пользователя на устройстве. Это обеспечивает доступ к предустановленным системным приложениям, которые обычно скрыты от пользователя.

Для активации функции необходимо установить параметр «Системные приложения» в значение «Разрешить». По умолчанию отображение системных приложений отключено («Запретить»).

Сотовые станции

Данное правило отслеживает подключение к сотовым станциям из списка и, в случае попадания устройства пользователя в радиус действия сотовой станции, автоматически активирует работу следующих правил (если они входят в состав данной политики):

- использование Bluetooth;
- использование звукозаписи;
- использование камеры;
- использование Wi-Fi.

Активация данных политик происходит при включении на устройстве режима полета и/или в случае изъятия SIM-карты.

Деактивация правил происходит в следующих случаях:

- отключение от сотовой станции из списка;
- потеря сигнала сотовой связи;
- неисправность SIM-карты.

Установить / удалить приложения

Данная политика позволяет сформировать список приложений, которые будут установлены на устройство пользователя либо удалены с него при её применении.

Для формирования списка приложений для установки:

1. Нажмите кнопку **Выбрать приложение для установки** (см. рисунок 61). Появится модальное окно (см. рисунок 62).
2. Выберите приложение или пакет из каталога. При выборе приложений из списка доступен текстовый поиск.
3. Нажмите кнопку **Добавить** . Приложение добавится.

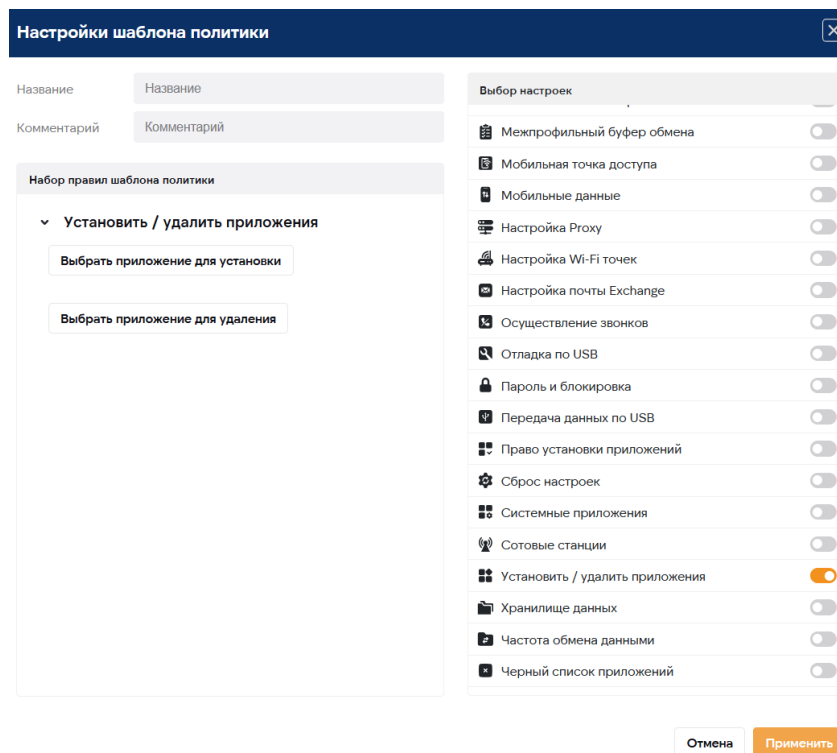


Рисунок 61 – Политика Право установки/удаления приложений

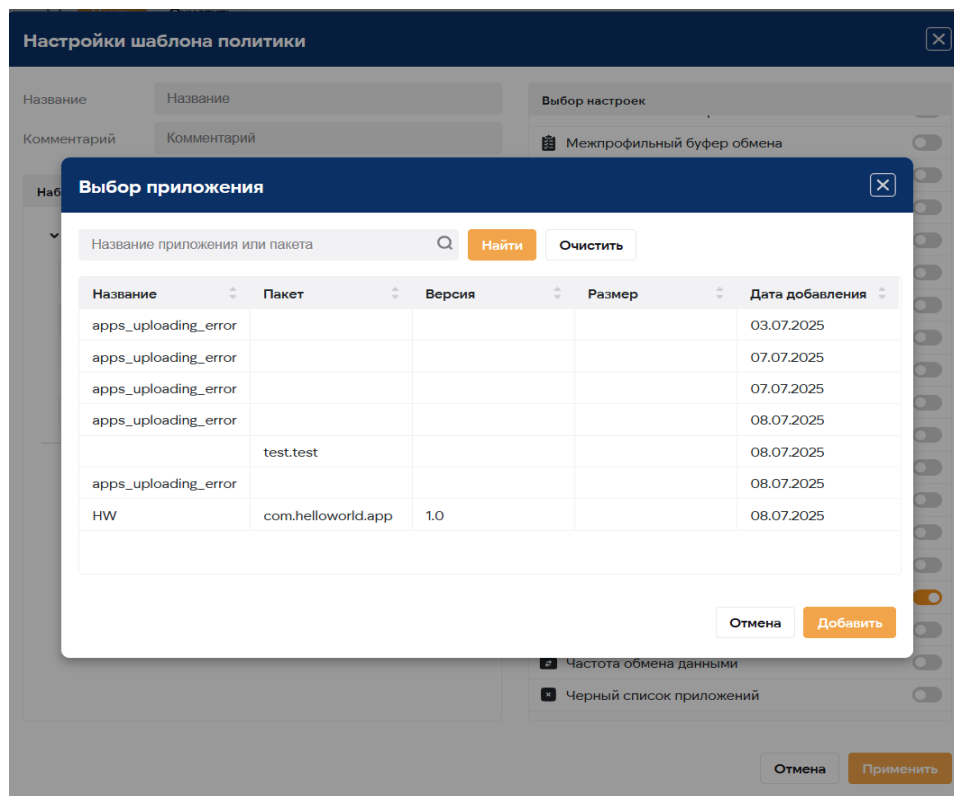


Рисунок 62 – Модальное окно для установки/удаления приложений

Формирование списка приложений для удаления

Для формирования списка приложений для удаления выполните следующие действия:

1. Нажмите кнопку **Выбрать приложение для удаления** (см. рисунок 61). Появится модальное окно (см. рисунок 62).
2. Выберите приложение или пакет из каталога. При выборе приложений из списка доступен текстовый поиск.
3. Нажмите кнопку **Добавить**. Приложение удалится.

Хранилище данных

Данное правило ограничивает использования внешнего хранилища данных.

Для разрешения необходимо установить параметр в значение «Разрешить». По умолчанию параметр находится в режиме «Запретить».

Частота обмена данными

Данное правило регулирует частоту обмена данными с сервером. Необходимо задать обязательный параметр «Интервал обновления (в мс)».

Черный список приложений

Данное правило позволяет сформировать список приложений, которые будут недоступны на устройстве пользователя. По умолчанию список пуст - ни одно приложение не выбрано.

Для создания чёрного списка приложений выполните следующие действия:

1. Нажмите кнопку **Выбрать приложение** (см. рисунок 63). Появится модальное окно выбора (см. рисунок 64).
2. Выберите приложение или пакет из каталога. Для удобства поиска доступна функция текстового поиска (фильтрация).
3. Нажмите кнопку . Приложение добавится в список блокируемых.

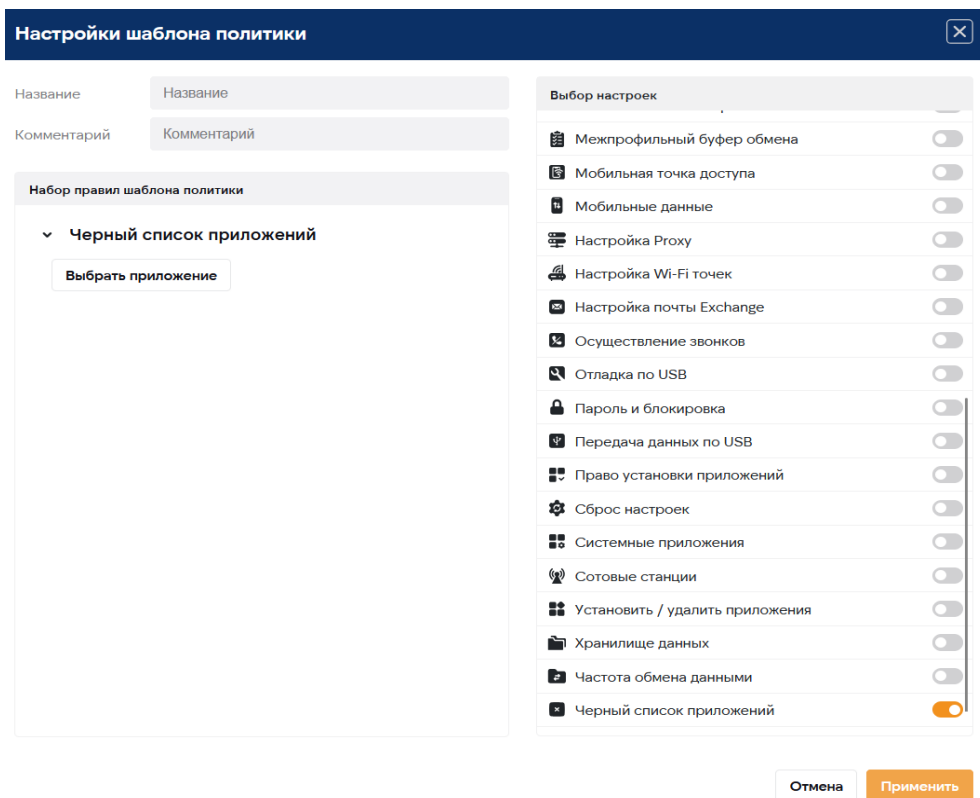


Рисунок 63 – Политика Черный сримок приложений

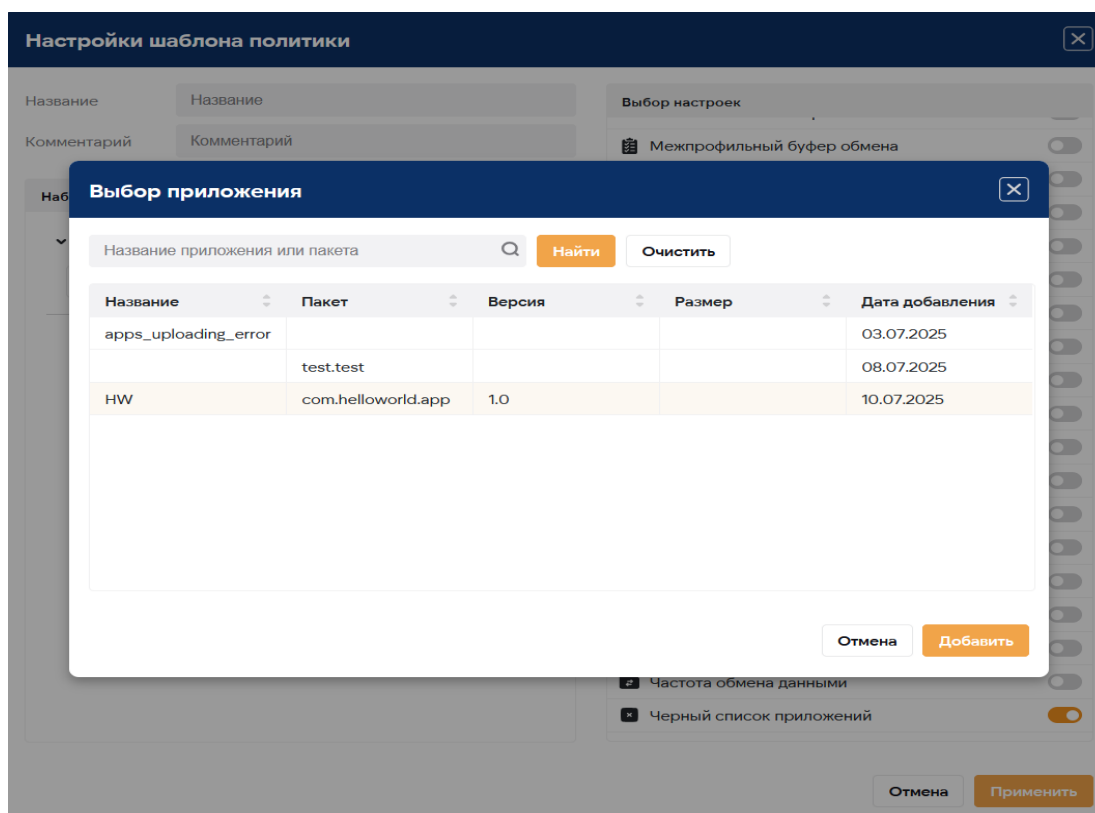


Рисунок 64 – Модально окно для выбора приложений

