НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

РУКОВОДСТВО АДМИНИСТРАТОРА

SAFEMOBILE

Москва

2024

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений 8

1 Введение 11

2 Описание действий при работе с АРМ Администратора SafeMobile 12

2.1 Аутентификация в АРМ Администратора SafeMobile 12

2.2 Обзор интерфейса АРМ Администратора SafeMobile 13

2.3 Панель ОШС 21

2.4 Главная таблица 23

2.5 Информационная таблица 27

2.6 Главное меню 28

2.6.1 Отчёт «Информация об устройстве» 30

2.6.2 Раздел «Сообщения» 34

2.6.3 Раздел «Звонки» 36

2.6.4 Раздел «Местоположения» 39

2.6.5 Раздел «Действия» 43

2.6.6 Раздел «События» 45

2.6.7 Раздел «Команды» 60

2.6.8 Раздел «Профили» 67

2.6.8.1 Создание профиля 68

2.6.8.2 Настройка параметров профиля 74

2.6.8.3 Задание условий применения профиля 77

2.6.8.4 Назначение профиля 79

2.6.8.5 Смена владельца сущности 80

2.6.8.6 Делегирование сущности 81

2.6.8.7 Применение профиля 81

2.6.8.8 Удаление профиля 86

2.6.9 Раздел «Правила несоответствия» 86

2.6.9.1 Добавление нового правила несоответствия 87

2.6.9.2 Редактирование существующего правила несоответствия 91

2.6.9.3 Удаление существующего правила несоответствия 91

2.6.10 Раздел «Установленные приложения» 92

2.6.11 Раздел «Правила управления» 94

2.6.11.1 Создание нового Правила управления приложениями 96

2.6.11.2 Задание условий применения ПУП 98

2.6.11.3 Назначение ПУП 98

2.6.11.4 Смена владельца сущности 99

2.6.11.5 Делегирование сущности 99

2.6.11.6 Применение ПУП 100

2.6.11.7 Особенности при удалении ПУП 101

2.6.11.8 Особенности обновления приложений 101

2.6.12 Раздел «Конфигурации» 104

2.6.12.1 Добавление конфигурации 105

2.6.12.2 Назначение конфигурации 109

2.6.12.3 Смена владельца сущности 110

2.6.12.4 Делегирование сущности 110

2.7 Построение отчётов (пункт меню «Отчёты») 111

2.7.1 Отчёт «Аудит» 111

2.7.2 Отчёт «Звонки и SMS» 114

2.7.3 Отчёт «События ИБ» 115

2.7.4 Отчёт «Перемещения» 116

2.7.5 Отчёт «Профили» 117

2.7.6 Отчёт «Правила управления» 119

2.7.7 Отчет «Правила управления (UID)» 120

2.7.8 Отчет «Геозоны» 123

2.7.9 Отчет «SafeLife» 124

2.7.10 Аудит SMAPI 127

2.8 Управление объектами учёта (пункт меню «Объекты учёта») 129

2.8.1 Организационно-штатная структура 129

2.8.2 Сотрудники 132

2.8.3 Роли 136

2.8.4 Администраторы 139

2.8.4.1 Редактирование данных администратора 141

2.8.4.2 Добавить нового администратора 141

2.8.5 Парольные политики АРМ 143

2.8.6 Операционные системы 145

2.8.7 Приложения 146

2.8.7.1 Добавление записи о приложении в систему 148

2.8.7.2 Редактирование записи о приложении 151

2.8.7.3 Удаление записи о приложении 152

2.8.8 SIM-карты 152

2.8.9 Комплекты 154

2.8.10 Комплекты Linux 160

2.8.10.1 Добавить новый комплект Linux 161

2.8.10.2 Удаление комплекта Linux 161

2.8.11 Геозоны 162

2.8.12 Серверные сертификаты 165

2.8.13 Подключения к серверам 167

2.8.14 Настройки SCEP 173

2.8.14.1 Добавление новой настройки SCEP 176

2.8.14.2 Удаление настроек SCEP 177

2.8.15 Клиентские сертификаты 177

2.8.16 Группы 180

2.8.17 Шаблоны писем 181

2.8.17.1 Добавление нового шаблона письма 182

2.8.17.2 Редактирование и удаление шаблона письма 183

2.8.18 Именованные условия применения 184

2.8.18.1 Добавление нового условия применения 185

2.8.18.2 Удаление условия применения 185

2.8.19 Метки устройств 185

2.8.19.1 Создание и удаление метки 186

2.8.20 Сервисные учетные записи 188

2.9 Синхронизация данных AD 190

2.9.1 Внешние каталоги 190

2.9.1.1 Создание нового подключения к службе каталогов 193

2.9.1.2 Удаление существующего подключения 194

2.9.1.3 Принудительная синхронизация с каталогом AD.....196

2.9.2 Пользователи 196

2.9.2.1 Изменение параметров существующего правила.....200

2.9.2.2 Создание нового правила импорта пользователей 201

2.9.2.3 Удаление правила импорта пользователей 201

2.9.2.4 Создание правила импорта пользователей с помощью файла списка групп пользователей 202

2.9.2.5 Настройка приоритетов правила импорта пользователей.....203

2.9.3 Группы.....204

2.9.3.1 Изменение параметров существующего правила импорта 207

2.9.3.2 Добавить новое правило импорта групп пользователей.....207

2.9.3.3 Удалить существующее правило импорта групп из списка.....208

2.9.3.4 Создание правила импорта групп из файла, содержащего список групп внешнего каталога.....209

2.9.4 Администраторы 210

2.9.4.1 Изменение параметров существующего правила.....212

2.9.4.2 Добавить новое правило импорта администраторов 212

2.9.4.3 Удалить существующее правило импорта администраторов.....213

2.9.4.4 Создание правила импорта администраторов из файла, содержащего список групп администраторов внешнего каталога.....213

2.9.5 Журнал.....215

2.10 Управление кодами приглашения (пункт меню «Загрузчик») 216

2.11 Корпоративный календарь рабочего времени (пункт меню «Календарь»).....222

2.11.1 Создание правил.....225

2.11.2 Изменение правил 227

2.11.3 Удаление правила 228

2.12 Контроль за лицензией на «UEM SafeMobile» (пункт меню «Лицензия») 229

2.12.1 Отчет по подключенным устройствам....230

2.13 Управление пользовательским соглашением 232

2.14 Информация....233

2.14.1 Компоненты 233

2.15 Очистка данных в «UEM SafeMobile»....235

2.16 Завершение работы в «UEM SafeMobile»....235

3 Частые вопросы 236

Приложение А Установка МСК на платформе iOS в режим Supervised 239

Приложение Б Перечень возможных ошибок при выполнении
команд Администраторов....245

Приложение В Приложения для мобильных устройств iOS....247

Приложение Г Состав полномочий предустановленных ролей....251

Приложение Д Подготовка устройства Windows для установки МСК 252

Приложение Е Основные сценарии работы с системой....253

Приложение Ж Поддерживаемые платформы мобильных устройств 256

Перечень используемых терминов и сокращений

Таблица 1 − Перечень терминов и сокращений

Сокращение	Полное наименование
ADEP	Программа управления корпоративная приложениями на устройствах Apple (Apple Developer Enterprise Program)
APN	Имя точки доступа (Access Point Name)
Auth-server	Сервер аутентификации SafeMobile. Отвечает за проверку сертификатов мобильных устройств, при доступе к серверу управления Android (socket-server).
CA	Удостоверяющий центр SafeMobile. Отвечает за выпуск сертификатов для мобильных устройств, используемых для авторизации в SafeMobile.
CHAP	Протокол аутентификации с косвенным согласованием (Challenge Handshake Authentication Protocol)
DN	Уникальное имя записи в ADт (Distinguished Name)
DN базового подразделения	DN раздела каталога. Используется при импорте данных из внешнего каталога AD, в качестве «корня дерева» поиска объектов для импорта.
GPRS	Пакетная радиосвязь общего пользования (General Packet Radio Service) — служба передачи данных в мобильных сетях
GPS	Глобальная система спутникового позиционирования (Global Positioning System)
HTTP	Протокол передачи гипертекста (HyperText Transfer Protocol)
ICCID	Уникальный идентификатор SIM-карты (Integrated Circuit Card Identifier)
IMEI	Международный идентификатор мобильного оборудования (International Mobile Equipment Identity)
IMSI	Международный идентификатор мобильного абонента (International Mobile Subscriber Identity)
IP-адрес	Идентификатор (адрес) устройства, подключенного к сети (Internet Protocol Address)
KME	Облачный инструмент автоматической регистрации корпоративных мобильных устройств производства Samsung (Knox Mobile Enrollment)
Knox	Технология управления смартфонами и планшетами от производителя Samsung
MCC	Мобильный код страны (Mobile Country Code)
MMS	Служба мультимедийных сообщений (Multimedia Messaging Service)
MNC	Код мобильной сети (Mobile Network Code)
MTP	Протокол передачи мультимедиа (Media Transfer Protocol)

Сокращение	Полное наименование
mTLS	Протокол взаимной аутентификации клиента и сервера (mutual TLS)
PAP	Протокол аутентификации, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (Password Authentication Protocol)
PKI	Инфраструктура открытых ключей (Public Key Infrastructure)
PTP	Протокол передачи изображений (Picture Transfer Protocol)
SCEP	Протокол инфраструктуры PKI, который используется для упрощенного способа получения сертификатов (Simple Certificate Enrollment Protocol)
SDK	Комплект средств разработки для создания приложений для определенного ПО (Software Development Kit)
SIM	Модуль идентификации абонента (Subscriber Identification Module)
SIP-аккаунт	Учетная запись пользователя в системе интернет-телефонии
SMS	Служба коротких сообщений (Short Message Service)
SSID	Идентификатор сети (Service Set Identifier)
Supervised	Режим осуществления контроля над МСК на платформе iOS. Для перевода в режим контроля требуется перепрошивка МСК при помощи ПО Apple Configurator 2 на ПК с ОС MacOS с потерей данных пользователя (описание установки iOS-устройства в Supervised-режим приведено в приложении А)
TLS	Криптографический протокол, обеспечивающие защищённую передачу данных между узлами в сети Интернет (Transport Layer Security)
UDID	Уникальный идентификатор устройства (Unique Device Identifier)
UID	Идентификатор приложения (Unique Identifier)
UEM	Унифицированное управление конечными устройствами (Unified Endpoint Management)
USB	Последовательный интерфейс для подключения периферийных устройств (Universal Serial Bus)
USSD	Сервис в сотовых сетях, организующий интерактивное взаимодействие между абонентом сети и сервисным приложением (Unstructured Supplementary Service Data)
VPN	Виртуальная частная сеть – технология организации защищенных линий связи между абонентами по незащищенным каналам передачи данных (Virtual Private Network)
WAP	Беспроводной протокол передачи данных (Wireless Application Protocol)
АРМ	Автоматизированное рабочее место
ЗУ	Зарядное устройство

Сокращение	Полное наименование
ИБ	Информационная безопасность
Контейнер	Изолированная область на МСК, предназначенная для корпоративных приложений и данных. Для МСК на платформе Android производителя Samsung поддерживаются два типа контейнеров: Samsung KNOX и Work Profile.
КП	Конфигурация приложения
КРП	Корпоративный рабочий профиль
ЛРП	Личный рабочий профиль
Метаинформация	Дополнительная информация, раскрывающая сведения о признаках и свойствах, характеризующих какие-либо сущности, позволяющие автоматически искать и управлять ими в больших информационных потоках
Метка устройства	Маркер устройства, заданный пользователем. Объект учета.
МСК	Мобильное средство коммуникации (мобильный телефон, смартфон, планшетный компьютер, смарт-браслет)
ОС	Операционная система
ОШС	Организационно-штатная структура предприятия
ПК	Персональный компьютер
ПО	Программное обеспечение
Профиль	Совокупность значений и настроек ОС
ПУН	Приложение с управляемыми настройками
ПУП	Правило управления приложением
Режим киоска	Режим работы МСК, при котором разрешен запуск одного или нескольких определенных приложений.
Стратегия	Способ управления устройством Android. Стратегия задается администратором и определяет: чем и в каком объеме администратор сможет управлять на устройстве. Применяется при подключении устройства. Если монитор при подключении МСК не получит необходимых для исполнения заданной стратегии привилегий, то МСК не будет подключено
Сущность	Именованный набор данных, который можно атомарно (целиком) назначить или снять с узла ОШС, сотрудника или МСК. К сущностям относятся профиль, ПУП и КП
УПАТС	Учрежденческо-производственная автоматическая телефонная станция
УЦ	Центр сертификации или удостоверяющий центр (англ. Certification authority, CA)
ФИО	Фамилия, имя и отчество

1 Введение

Настоящее руководство предназначено для Администраторов «UEM SafeMobile» (далее по тексту – система или SafeMobile) и содержит описание веб-интерфейса АРМ Администратора, а также действий по управлению комплексной цифровой мультиплатформой управления мобильными средствами коммуникаций посредством интерфейса, а именно в:

- регистрации МСК;
- настройке по применению политик безопасности на МСК, в том числе политик при смене SIM-карты устройства;
- рассылке внутренних сообщений;
- удаленной настройке и управлении приложениями на МСК, в том числе в контейнере;
- удаленной блокировке и разблокировке мобильного устройства;
- удалённом отключении МСК от управления системой;
- управлении списком доверенных беспроводных точек доступа;
- осуществлении настройки доступа на МСК к электронной почте;
- управлении настройками ОС МСК, в зависимости от принадлежности устройства и его местонахождения;
- просмотре отчётов;
- выгрузке информации о МСК, включая реестр установленных на него корпоративных приложениях
- мониторинге состояния здоровья сотрудников посредством смарт-браслетов.

2 Описание действий при работе с АРМ Администратора SafeMobile

2.1 Аутентификация в АРМ Администратора SafeMobile

Для входа в АРМ Администратора SafeMobile необходимо открыть браузер (Mozilla Firefox или Google Chrome актуальной версии) и в адресной строке набрать адрес (например, https://ip-address:8443), по которому был размещен АРМ Администратора, после чего отобразится окно аутентификации в соответствии с рисунком 2.1.

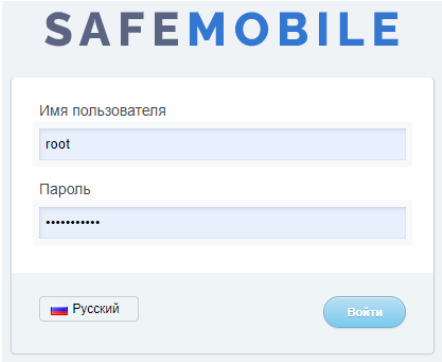


Рисунок 2.1 - Окно аутентификации

При первом входе необходимо ввести имя пользователя (*root*) и временный пароль (*change_on_install*) в соответствующие поля и нажать кнопку **«Войти»**. Временный пароль действует только при первом входе в систему. Сразу же после его успешного ввода потребуется сменить пароль на новый, в соответствии с параметрами парольной политики АРМа, заданными в 2.8.5.

Примечание.

Если учетная запись администратора была импортирована из AD посредством «правил импорта администраторов», то для авторизации администратора необходимо вводить имя пользователя в формате UPN (username@domain) домена, из которого был произведен импорт учетной записи.

В окне аутентификации доступно изменения языка интерфейса. При нажатии на кнопку Русский интерфейс переключится на английский язык, при нажатии на кнопку English интерфейс снова отобразится на русском языке.

После первого успешного входа в системе доступен только Суперадминистратор **«root»** с доступом к разделу **«Лицензия»**. После ввода лицензии **«root» получает** неограниченные полномочия и доступ ко всем функциональным возможностям системы.

Добавление новых пользователей системы, в том числе Администраторов ИТ и ИБ, осуществляется согласно разделу 2.8.4.

Отображение интерфейса в данном руководстве приведено для Суперадминистратора **«root»**, для пользователей с ограниченными правами отображение интерфейса может отличаться.

В системе предусмотрен принудительный выход Администратора из системы, после которого потребуется повторный вход в систему. Принудительный выход Администратора из системы происходит в следующих случаях:

- если Администратор был заблокирован;
- если у Администратора изменился состав ролей;
- если у ролей Администратора изменился состав полномочий;
- если время сессии Администратора истекло (по умолчанию время сессии равно 30 минутам, время сессии является параметром настройки сервера веб-приложений SafeMobile).

В системе доступен контроль клиентских сессий, при котором возможен повторных вход с учетной записи уже подключенного Администратора (по умолчанию количество сессий одного пользователя равно двум, параметры контроля сессий устанавливаются при настройке сервера веб-приложений SafeMobile).

Набор доступных функций системы, а также соответствующий вид интерфейса АРМ, зависит от полномочий Администратора, от имени которого выполнен вход в систему.

2.2 Обзор интерфейса АРМ Администратора SafeMobile

Главное окно АРМ Администратора SafeMobile, открывающееся после аутентификации, состоит из следующих компонентов:

- главное меню навигации по разделам АРМ. Находится в левой части окна. Для того, чтобы скрыть главное меню следует нажать соответствующую кнопку (рисунок 2.2а).

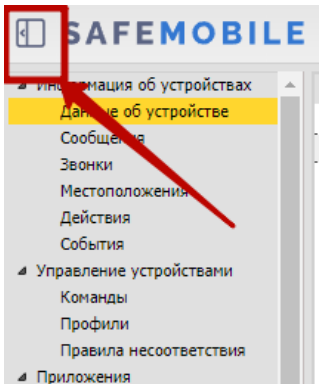


Рисунок 2.2а – расположение кнопки «скрыть главное меню»

- панель организационно-штатной структуры (ОШС) организации в виде иерархического списка подразделений;
- главная таблица, содержащая список МСК сотрудников организации или подразделения, выбранного в панели ОШС;
- информационная таблица, которая находится в нижней части окна и отображает данные по МСК, выбранному в главной таблице;
- кнопка **«Обновить»** (рисунок 2.2b), расположенная в правом верхнем углу окна, предназначена для обновления всей информации в главном окне, кнопки **«Обновить»** для главной и информационной таблиц расположены на панели внизу каждой из таблиц.

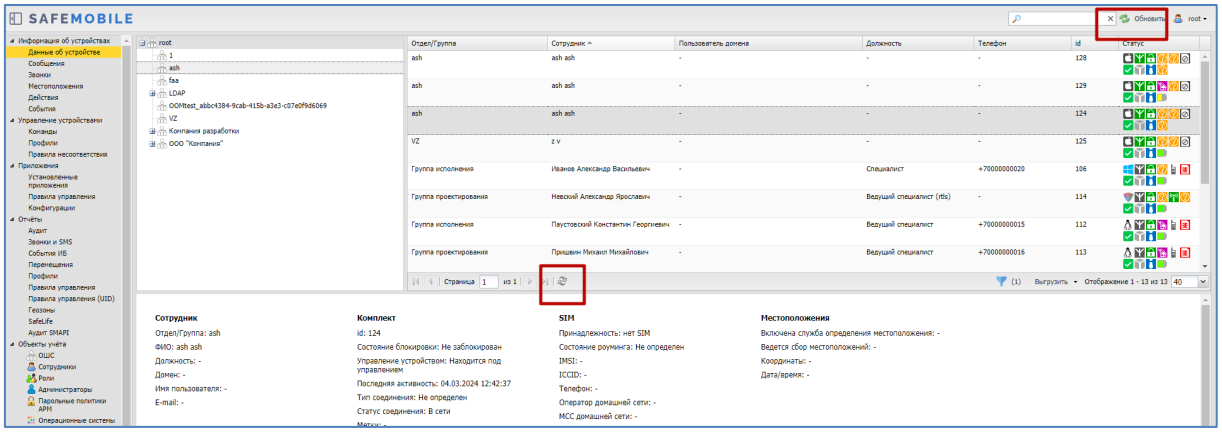


Рисунок 2.2b - Главное окно АРМ Администратора SafeMobile

В правом верхнем углу окна расположена также кнопка, отображающая имя пользователя (логин), под учётной записью которого выполнен вход в систему. Кроме того, нажатие на эту кнопку позволяет выбрать команду в раскрывающемся меню, а именно: **«Изменить пароль»**, введенный при аутентификации; выполнить **«Выход»** из АРМ Администратора SafeMobile; переключить интерфейс на английский язык, нажав на кнопку Русский (рисунок 2.3), после перехода на английский язык кнопка изменится на English.

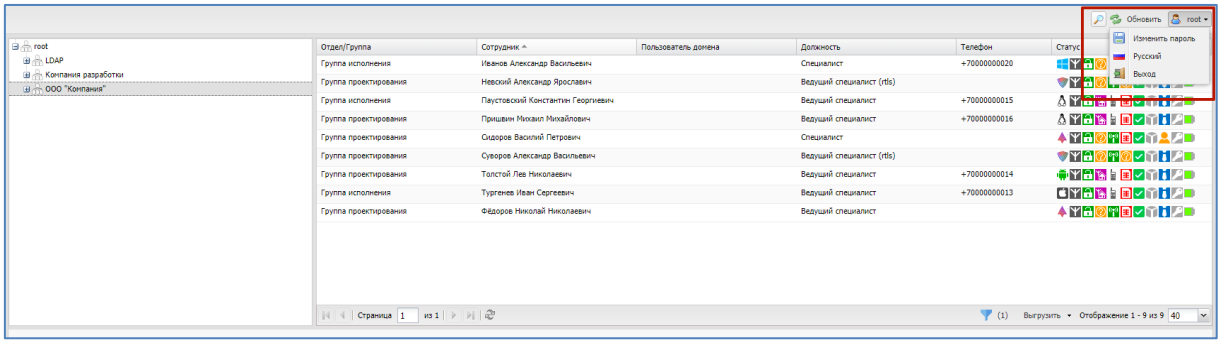


Рисунок 2.3 - Меню, отображающее имя пользователя (логин)

Для осуществления поиска в таблицах предназначена строка ввода поискового запроса и расположена в верхней части таблицы, в которой осуществляется поиск (рисунок 2.4). Поиск производится по различными колонкам, в зависимости от таблицы.

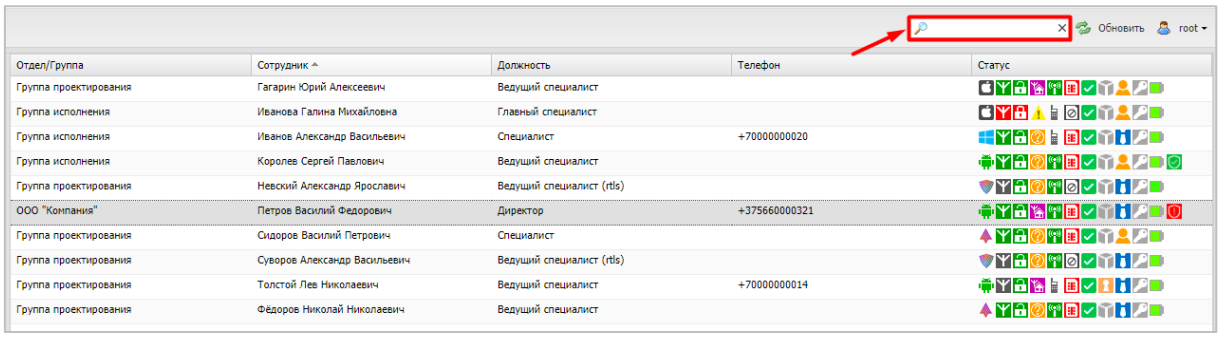


Рисунок 2.4 – Строка поиска в главной таблице

В АРМ Администратора SafeMobile существует возможность формирования отчета «Инвентаризация МСК» с учетом заданных параметров фильтрации для устройств подразделения, выбранного на панели ОШС. Для этого необходимо нажать кнопку Выгрузить на нижней панели главной таблицы, после чего в выпадающем меню выбрать параметр: «Без приложений/С приложениями» (рисунок 2.5). В отчет «Инвентаризация МСК» войдет имеющаяся в системе информация по МСК независимо от количества полей, отображаемых в главной таблице. Если задан параметр «С приложениями», то отчет сформируется с дополнительной информацией о приложениях (зарегистрированных в системе), установленных на МСК.

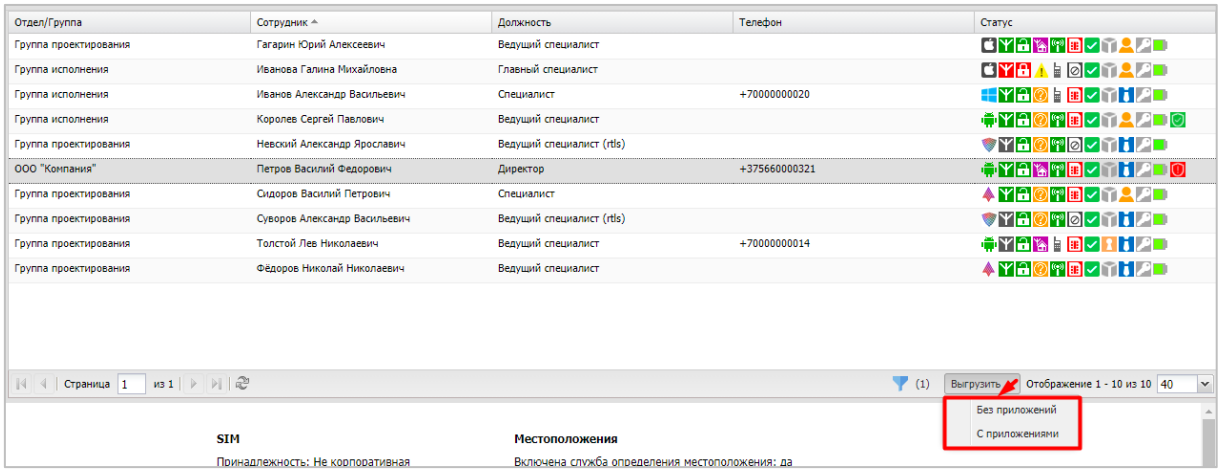


Рисунок 2.5 - Меню «Выгрузить» в главной таблице

При нажатии на кнопку **«Выгрузить»** на панели других таблиц (информационной таблицы и т.п.) отчет формируется с данными, отображаемыми в этих таблицах. Отчеты выгружаются в отдельном окне. Если отчет содержит менее 10000 записей, то выгрузка производится в формате XLSX. Если отчет содержит более 10000 записей, то выгрузка производится в формате CSV.

В таблицах АРМ Администратора SafeMobile имеются следующие возможности по управлению записями:

- изменение порядка столбцов путем перемещения заголовка столбца в нужное место с помощью мыши;
- сортировка записей таблиц по выбранному столбцу;
- изменение состава отображаемых столбцов в таблицах с помощью раскрывающегося меню в заголовках столбцов.

Записи в таблицах отображаются в постраничном режиме, количество отображаемых записей для удобства пользователя можно изменять в соответствии с рисунком 2.6 в зависимости от объема информации.

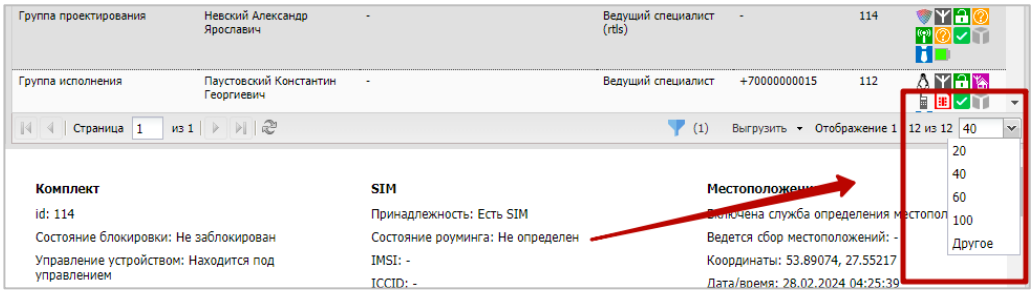


Рисунок 2.6 - Количество отображаемых записей в главной таблице

Для сортировки записей в таблице в порядке убывания или возрастания значений необходимо открыть раскрывающееся меню, нажав стрелку справа от заголовка выбранного столбца, в соответствии с рисунком 2.7 и выбрать требуемый порядок сортировки: **«По возрастанию»** или **«По убыванию»**.

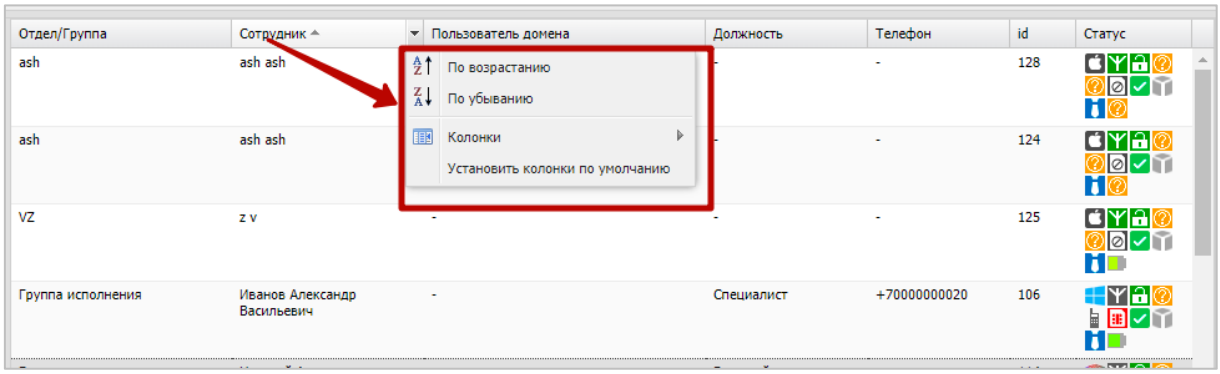


Рисунок 2.7 - Сортировка записей в столбце главной таблиц

Изменить состав отображаемых столбцов в таблицах можно с помощью раскрывающегося меню в заголовках столбцов, как показано на рисунке 2.8.

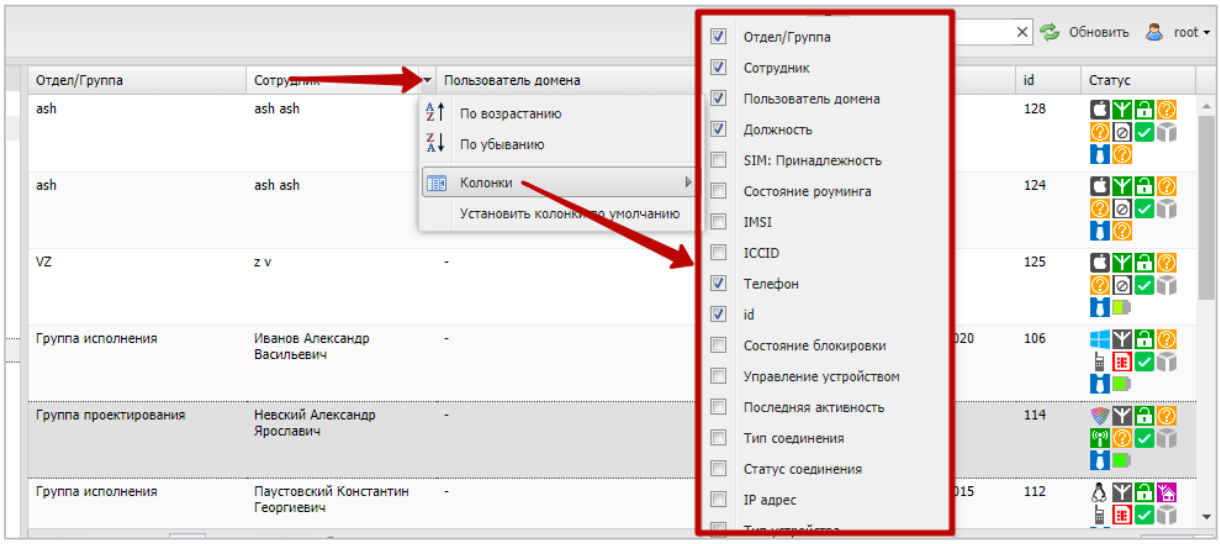


Рисунок 2.8 - Управление столбцами в главной таблице

Для включения столбцов в состав, отображаемых в таблице или исключения их необходимо открыть раскрывающееся меню, нажав стрелку справа от заголовка выбранного столбца, выбрать пункт меню **«Колонки»**, а затем отметить флажками те столбцы, которые требуется отобразить, или снять флажки с тех столбцов, которые требуется скрыть.

Система запоминает для каждого пользователя состав колонок, порядок расположения колонок, ширину колонок в следующих разделах системы:

- Информация об устройстве,
- Управлении устройствами:
  - Профили,
  - Правила несоответствия,
- Приложения,
- Отчеты:
  - Профили,
  - Правила управления,
- Объекты учета:
  - Комплекты,
  - Сотрудники,
  - Администраторы,
  - Клиентские сертификаты.

Для быстрого приведения этих параметров в исходное состояние следует нажать кнопку "Установить колонки по умолчанию" (рисунок 2.9). При её нажатии восстанавливается первоначальные:

- состав колонок,
- порядок расположения колонок,
- ширина колонок.

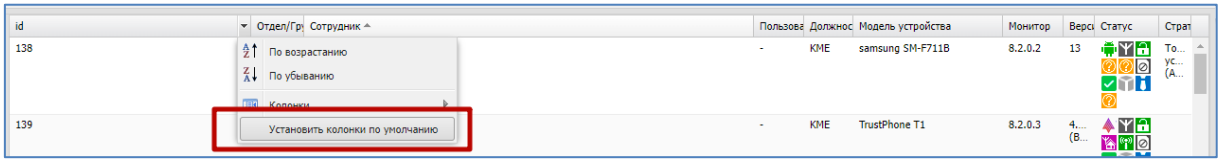


Рисунок 2.9 - Расположение кнопки «Установить кнопки по умолчанию»

Аналогичным образом осуществляется управление записями в информационной таблице. По умолчанию записи в главной таблице сортируются по возрастанию ФИО сотрудника.

Для задания в главной таблице фильтрации записей следует нажать кнопку фильтра в соответствии с рисунком 2.10.

Рисунок 2.10 - Фильтрация записей в главной таблице

В окне фильтров отображаются три вкладки:

- Статусы;
- Платформа;
- Приложения.

Во вкладке **«Статусы»** можно задать фильтрацию записей в главной таблице по статусу комплектов в соответствии с рисунком 2.11.

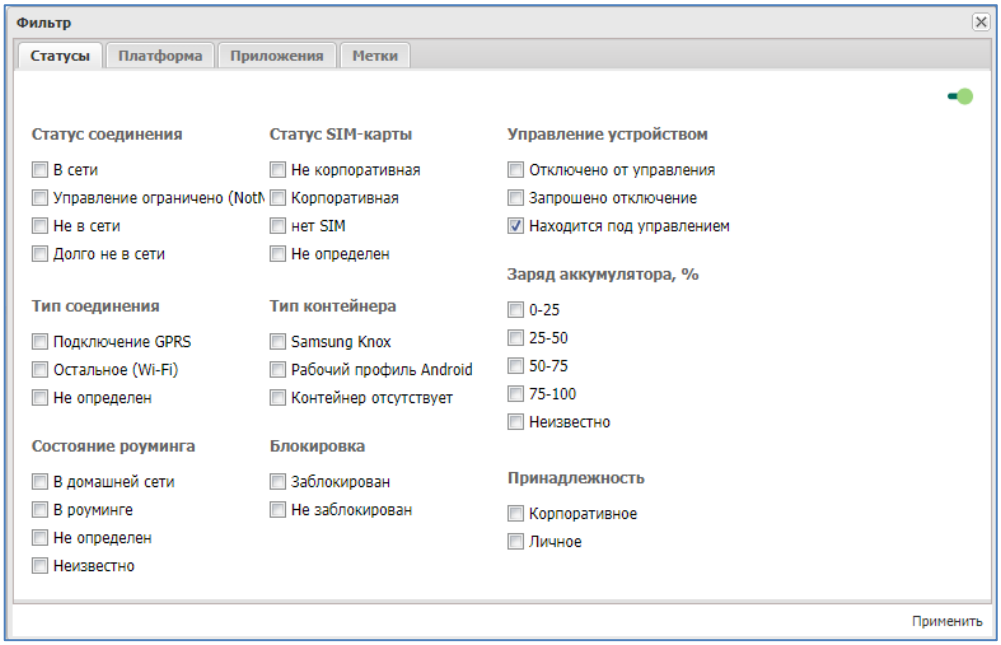


Рисунок 2.11 - Вкладка «Статусы»

По умолчанию установлен фильтр по статусу «Управление устройством», а именно: «Находится под управлением».

Во вкладке «Платформа» (рисунок 2.12) можно задать фильтрацию записей в зависимости платформы МСК. По умолчанию фильтр «Платформа» выключен.

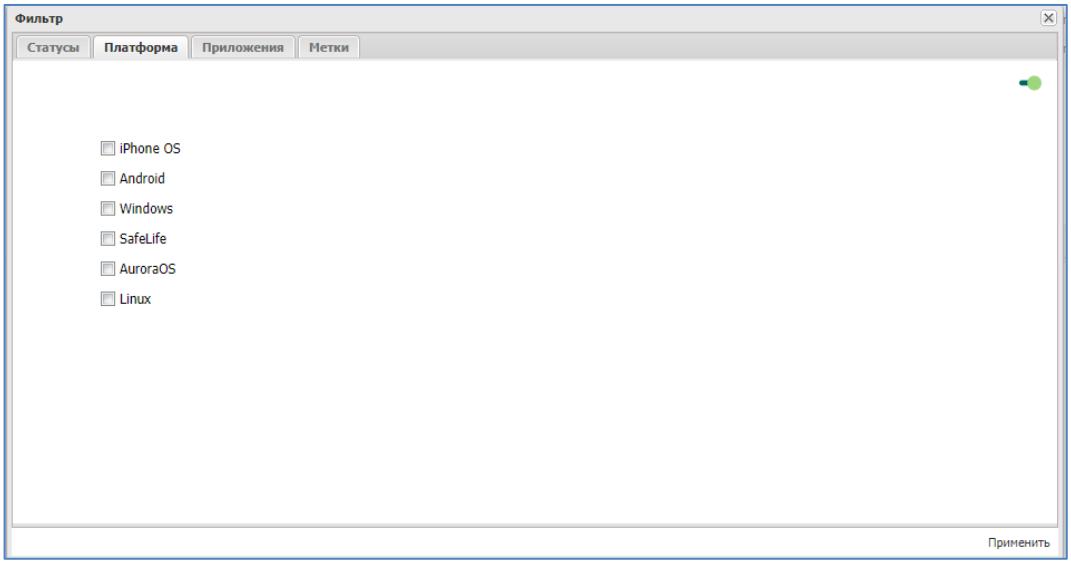


Рисунок 2.12 - Вкладка «Платформа»

Во вкладке **«Приложения»** можно задать фильтрацию записей в зависимости от установленных/неустановленных приложений на МСК соответствии с рисунком 2.13. По умолчанию фильтр «Приложения» выключен.

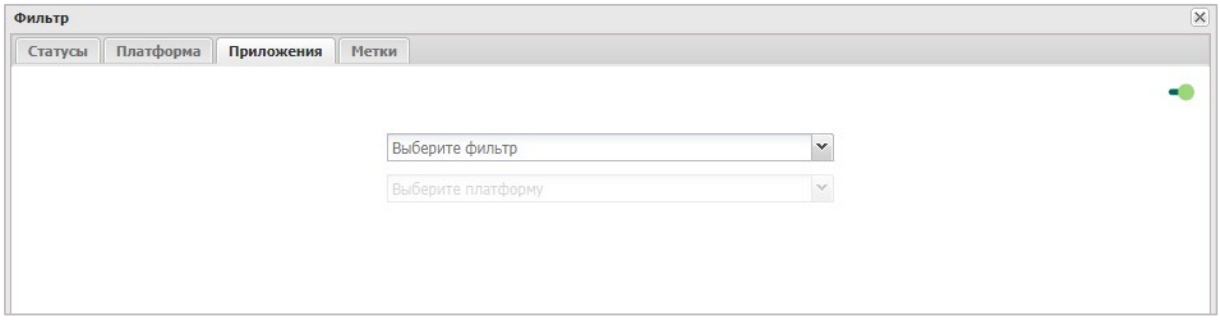


Рисунок 2.13 - Вкладка «Приложения»

Для задания фильтрации следует выбрать требуемые параметры и нажать **«Применить»**. Рядом с кнопкой фильтра в панели инструментов отобразится количество установленных фильтров. Для отмены фильтров требуется переключатель перевести в состояние «выключено» .

2.3 Панель ОШС

В главном окне системы расположена панель, содержащая организационно-штатную структуру организации (ОШС) в соответствии с рисунком 2.14.

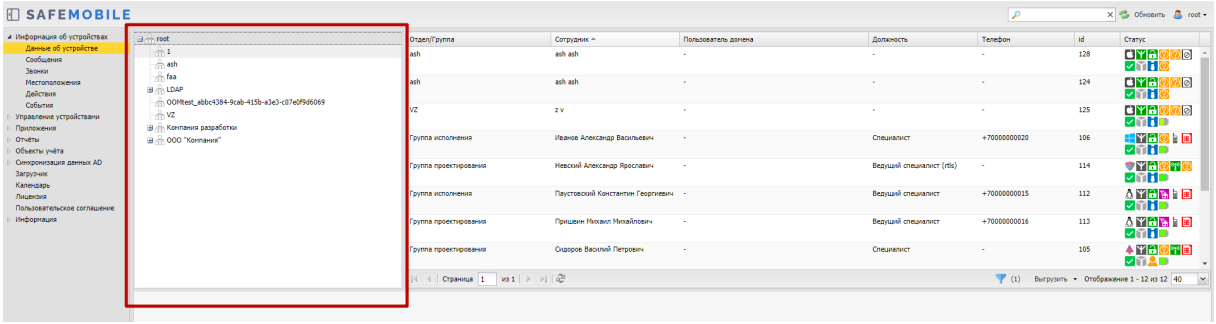


Рисунок 2.14 - Панель ОШС

Иерархический список подразделений позволяет выбрать подразделение, после чего в главной таблице справа отобразится список МСК, имеющихся у сотрудников этого подразделения. Кроме того, можно отобразить всех сотрудников и МСК организации, выбрав название всей организации в верхней строке ОШС в соответствии с рисунком 2.15.

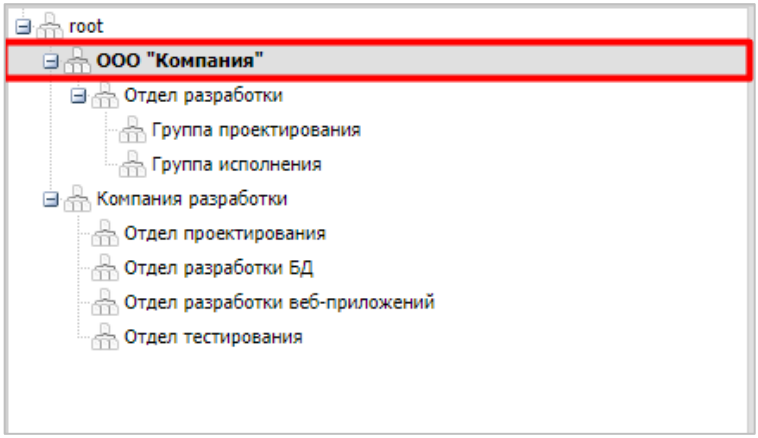


Рисунок 2.15 - Выбор корневого узла предприятия в панели ОШС

Строка пути ОШС отображает полный путь от корня, до выделенного пользователем объекта (риск 2.16)

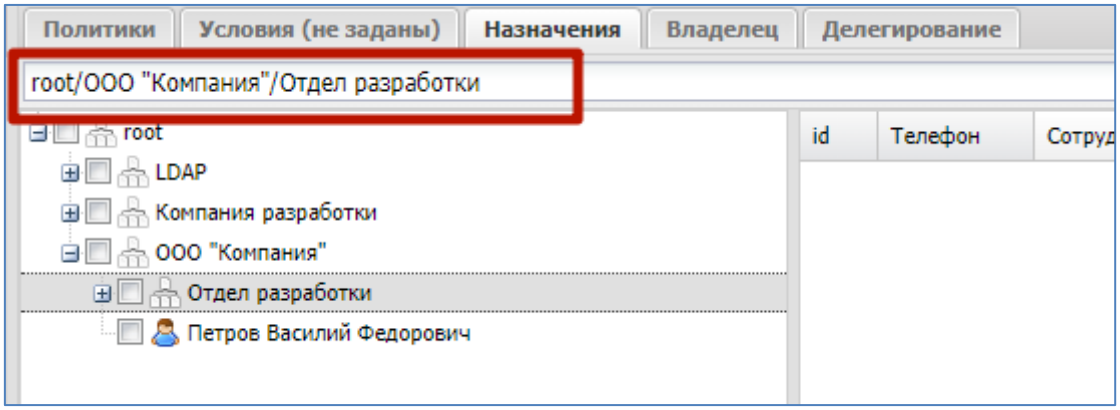


Рисунок 2.16 - Строка пути ОШС

2.4 Главная таблица

В главной таблице (рисунок 2.17) отображается список и параметры комплектов, зарегистрированных в системе. Количество отображаемых комплектов зависит от выбранного в ОШС элемента – если выбран корневой элемент, в главной таблице отображается перечень всех комплектов предприятия; если выбран другой элемент ОШС (подразделение предприятия), в таблице будут показаны комплекты сотрудников и МСК этого подразделения.

При выборе комплекта в главной таблице подразделение, которому он принадлежит, выделяется в разделе ОШС жирным шрифтом, что упрощает поиск подразделения, в котором работает сотрудник с выбранным комплектом.

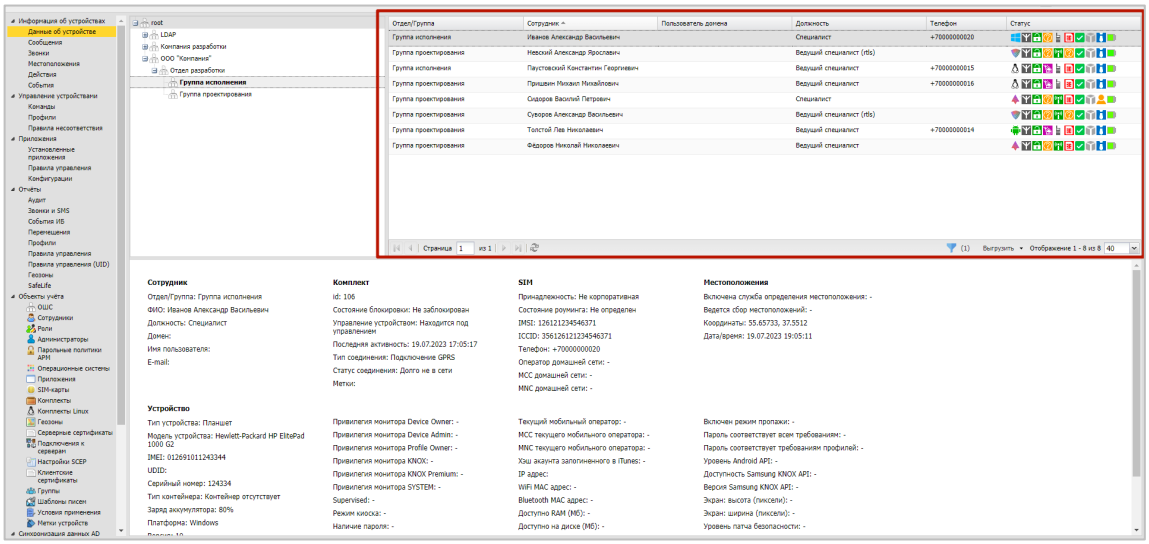


Рисунок 2.17 - Главная таблица

Главная таблица содержит следующие столбцы:

- Отдел/Группа – название подразделения, в котором работает сотрудник (по умолчанию, отображается в таблице);
- Сотрудник – ФИО сотрудника (по умолчанию, отображается в таблице);
- Пользователь домена – ФИО сотрудника или e-mail, если ФИО не было импортировано (по умолчанию, отображается в таблице);
- Должность – должность сотрудника (по умолчанию, отображается в таблице);
- SIM: Принадлежность − признак принадлежности SIM-карты организации, в которой работает сотрудник (корпоративная / не корпоративная/ нет SIM);

- Состояние роуминга − статус сети, к которой подключено МСК (в домашней сети / в роуминге / не определен / значение неизвестно);
- IMSI - международный идентификатор мобильного абонента (индивидуальный номер абонента);
- ICCID - уникальный серийный номер SIM-карты;
- Телефон – номер телефона комплекта (по умолчанию, отображается в таблице);
- id – уникальный идентификационный номер МСК в системе;
- Состояние блокировки − состояние телефона сотрудника для защиты данных (заблокирован / не заблокирован);
- Управление устройством − состояние подключения устройства к управлению «UEM SafeMobile» (отключено от управления / запрошено отключение / находится под управлением);
- Последняя активность − дата и время регистрации последнего нахождения МСК в системе;
- Тип соединения − тип подключения для передачи данных между МСК и системой (подключение GPRS / остальное (Wi-Fi) / не определен);
- Статус соединения − состояние соединения МСК с системой (в сети / не в сети / долго не в сети);
- IP адрес − только для МСК на платформе Android;
- Тип устройства − тип МСК, подключенного к системе (смартфон / планшет / иное);
- Модель устройства − модель МСК, подключенного к системе;
- Серийный номер − серийные номера МСК на платформе iOS и Android;
- Тип контейнера − тип созданного контейнера на устройстве (Samsung Knox / контейнер отсутствует);
- Заряд аккумулятора − уровень заряда батареи, %;
- Устройство: Принадлежность − признак собственности МСК (корпоративное / личное);
- Монитор − версия монитора, установленного на МСК;
- Платформа − мобильная платформа МСК;
- Версия − версия ОС МСК;
- Статус – отображает значки состояния МСК сотрудника в системе, описание которых содержится в таблице 2.1 (по умолчанию, отображается в таблице);
- Стратегия – примененная на МСК стратегия управления;
- Метки – список меток на устройстве.

Таблица 2.1 – Состояния мобильного средства коммуникации

Значок	Значение
Платформа	
	Android
	iOS
	Windows
	Аврора
	SafeLife
Статус соединения	
	В сети
	Не в сети
	Долго не в сети
	Управление ограничено (NotNow) (см.примечание)
Блокировка	
	Заблокирован
	Не заблокирован
Состояние роуминга	
	В домашней сети
	В роуминге
	Неизвестно
	Не определен

Значок	Значение
Тип соединения	
	Подключение GPRS
	Остальное (Wi-Fi)
	Не определен
Статус SIM-карты в МСК	
	Корпоративная
	Не корпоративная
	SIM не определен
	Нет SIM
Тип контейнера	
	Samsung Knox
	Контейнер отсутствует
	Android for Work
Состояние батареи	
	Уровень заряда батареи
Управление устройством	
	Отключено от управления
	Запрошено отключение
	Находится под управлением
Принадлежность устройства	
	Корпоративное
	Личное

Значок	Значение
Примечание. *Статус подключения NotNow – этот статус может быть только у устройств iOS. Устройство в этом статусе соединения может принимать только команды блокировки и отключения от управления со сбросом к заводским настройкам. Команда синхронизации только обновит статус подключения устройства. Никакие профили, правила управления и конфигурации приложений не применяются. Данный статус может отображаться сразу после перезагрузки устройства, при низком заряде батареи и т.п.*	

2.5 Информационная таблица

В информационной таблице, расположенной в нижней части главного окна АРМ Администратора в соответствии с рисунком 2.18, отображаются сведения по МСК, выбранному в главной таблице.

В информационной таблице воспроизводятся данные в зависимости от выбранных разделов главного меню. Детальное описание данных таблицы описано в разделе 2.6.1.

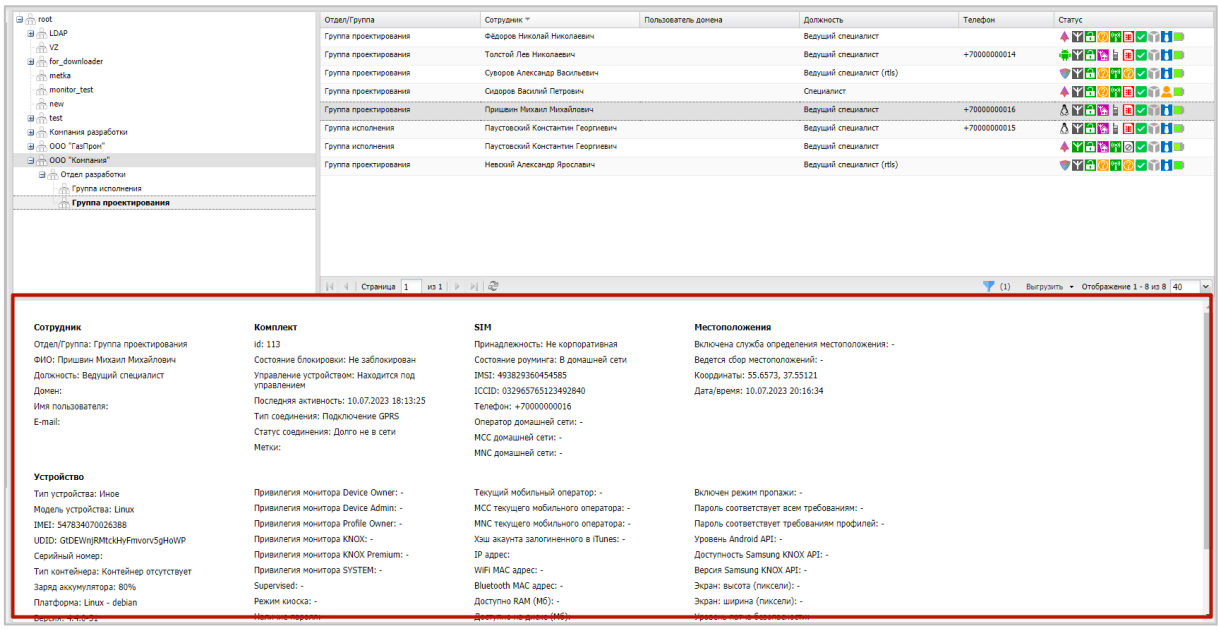


Рисунок 2.18 - Информационная таблица

2.6 Главное меню

В левой части главного окна АРМ Администратора SafeMobile в соответствии с рисунком 2.19 расположена панель главного меню, содержащая следующие разделы:

- Информация об устройствах
  - Данные об устройстве
  - Сообщения
  - Звонки
  - Местоположения
  - Действия
  - События
- Управление устройствами
  - Команды
  - Профили
  - Правила несоответствия
- Приложения
  - Установленные приложения
  - Правила управления
  - Конфигурации
- Отчёты
  - Аудит
  - Звонки и SMS
  - События ИБ
  - Перемещения
  - Профили
  - Правила управления
  - Правила управления (UID)
  - Геозоны
  - SafeLife
- Объекты учёта
  - ОШС
  - Сотрудники
  - Роли
  - Администраторы

- Парольные политики АРМ
- Операционные системы
- Приложения
- SIM-карты
- Комплекты
- Комплекты Linux
- Геозоны
- Серверные сертификаты
- Подключения к серверам
- Настройки SCEP
- Клиентские сертификаты
- Группы
- Шаблоны писем
- Условия применения
- Метки устройств

- Синхронизация данных AD
  - Внешние каталоги
  - Пользователи
  - Группы
  - Администраторы
  - Журнал
- Загрузчик
- Календарь
- Лицензия
- Пользовательское соглашение

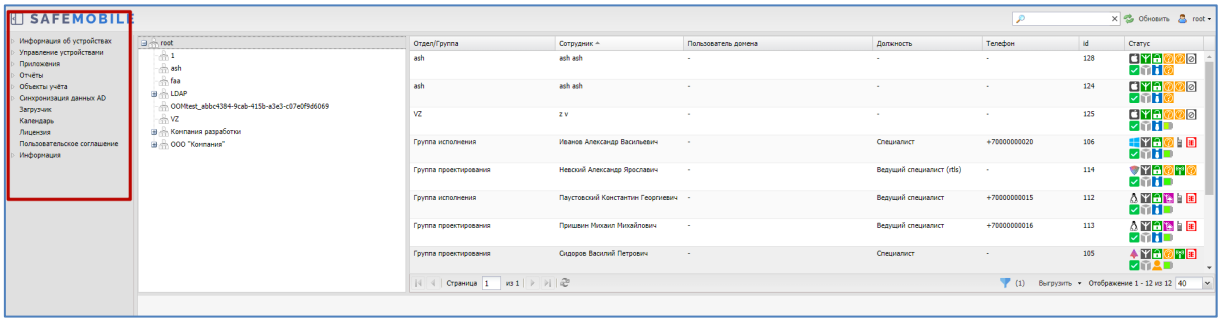


Рисунок 2.19 - Главное меню

2.6.1 Отчёт «Информация об устройстве»

Для просмотра информации о параметрах комплекта следует нажать пункт **«Данные об устройстве»** главного меню и выбрать требуемый комплект в главной таблице в соответствии с рисунком 2.20.

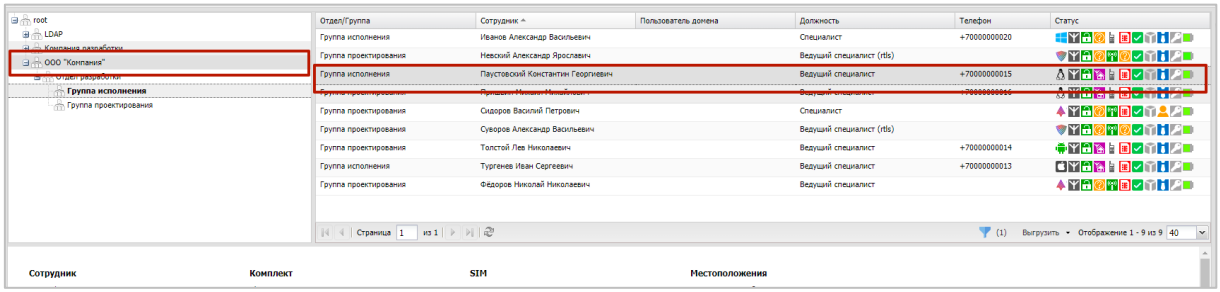


Рисунок 2.20 - Информация о параметрах комплекта

После этого в нижней части АРМ отобразятся следующие функциональные группы с параметрами сотрудника и его МСК:

- **Сотрудник**
  - Отдел/Группа;
  - ФИО;
  - Должность;
  - Домен;
  - Имя пользователя;
  - E-mail;
- **Комплект**
  - id;
  - Состояние блокировки (заблокирован/не заблокирован).
    Если устройство статусе «заблокировано», то дополнительно отображается причина блокировки:
    - командой администратора,
    - политикой,
    - меткой NFC,
    - прежней версией,
    - сменой пароля.

    При наведении курсора на пиктограмму блокировки (в колонке «статус») в всплывающей подсказке будут отображены причины блокировки (рисунок 2.21).

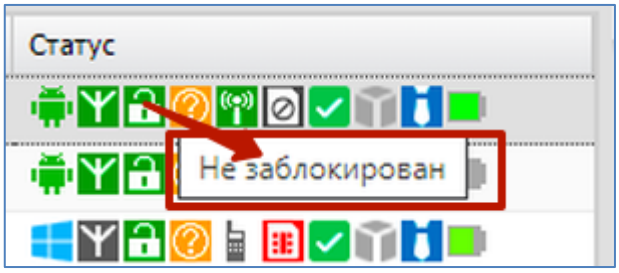


Рисунок 2.21 - Всплывающая подсказка, с информацией о блокировке

- Управление устройством (находится под управлением/отключен от управления/запрошено отключение);
- Последняя активность (дата и время);
- Тип соединения (GPRS/остальное (wi-fi)/не определен);
- Статус соединения:
  - В сети - Последняя активность была менее 15 минут назад. Если устройство iOS, то в последние 10 минут ни одна из команд протокола apple mdm НЕ завершилась со статусом NotNow;
  - Не в сети - Последняя активность была в диапазоне от 15 минут до 24 часов;
  - Долго не в сети - Последняя активность была более 24 часов назад;
  - Управление ограничено (NotNow) - Последняя активность была менее 15 минут назад и в последние 10 минут хотя бы одна из команд протокола apple mdm завершилась со статусом NotNow;
- Метки;

- **SIM**
  - Принадлежность (корпоративная, не корпоративная, нет SIM, есть SIM);
  - Состояние роуминга (в домашней сети/в роуминге/не определено/неизвестно);
  - IMSI;
  - ICCID;
  - Телефон (номер телефона);
  - Оператор домашней сети;
  - MCC домашней сети;
  - MNC домашней сети;

- **Местоположения**
    - Включена служба определения местоположения (да/нет);
    - Ведется сбор местоположений: (+/-);
    - Координаты (последние зарегистрированные в системе координаты абонента);
    - Дата/время (дата и время последней регистрации абонента в системе);
- **Устройство**
    - Тип устройства (смартфон/планшет/иное/браслет SafeLife);
    - Модель устройства;
    - IMEI;
    - UDID;
    - Серийный номер (для МСК на платформе iOS и Android);
    - Тип контейнера (Samsung Knox/Рабочий профиль Андроид/контейнер отсутствует);
    - Заряд аккумулятора (от 0 до 100 %);
    - Платформа;
    - Дистрибутив Linux;
    - Версия;
    - Версия ядра Linux;
    - Версия дистрибутива Linux
    - Принадлежность (корпоративное/личное);
    - Монитор (версия монитора);
    - Стратегия (устройство/устройство и контейнер KNOX/личный рабочий профиль/корпоративный рабочий профиль);
    - Привилегия монитора Device Owner (да/нет);
    - Привилегия монитора Device Admin (да/нет);
    - Привилегия монитора Profile Owner (да/нет);
    - Привилегия монитора KNOX (да/нет);
    - Привилегия монитора KNOX Premium (да/нет);
    - Привилегия монитора SYSTEM (да/нет);
    - Supervised;
    - Режим киоска (да/нет);
    - Наличие пароля (да/нет);
    - Текущий мобильный оператор;
    - MCC текущего мобильного оператора;
    - MNC текущего мобильного оператора;

- Хэш аккаунта, залогиненного в iTunes;
- IP адрес;
- WiFi MAC адрес;
- Bluetooth MAC адрес;
- Доступно RAM (Мб);
- Доступно на диске (Мб);
- Включено резервное копирование в облако;
- Шифрование хранилищ;
- Включен режим пропажи;
- Пароль соответствует всем требованиям − пароль соответствует не только требованиям парольных профилей системы (SafeMobile), но и требованиям всех парольных профилей, установленных на устройстве. Помимо профилей системы на устройство могут быть так же установлены профили Exchange и Apple Configurator. Только для МСК на платформе iOS;
- Пароль соответствует требованиям профилей (да/нет);
- Уровень Android API;
- Доступность Samsung KNOX API (да/нет);
- Версия Samsung KNOX API;
- Экран: высота (пиксели);
- Экран: ширина (пиксели);
- Уровень патча безопасности (дата);
- Архитектура ОС;
- Стратегия управления;
- Дистрибутив Linux;
- Версия ядра Linux;
- Версия дистрибутива Linux;
- Заряд аккумулятора;
- Общий объём памяти (Мб);
- Имя устройства;
- Возможность сброса устройства;
- Идентификатор Exchange Active Sync;
- Устройство отображается в Find My (или в аналоге на Android);
- Включён режим "Не беспокоить";
- Включён режим нескольких пользователей;
- Включена связанность устройств в сети;
- Присутствует активный аккаунт iTunes;
- Дата последнего бекапа в облако;

- Версия прошивки модема;
- Персональная точка доступа включена;
- Имя продукта;
- Идентификатор устройства для поиска обновления;
- Какой тип обновлений отображается на устройстве;
- Часовой пояс;
- Способы аппаратного шифрования;
- Корпоративный идентификатор устройства;
- Доступно обновление ОС;
- Дата получения обновления ОС.

2.6.2 Раздел «Сообщения»

Пункт главного меню «Сообщения» предназначен для отображения зарегистрированных сообщений на МСК, выбранном в главном окне, включая SMS и внутренние сообщения (в том числе, фото и голосовые сообщения) согласно рисунку 2.22.

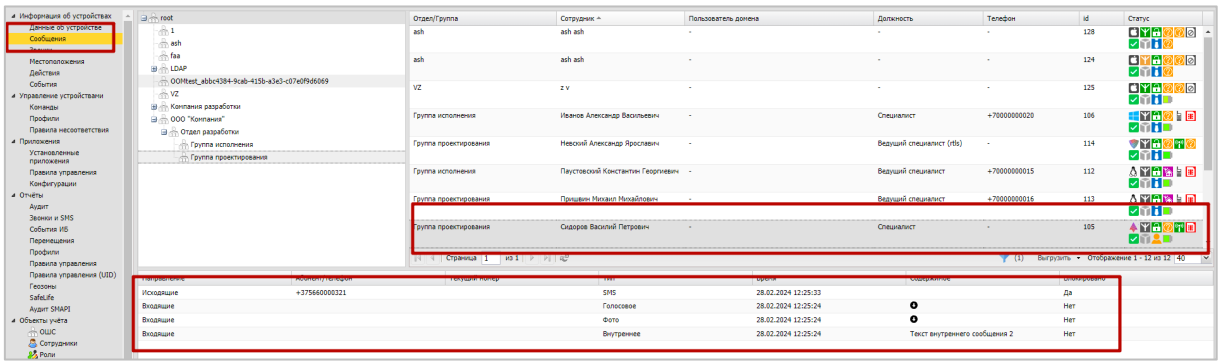


Рисунок 2.22 - Раздел «Сообщения»

Примечание.

Информация о сообщениях доступна только для МСК на платформе Android версии не новее 9.0, при наличии у монитора привилегии владелец устройства (Device Owner).

Информационная таблица раздела «Сообщения» содержит следующие столбцы:

- Направление (входящее или исходящее);
- Абонент/телефон – ФИО сотрудника, если сообщение внутрикорпоративное (абонент зарегистрирован в «UEM SafeMobile»), и номер телефона, если сообщение внешнее;
- Текущий номер – номер телефона SIM-карты МСК (сотрудника, выбранного в главной таблице), с которого получено или на которое отправлено сообщение;
- Тип − тип сообщения: SMS или внутреннее сообщение (текстовое, голосовое, фото);
- Время − время регистрации сообщения;
- Содержимое – в столбце отображается содержимое внутренних сообщений: для внутренних текстовых сообщений – текст, для фото и голосовых сообщений – ссылки, при помощи которых можно скачать соответствующее сообщение. Содержимое SMS сообщений не отображается;
- Блокировано – содержит «Да», если сообщение блокировано политиками безопасности; содержит «Нет», если сообщение не блокировано.

В информационной таблице имеется возможность отображения сообщений в соответствии с выбранным фильтром (рисунок 2.23).

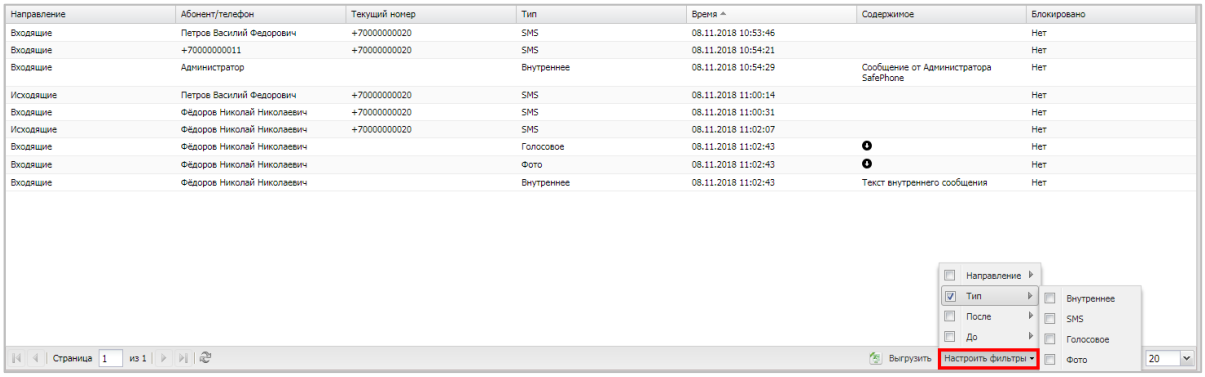


Рисунок 2.23 - Фильтрация сообщений

Чтобы открыть меню настройки фильтрации списка сообщений, следует нажать в нижней панели информационной таблицы кнопку Настроить фильтры, после чего раскроется меню со следующими пунктами:

Направление – установите этот флажок и выберите в появившемся списке, какие сообщения необходимо показать в таблице: Входящие и/или Исходящие.

Тип – установите этот флажок и выберите в появившемся списке типы сообщений, которые необходимо отобразить в таблице: Внутреннее, SMS, MMS, Голосовое или Фото.

После – установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке сообщения, произошедшие после этой даты и времени.

До – установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке сообщения, произошедшие до этой даты и времени.

По умолчанию в таблице показываются все сообщения без фильтрации (флажки в раскрывающемся меню «**Настроить фильтры»** сняты).

Для просмотра/прослушивания внутренних фото и голосовых сообщений, отображающихся в информационной таблице, необходимо нажать значок ⬇ и файл с сообщением скачается в папку Загрузки (Downloads) на ПК. Просмотреть скачанные файлы можно в любом прикладном ПО, предназначенном для просмотра файлов формата JPG и прослушивания файлов формата AMR.

Примечание.

Действия при скачивании файлов могут отличаться в зависимости от настроек используемого браузера.

2.6.3 Раздел «Звонки»

В разделе «Звонки» отображаются сведения о зарегистрированных в системе звонках, выполненных с/на МСК, выбранное в главной таблице в соответствии с рисунком 2.24.

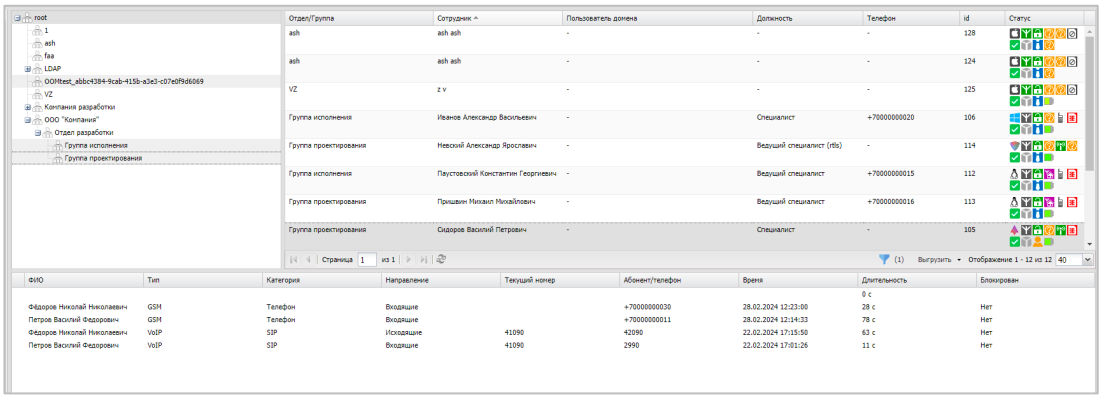


Рисунок 2.24 - Раздел «Звонки»

Примечание.
Информация о звонках доступна только для МСК на платформе Android версии не новее 9.0, при наличии у монитора привилегии владелец устройства (Device Owner).

Информационная таблица раздела «Звонки» содержит следующие столбцы:

- ФИО – фамилия, имя и отчество абонента, которому или от которого был выполнен звонок на МСК, выбранное в главной таблице;
- Тип – тип связи, использованный при выполнении звонка – GSM (для незащищенных звонков) или VoIP (для защищенных звонков);
- Категория – категория вызова: Телефон, SIP, УПАТС;
- Направление – входящий или исходящий звонок;
- Текущий номер – номер телефона SIM-карты МСК (сотрудника, выбранного в главной таблице), с которого или на который выполнялся вызов;
- Абонент/Телефон (номер вызываемого или позвонившего абонента) – отображается ФИО сотрудника, если звонок корпоративный (абонент зарегистрирован в «UEM SafeMobile»), и номер телефона, если звонок внешний. Если в столбце отображается ФИО, то при наведении на него курсора мыши отображается подсказка, содержащая номер телефона;
- Время – дата и время звонка;
- Длительность – продолжительность звонка в секундах;
- Блокирован – столбец содержит значок блокирования, если звонок был блокирован политиками безопасности, в противном случае отображается сообщение «Нет».

В информационной таблице имеется возможность отображения звонков в соответствии с выбранным фильтром (рисунок 2.25).

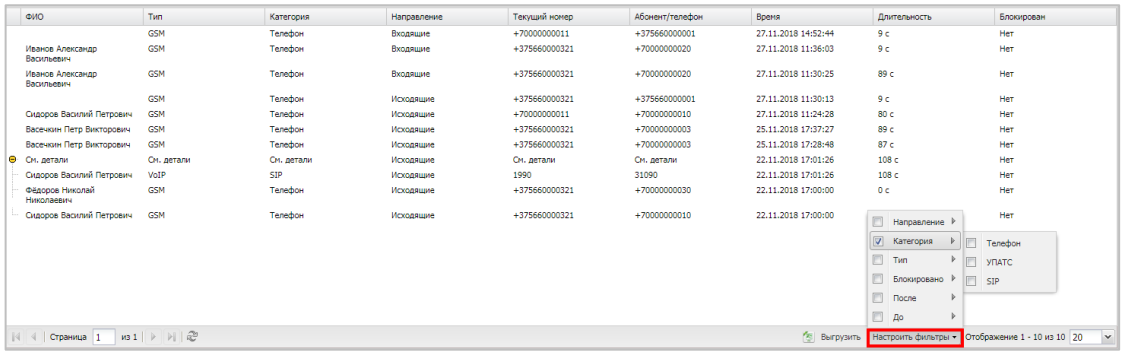


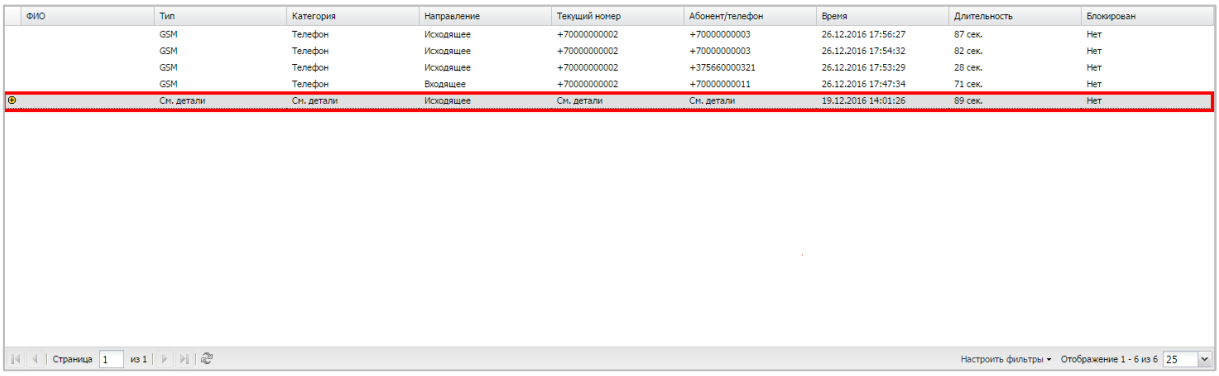
Рисунок 2.25 - Фильтрация звонков

Чтобы открыть меню настройки фильтрации списка звонков, следует нажать в нижней панели информационной таблицы кнопку «**Настроить фильтры**», после чего отобразятся меню со следующими пунктами:

- **Направление** – установите этот флажок и выберите в появившемся списке, какие звонки необходимо показать в таблице: **Входящие** и/или **Исходящие**.
- **Категория** – установите этот флажок и выберите в появившемся списке категорию звонков для отображения в таблице: **Телефон**, **УПАТС**, **SIP**.
- **Тип** – установите этот флажок и выберите в появившемся списке типы звонков, которые необходимо отобразить в таблице: GSM (незащищенные) или VoIP (защищенные);
- **Блокировано** – позволяет отображать записи о звонках в зависимости от признака их блокировки.
- **После** – установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке звонки, выполненные после этой даты и времени.
- **До** – установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке звонки, выполненные до этой даты и времени.

По умолчанию в таблице показываются все звонки без фильтрации (флажки в раскрывающемся меню **«Настроить фильтры»** сняты).

Вызовы, относящиеся к единому номеру абонента, отображаются в таблице звонков в виде сгруппированных элементов. В этом случае в столбцах **«Категория»** и **«Абонент/телефон»** отображается сообщение **«См. детали»** в соответствии с рисунком 2.26.



ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
	GSM	Телефон	Исходящее	+70000000002	+70000000003	26.12.2016 17:56:27	87 сек.	Нет
	GSM	Телефон	Исходящее	+70000000002	+70000000003	26.12.2016 17:54:32	82 сек.	Нет
	GSM	Телефон	Исходящее	+70000000002	+375660000321	26.12.2016 17:53:29	28 сек.	Нет
	GSM	Телефон	Входящее	+70000000002	+70000000011	26.12.2016 17:47:34	71 сек.	Нет
	См. детали	См. детали	Исходящее	См. детали	См. детали	19.12.2016 14:01:26	89 сек.	Нет

Рисунок 2.26 - Звонок на единый номер в свернутом виде

Чтобы просмотреть дополнительные сведения обо всех звонках, содержащихся в едином звонке на номер абонента, нажмите значок , после чего записи о звонках будут развернуты в таблице, как показано на рисунке 2.27.

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
	GSM	Телефон	Входящие	+70000000011	+375660000001	27.11.2018 14:52:44	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящие	+375660000321	+70000000020	27.11.2018 11:36:03	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящие	+375660000321	+70000000020	27.11.2018 11:30:25	89 с	Нет
	GSM	Телефон	Исходящие	+375660000321	+375660000001	27.11.2018 11:30:13	9 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящие	+70000000011	+70000000010	27.11.2018 11:24:28	80 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящие	+375660000321	+70000000003	25.11.2018 17:37:27	89 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящие	+375660000321	+70000000003	25.11.2018 17:28:48	87 с	Нет
См. детали	См. детали	См. детали	Исходящие	См. детали	См. детали	22.11.2018 17:01:26	108 с	Нет
Сидоров Василий Петрович	VoIP	SIP	Исходящие	1990	31090	22.11.2018 17:01:26	108 с	Нет
Фёдоров Николай Николаевич	GSM	Телефон	Исходящие	+375660000321	+70000000030	22.11.2018 17:00:00	0 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящие	+375660000321	+70000000010	22.11.2018 17:00:00	0 с	Нет

Рисунок 2.27 - Звонок на единый номер в развернутом виде

2.6.4 Раздел «Местоположения»

Раздел «Местоположения» отображает фрагмент карты, на которой в виде ломаной линии отображена информация о местоположении и перемещении абонента. Кроме того, эта информация выводится в виде таблицы с координатами абонента в определенный момент времени в соответствии с рисунком 2.28.

В правой части информационной таблицы раздела «Местоположения» расположен реестр координат точек маршрута перемещений абонента МСК, а также время регистрации координат МСК в каждой указанной точке маршрута.

Для изменения масштаба карты (увеличения или уменьшения изображения) используется шкала масштабирования, расположенная в верхнем левом углу карты. Кроме того, масштаб изображения можно изменять, используя вращение колеса мыши, если курсор расположен в области карты.

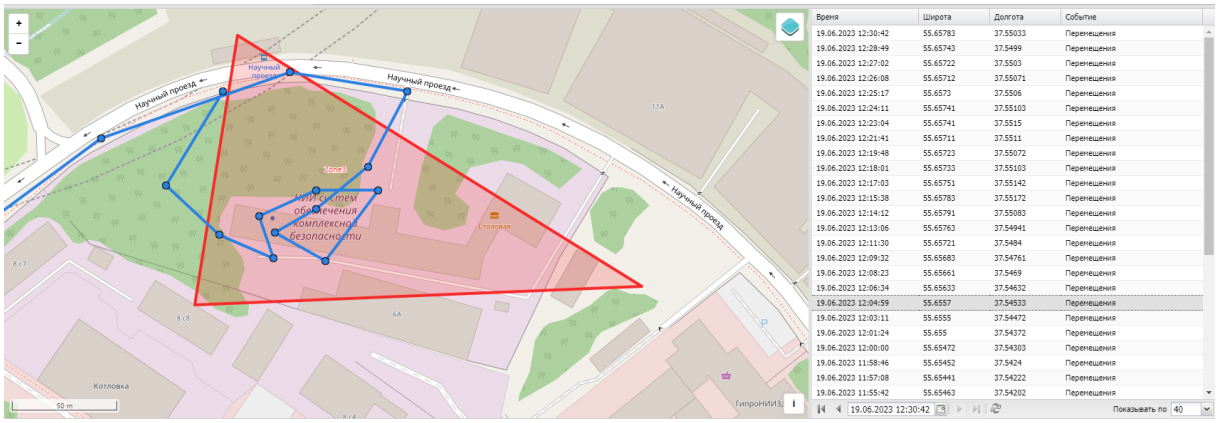


Рисунок 2.28 - Раздел «Местоположения»

При нажатии на значок в правой верхней части карты отображается меню настройки отображения информации на карте (рисунок 2.29).

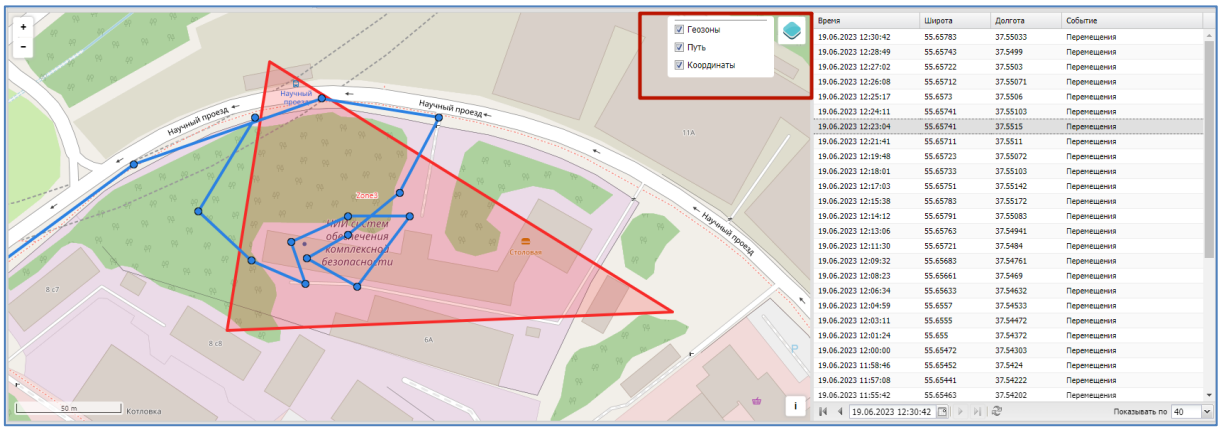


Рисунок 2.29 - Настройка режима отображения информации о местоположении абонента на карте

В меню расположены флажки, позволяющие выбрать слои отображения графической информации на карте (можно выбрать все параметры одновременно):

- Геозоны;
- Путь;
- Координаты.

При установленном флажке **«Геозоны»** на карте отображаются созданные области (описание приведено в 2.8.10), с установленными параметрами и ограничениями для применения на МСК. При установленном флажке **«Путь»** на карте отображается линия перемещения абонента. При установленном флажке **«Координаты»** в точках местоположения абонента выводятся координаты абонента.

Кроме того, меню позволяет выбрать источник картографической информации (сервер ГИС), который используется для отображения карты, по умолчанию: openstreetmap.org.

В информационной таблице имеется возможность отображения реестра координат местоположения абонента в соответствии с сортировкой по колонкам таблицы и настроек пагинации реестра (рисунок 2.30).

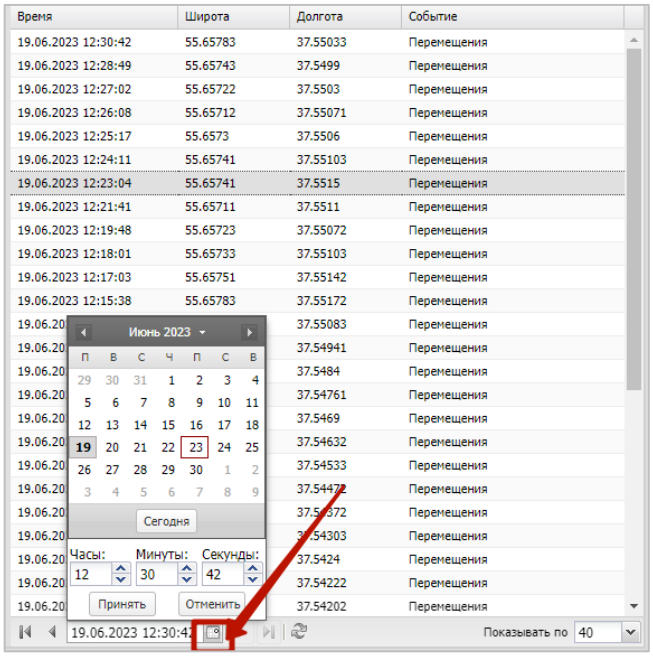
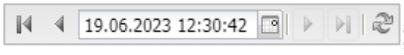


Рисунок 2.30 - Фильтрация местоположений абонента

Настройки пагинации реестра координат позволяют просматривать записи изменения координат, с указанного времени и даты. Чтобы задать дату и время необходимо выполнить следующие действия:

1. Нажать кнопку , после чего откроется модальное окно выбора даты и времени;

2. Ввести дату и время. Так же ввести дату и время допустимо напрямую, в строке отображения даты и времени 

;

3. Нажать кнопку «Принять», после чего реестр отобразит страницу данных изменения координат, совершенные после указанной даты и времени.

Для удобства работы со списком рекомендуется указывать необходимое количество записей на одной странице в соответствующем поле настройки пагинации.

Для просмотра отчётов о местоположении одного или нескольких абонентов в заданных интервалах времени следует использовать отчёт **«Перемещения»**, более подробные сведения о котором приведены в п. 2.7.4.

Примечание

Определение местоположения сотрудника и его комплекта выполняется только в рабочее время. Для того чтобы появилась такая возможность необходимо, чтобы у сотрудника или подразделения, в котором он работает, был настроен календарь рабочего времени в соответствующем разделе АРМ Администратора SafeMobile, более подробное описание которого приведено в п.2.11.

На карте имеется возможность просмотра местоположения сотрудника в выбранной точке траектории его передвижения. Для этого необходимо выбрать точку траектории, чтобы отобразить во всплывающем окне имя сотрудника и время его нахождения в этой точке местности (рисунок 2.31).

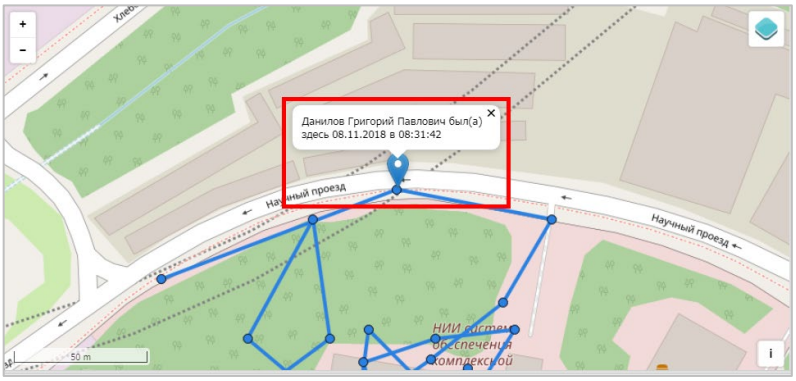


Рисунок 2.31 - Местонахождение сотрудника в выбранной точке траектории перемещения

2.6.5 Раздел «Действия»

Раздел **«Действия»** предназначен для просмотра команд, выполненных на выбранном МСК.

Для просмотра журнала действий следует выбрать пункт главного меню **«Действия»**, а затем требуемое устройство в главной таблице. В информационной таблице отобразится журнал действий в соответствии с рисунком 2.32.

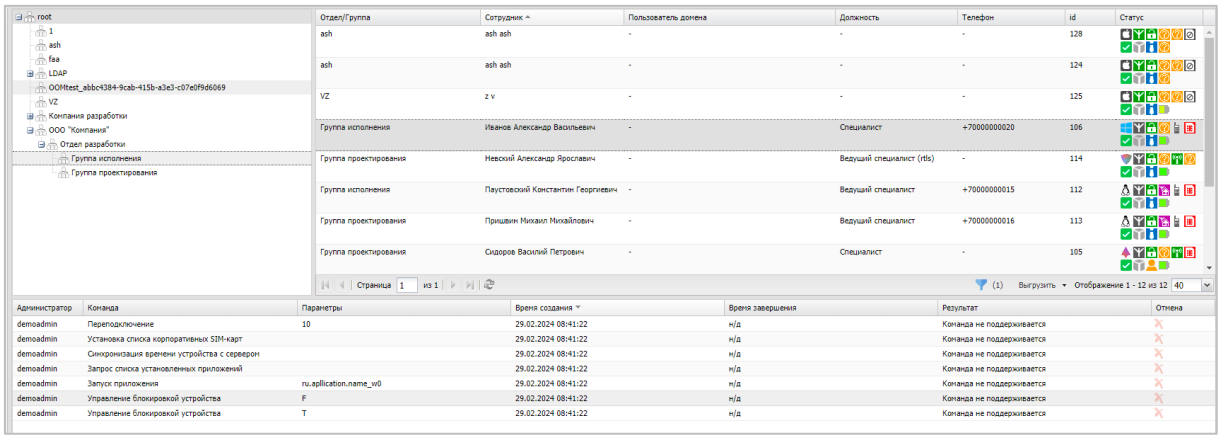


Рисунок 2.32- Раздел «Действия»

Информационная таблица раздела «Действия» содержит следующие столбцы:

- Администратор − имя пользователя (логин), который отправил команду на МСК, выбранное в главной таблице. Отсутствие имени пользователя (логина), указывает на то, что команда отправлена с МСК;
- Команда – команда, отправленная на МСК;
- Параметры – параметры команды (если есть);
- Время создания – время создания команды;
- Время завершения – время выполнения команды;
- Результат – результат выполнения команды;
- Отмена – в столбце отображается значок, позволяющий выполнить отмену отправленной на устройство команды, если значок отмены команды активен. Отменить команду можно пока не был получен её результат. Если команда завершена со статусом «Нормальное завершение» или завершена из-за ошибки (сбоя) устройства (или ПО), отменить команду невозможно (значок отмены неактивен).

В информационной таблице имеется возможность отображения журнала действий в соответствии с выбранным фильтром (рисунок 2.33).

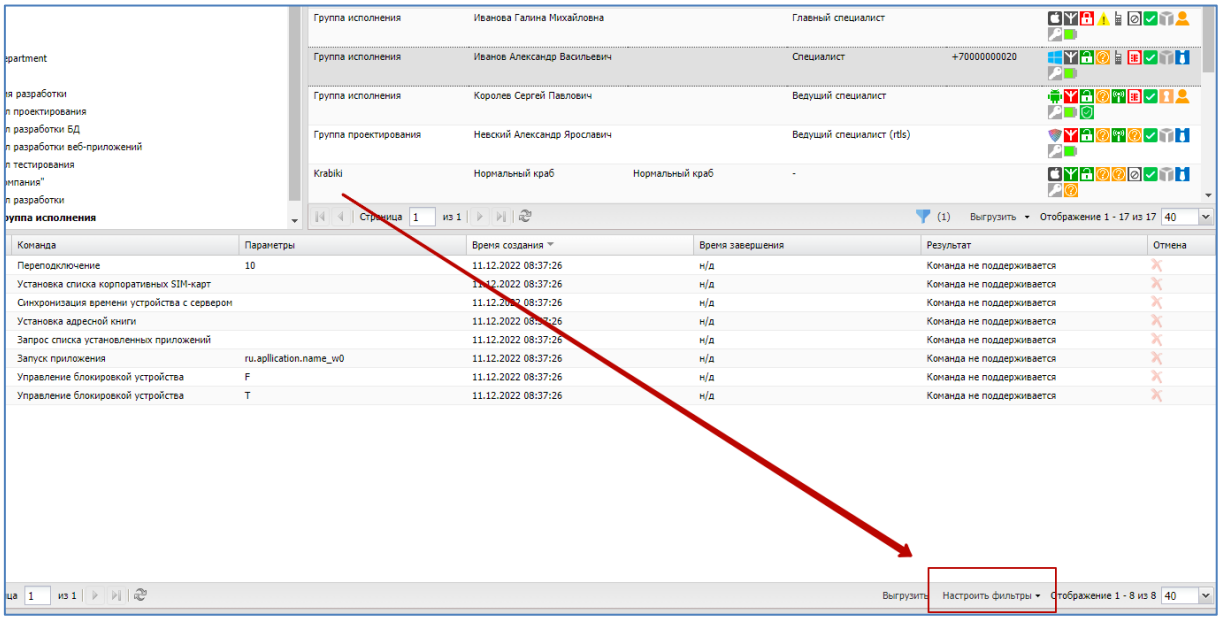


Рисунок 2.33 - Фильтрация действий

Чтобы открыть меню настройки фильтрации списка действий, нажмите кнопку Настроить фильтры, после чего отобразятся следующие пункты меню в соответствии с рисунком 2.33:

Команда – установка флажка позволяет выбрать в появившемся списке команды, которые необходимо отобразить в таблице. В списке присутствуют команды, исключенные из полномочий системы, но сохраненные для обеспечения целостности журнала команд МСК;

Результат – установка флажка позволяет выбрать в появившемся списке результаты выполнения команд, которые необходимо отобразить в таблице;

Создано после – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, созданные после этой даты и времени;

Создано до – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, созданные до этой даты и времени;

Завершено после – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, завершенные после этой даты и времени;

Завершено до – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, завершенные до этой даты и времени.

По умолчанию в таблице показываются все действия без фильтрации (флажки в раскрывающемся меню **«Настроить фильтры»** сняты).

Перечень команд и описание их параметров приведены в п. 2.6.7.

Отправка команд на устройства осуществляется Администратором посредством раздела главного меню **«Команды»**, описание которого приведено в п. 2.6.7.

2.6.6 Раздел «События»

Раздел **«События»** предназначен для просмотра журнала событий на выбранном МСК. Информационная таблица раздела «События» содержит следующие столбцы в соответствии с рисунком 2.34:

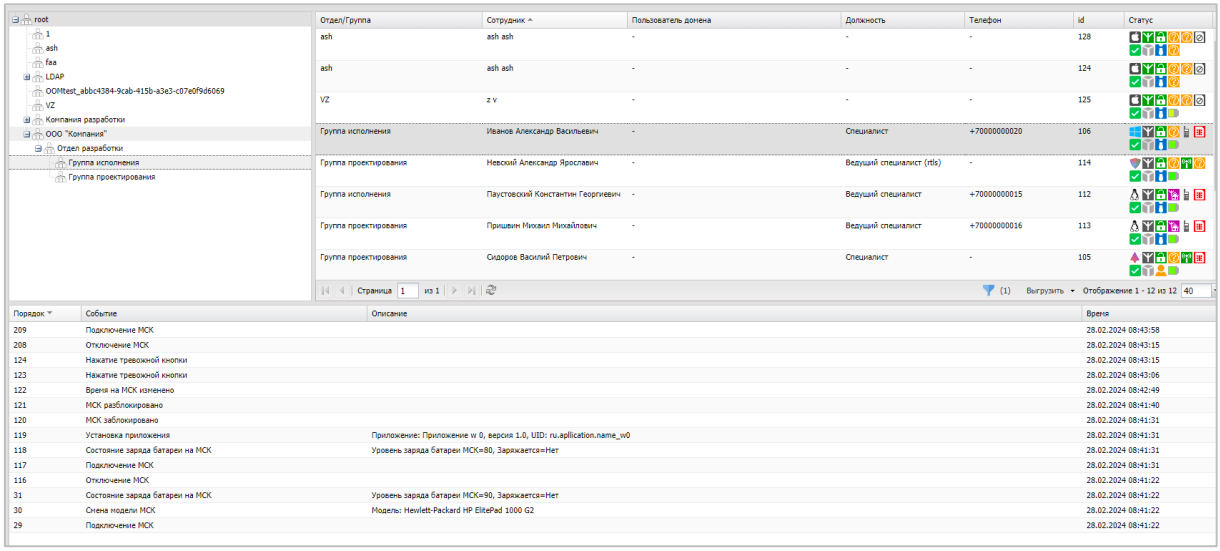


Рисунок 2.34 - Раздел «События»

- Порядок – порядковый номер события в общем журнале событий;
- Событие – тип события;
- Описание – параметры события;
- Время – время и дата регистрации события.

В информационной таблице имеется возможность отображения журнала событий в соответствии с выбранным фильтром (рисунок 2.35).

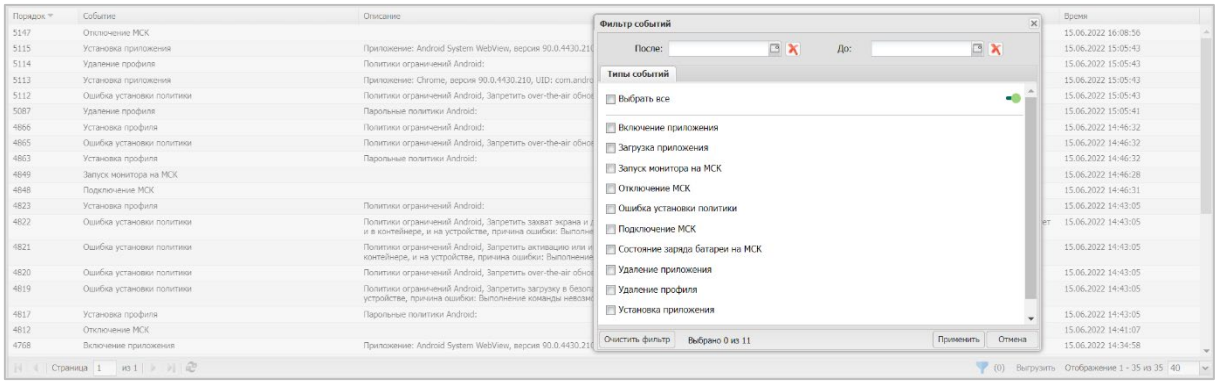


Рисунок 2.35 - Фильтрация событий

Чтобы открыть меню настройки фильтрации списка событий, нажмите кнопку настройки фильтра (рисунок 2.36), после чего отобразятся следующие пункты меню:

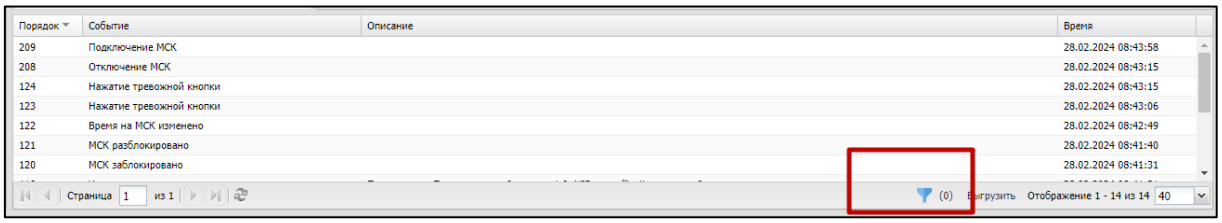


Рисунок 2.36 - Кнопка настройки фильтров

Типы событий – установка флажка позволяет выбрать в появившемся списке типы событий, которые необходимо отобразить в таблице. В списке отображаются только те события, которые хоть раз происходили с МСК;

После – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке события, произошедшие после этой даты и времени;

До – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке события, произошедшие до этой даты и времени.

По умолчанию в таблице показываются все события без фильтрации (флажки в раскрывающемся меню **«Настроить фильтры»** сняты).

Для выгрузки событий необходимо нажать кнопку ***«Выгрузить»*** на нижней панели инструментов. Если отчет содержит менее 10000 записей, то выгрузка производится в формате XLSX. Если отчет содержит более 10000 записей, то выгрузка производится в формате CSV. По завершении формирования отчета появится сообщение о готовности отчета, в котором будет необходимо нажать кнопку ***«Скачать».***

В таблице 2.2 приводится краткое описание событий «UEM SafeMobile».

В столбце «Платформа» указаны значки платформ МСК, для которых актуально указанное событие «UEM SafeMobile».

Таблица 2.2 – Краткое описание событий

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Подключение МСК	Нет		Подключение МСК к «UEM SafeMobile»	Отсутствуют
Отключение МСК	Нет		Отключение МСК от «UEM SafeMobile»	Отсутствуют
Установка приложения	Нет		Приложение установлено на МСК	Название приложения, его версия и UID
Удаление приложения	Нет		Приложение удалено с МСК	Название приложения, его версия и UID

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Запуск монитора на МСК	Да		Мобильный клиент SafeMobile запущен на устройстве	Отсутствуют
Состояние заряда батареи на МСК	Нет		Отчёт об изменении уровня заряда батареи	Уровень заряда батареи в процентах от уровня полного заряда и признак подключенного ЗУ (T − подключено, F− не подключено)
SIM-карта изменена	Да		На устройстве произошла смена SIM-карты	ICCID/IMSI старой SIM-карты, номер телефона (если определен), ICCID/IMSI новой SIM-карты, признак возможности блокировки МСК (T − мобильный клиент заблокирует устройство, F− не заблокирует)
Время на МСК изменено	Нет		На устройстве изменено значение системного времени	Значение установленного времени (временная метка в миллисекундах от 1970 года по Гринвичу)

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Очистка БД от старых подключений	Нет		При завершении работы сервера управления SafeMobile (например, при его отключении) все МСК, подключенные к нему, остаются в подключенном состоянии. При следующем запуске сервера управления SafeMobile, эти МСК отмечаются в БД как отключенные (что представляет собой процедуру очистки БД от старых подключений)	Отсутствуют
Несоответствие IMSI/ICCID хранимому в БД	Да		Определено, что в БД для данного МСК хранится иной идентификатор SIM-карты	ICCID/IMSI старой SIM, ICCID/IMSI новой SIM
Смена модели МСК	Да		Определено, что в БД данному МСК соответствует иная модель устройства	Новая модель МСК
Ошибка при обработке пакета	Да		В ходе регистрации события, поступившего от МСК, произошла ошибка (сбой при обработке пакета, отправленного от МСК на сервер управления SafeMobile)	Отсутствуют

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
SIM-карта извлечена	Нет		На устройстве произошло извлечение SIM-карты	ICCID/IMSI извлеченной SIM
SIM-карта установлена	Да		На устройстве произошла установка SIM-карты	ICCID/IMSI установленной SIM
МСК за пределами домашней сети GSM	Нет		Устройство переместилось за пределы домашней сети GSM (находится в роуминге)	ICCID/IMSI SIM
МСК в пределах домашней сети GSM	Нет		Устройство находится в домашней сети GSM (вернулось из роуминга)	ICCID/IMSI SIM
Принадлежность сети GSM не определена	Нет		Устройство не может определить, находится ли оно в домашней сети или в роуминге. Такая ситуация возможна сразу после установки новой SIM-карты в устройство	ICCID/IMSI SIM с нулевыми значениями
GSM не поддерживается	Нет		На устройстве отсутствует модуль GSM	ICCID/IMSI SIM с нулевыми значениями
МСК заблокировано	Да		Блокировка МСК по команде Администратора или применению политик работы с SIM-картами	Признаки блокировки по команде Администратора и по политикам работы с SIM

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
МСК разблокировано	Да		Разблокировка (удаленный сброс пароля) МСК по команде Администратора	Признаки блокировки по команде Администратора и по политикам работы с SIM
Сброс МСК к заводским настройкам	Да		Сброс МСК к заводским настройкам по команде Администратора «Отключение от управления со сбросом к заводским настройкам»	id и действие с командой удаления данных
Нажатие тревожной кнопки	Да		Пользователь МСК выполнил нажатие тревожной кнопки	Признаки работы под принуждением и физического нападения
Выход МСК из-под управления	Да		Отключение МСК от управления с удалением корпоративных данных средствами «UEM SafeMobile»	Отсутствуют
Взлом устройства	Да		Обнаружение признаков взлома (jailbreak − МСК iOS, root − МСК Android) мобильным клиентом SafeMobile	Отсутствуют
Изменение UDID устройства	Да		Изменение идентификатора при замене устройства в составе зарегистрированного в «UEM SafeMobile» комплекта	UDID старого устройства, UDID нового устройства
Установка профиля управления	Да		Установка профиля управления на МСК	Отсутствуют

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Включение приложения	Нет		Включение установленного приложения на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Отключение приложения	Нет		Отключение включенного приложения на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Создание контейнера	Нет		Создание изолированной области на МСК для корпоративных приложений (данных)	Тип контейнера
Удаление контейнера	Нет		Удаление изолированной области на МСК для корпоративных приложений (данных)	Признак удаления контейнера
Установка приложения в контейнер	Нет		Приложение установлено в контейнер на МСК	Название приложения, его версия и UID
Удаление приложения из контейнера	Нет		Приложение удалено из контейнера на МСК	Название приложения, его версия и UID
Включение приложения в контейнере	Нет		Включение установленного приложения в контейнере на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Отключение приложения в контейнере	Нет		Отключение включенного приложения в контейнере на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Подтверждение пользовательского соглашения	Нет		Пользователь подтвердил согласие с условиями управления МСК «UEM SafeMobile»	Признак действия с соглашением: соглашение подтверждено / соглашение отклонено

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Установка профиля	Нет		Установка на МСК заданных в профиле настроек ОС	Название профиля
Профиль не установлен (нет значения подстановки)	Нет		При установке на МСК настроек ОС произошла ошибка из-за отсутствия значения, заданного в профиле	Название профиля, причина ошибки, подстановка и ее значение
Ошибка формирования профиля (подстановки не соответствуют ограничениям)	Нет		При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки, подстановка и ее значение
Ошибка установки профиля	Нет		При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки
Удаление профиля	Нет		Удаление с МСК заданных в профиле настроек ОС	Название профиля

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка удаления профиля	Нет		При удалении с МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки
Ошибка установки политики	Нет		При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Тип профиля, название политики, причина ошибки
Установка конфигурации приложения	Нет		Установка на МСК заданных в конфигурации настроек приложения	Наименование ПУН (при наличии), UID ПУН, название КП
Ошибка формирования конфигурации приложения (подстановки не соответствуют ограничениям)	Нет		При установке на МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки, значение настройка, подстановка и ее значение
Ошибка установки конфигурации приложения	Нет		При установке на МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки
Удаление конфигурации приложения	Нет		Удаление с МСК заданных в конфигурации настроек приложения	Наименование ПУН (при наличии), UID ПУН, название КП
Ошибка удаления конфигурации приложения	Нет		При удалении с МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Активация лицензии Knox	Нет		Активация лицензии Knox на МСК посредством введения Knox ключей	Лицензия Knox активирована
Ошибка активации лицензии Knox	Нет		При активации лицензии Knox на МСК произошла ошибка при вводе ключа или пользователь МСК отклонил действие. Ошибка возникает также при отсутствии доступа к серверам Samsung	Причина ошибки
Ошибка создания контейнера	Нет		При создании контейнера на МСК произошла ошибка или пользователь отклонил действие. Если на МСК Samsung был установлен Knox warranty bit в результате проведения незаводской прошивки, то создание контейнера будет невозможно, и в АРМ администратора отобразится ошибка	Тип контейнера, причина ошибки
Регистрация пульса	Нет		На смарт-браслете измерена частота сердечных сокращений сотрудника, на котором этот браслет одет	Значение частоты сердечных сокращений (ударов в минуту)
Зафиксировано падение	Нет		Зафиксировано падение сотрудника с надетым смарт-браслетом	Отсутствуют
Показания тонометра	Нет		На смарт-браслете измерено артериальное давление сотрудника, на котором этот браслет одет	Значение давления (мм рт.ст.)

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка установки приложения	Нет		При установке приложения на МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка удаления приложения	Нет		При удалении приложения с МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка установки приложения в контейнер	Нет		При установке приложения в контейнер МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка удаления приложения из контейнера	Нет		При удалении приложения из контейнера МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Применение правила управления приложением	Нет		Применение правила управления приложением	Название приложения, его UID
Ошибка применения правила управления приложением	Нет		При применении правила управления приложения возникла ошибка	Название приложения, его UID, причина ошибки
Удаление правила управления приложением	Нет		Удаление правила управления приложением	Название приложения, его UID
Ошибка удаления правила управления приложением	Нет		При удалении правила управления приложения возникла ошибка	Название приложения, его UID, причина ошибки
Включение VPN	Нет		Подключение к сети VPN	

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Выключение VPN	Нет		Отключение от сети VPN	
Регистрация IP адреса	Нет		Определение IP адреса в сети сотового оператора	Название сотового оператора, IP адрес
Установка ключевого дистрибутива VipNet	Нет		При подключении к приложению ViPNet устанавливается ключевой дистрибутив из файла	Название файла ключевого дистрибутива
Ошибка подключения к VipNet	Нет		При подключении к приложению «ViPNet Client» возникла ошибка	Причина ошибки
Ошибка установки ключевого дистрибутива VipNet	Нет		При установке ключевого дистрибутива VipNet возникла ошибка или пользователь отклонил запрос	Причина ошибки
Ошибка валидации Knox ключей	Нет		При валидации ключей произошла ошибка из-за некорректного значения ключа	Причина ошибки
Приложение не может быть добавлено в киоск	Нет		При добавлении приложения в киоск произошла ошибка	Название приложения, его версия и UID, причина ошибки
Пуш токен недействителен	Нет		Не поступают уведомления из-за некорректного значения пуш токена	Причина ошибки
Нет движения	Нет		На устройстве отсутствует информации о передвижении	

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка синхронизации	Нет		При получении устройством профиля/ПУП/КП произошла ошибка	Устройство / контейнер, причина ошибки
Ошибка скачивания приложения	Нет		При скачивании корпоративного приложения возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка определения SIM-карты	Нет		При определении параметров SIM карты возникла ошибка	Причина ошибки
Запрос SafeStore на установку приложения	Нет		Пользователь через приложение SafeStore запросил установку приложения	Название приложения, его UID.
Запрос SafeStore на удаление приложения	Нет		Пользователь через приложение SafeStore запросил удаление приложения	Название приложения, его UID.
Загрузка приложения	Н		В процессе применение ПУП монитор скачивает корпоративное приложение	Название приложения, его версия и UID
Зарегистрирована корпоративная SIM-карта	Нет		В соответствии с политикой профиля настроек монитора первая установленная SIM карта зарегистрирована как корпоративная	IMSI: {{IMSI}}, ICCID: {{ICCID}}
Ошибка подключения к серверу	Нет		При подключении монитора к серверу системы произошла ошибка	Тип сервера, URL сервера, причина ошибки

2.6.7 Раздел «Команды»

Раздел **«Команды»** предназначен для отображения списка команд и отправки требуемой команды на выбранное устройство.

Для отправки команды необходимо выбрать МСК в главной таблице, затем пункт меню **«Команда»** и требуемую команду в информационной таблице в соответствии с рисунком 2.37.

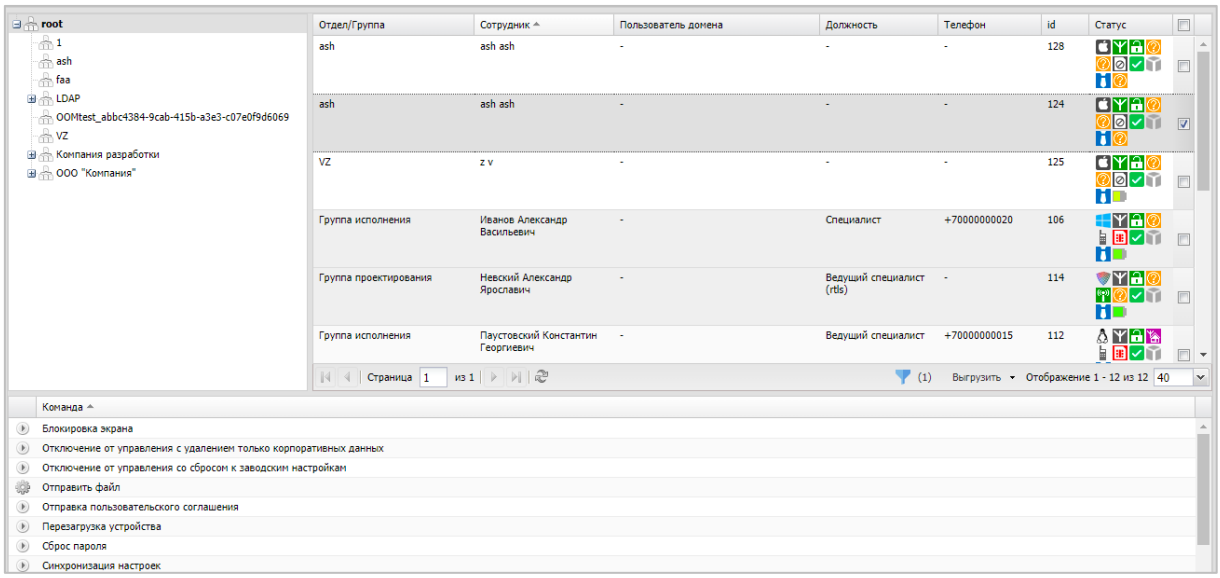


Рисунок 2.37 - Раздел «Команды»

Если команда выполняется без параметров, слева от названия команды отображается значок . Для отправки команды на устройство необходимо нажать этот значок, после чего в появившемся окне уведомления нажать кнопку **«ОК»** (рисунок 2.38).

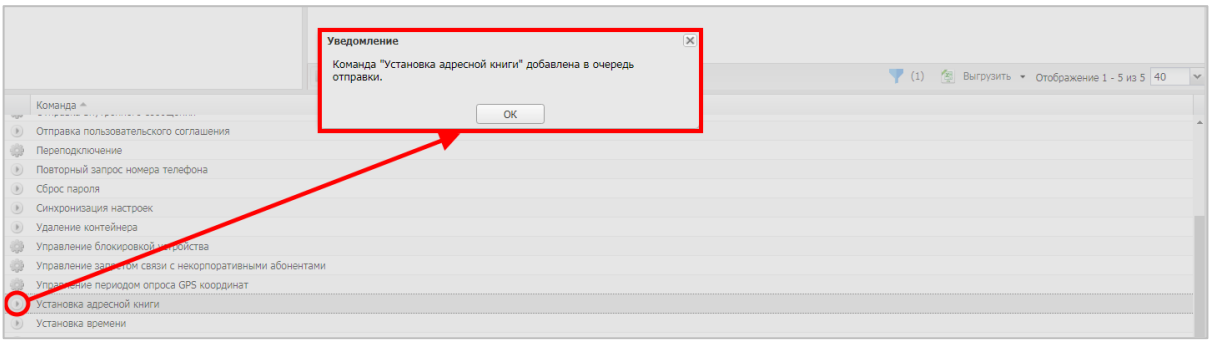


Рисунок 2.38 - Отправка команды без параметров

Если для выполнения команды требуется указать ее параметры, слева от названия команды отображается значок (рисунок 2.39).

Для отображения параметров команды следует нажать этот значок, после чего в правой части таблицы появится перечень параметров команды. Чтобы отправить команду, установите требуемые значения параметров, нажмите кнопку **«Отправить»**, затем кнопку **«ОК»** в появившемся окне уведомления.

Рисунок 2.39 - Отправка команды с параметрами

Результат выполнения команды отображается в разделе главного меню **«Действия»**. В этом разделе можно также выполнить отмену отправленной на устройство команды. Если выполнение команды прошло успешно, в столбце **«Результат»** отобразится значение **«Нормальное завершение»**. В противном случае, будет отображена причина невыполнения команды.

Полный перечень возможных ошибок и их описание приведен в приложении Б.

В таблице 2.3 приводится краткое описание команд системы.

В столбце «Платформа» таблицы 2.3 указаны значки платформ МСК, для которых актуальна указанная команда системы.

Администратор может отправить из раздела главного меню «Установленные приложения» команды по работе с приложениями.

Таблица 2.3 – Краткое описание команд

Команда	Плат-форма	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Управление блокировкой устройства		При получении команды **«Заблокировать устройство»** осуществляется полная блокировка устройства с отображением сообщения о блокировке и передаче устройства администратору для разблокировки. Команда выполняется на устройствах в режиме Supervised, на других устройствах результатом выполненной команды будет «Нарушение защиты ОС».	Заблокировать устройство	**T**
		При получении команды **«Заблокировать устройство»** осуществляется блокировка доступа к пользовательскому интерфейсу МСК. Команда не выполняется на устройствах с действующими стратегиями КРП и ЛРП. Результатом выполнения команды на этих устройствах будет «Выполнение команды невозможно».		
		При получении команды **«Разблокировать устройство»** осуществляется разблокировка устройства. Команда выполняется на устройствах с Supervised.	Разблокировать устройство	**F**
		При получении команды **«Разблокировать устройство»** осуществляется снятие блокировки доступа к пользовательскому интерфейсу МСК		
Блокировка экрана		При получении команды осуществляется блокировка экрана паролем пользователя	Отсутствуют	

Команда	Плат-форма	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Отправка внутреннего сообщения		На устройство отправляется созданное внутреннее сообщение. Для успешного выполнения команды на устройстве должно быть установлено приложение SafeMessages, идущее в комплекте поставки SafeMobile.	Текст сообщения	Порядковый номер сообщения
Переподключение		На устройство отправляется команда отключения и подключения заново мобильного клиента к серверу SafeMobile	Промежуток времени, указывающий, через сколько секунд МСК подключится к серверу заново после выполнения этой команды	
Установка списка корпоративных SIM-карт		На устройство отправляется актуальный список идентификаторов SIM, хранящихся в БД SafeMobile. Это действие применяется для обеспечения корректной работы устройств с установленной политикой смены SIM-карт	Отсутствуют	
Установка графика рабочего времени		На МСК отправляется команда установки графика рабочего времени для сотрудника-абонента МСК	Отсутствуют	
Синхронизация времени устройства с сервером*		На устройство отправляется команда установки текущего времени на сервере SafeMobile	Отсутствуют	

* Команда актуальна для МСК производства Samsung до Android 11 включительно, а также для устройств Android начиная с версии– 9.0 при наличии у монитора прав DO или корпоративного рабочего профиля.

Команда	Плат-форма	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Отключение от управления с удалением только корпоративных данных**		На МСК отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на МСК будет удалён профиль управления (на устройствах платформы iOS), а также все настройки (параметры Wi-Fi точек доступа, запрещающие правила доступа к интерфейсам, парольные политики, контейнер) и приложения, установленные «UEM SafeMobile». Личные данные сотрудника сохранятся	Отсутствуют	
Отключение от управления со сбросом к заводским настройкам***		На МСК отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на МСК будут удалены корпоративные и личные данные (настройки, журналы звонков и сообщений, файлы, приложения, контейнер) Если мобильный клиент Android не успел сообщить серверу об успешном завершении команды, тогда команда с результатом "Команда доставлена, ожидается результат" останется в системе на срок до 90 суток и будет удалена при периодической очистке БД. При повторном подключении устройства посредством КМЕ в указанный период команда отобразится с результатом «Нормальное завершение»	Отсутствуют	
Сброс пароля		На устройство отправляется команда сброса пароля. Если к устройству платформы Android уже предъявлены требования парольной политики, а именно:	Отсутствуют	

** На устройствах платформы Android после выполнения данной команды монитор останется с отключенным функционалом. Если монитор имел права Device Owner, пользователь не сможет удалить монитор ничем кроме сброса к заводским настройкам. Если требуется удалить монитор с правами Device Owner, рекомендуется отправлять команду «Отключение от управления со сбросом к заводским настройкам».

*** При наличии шифрования диска МСК с данными для ОС Windows 10.

Команда	Плат-форма	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
		минимальная длина пароля и категория сложности, перед сбросом пароля эти требования следует отменить. На МСК с ОС Android версий 8.0 и 8.1 команда не поддерживается производителем Samsung		
Изменение пароля		На устройство отправляется команда изменения текущего пароля на полученный. На МСК с ОС Android версий 8.0 и 8.1 команда не поддерживается производителем Samsung	Новый пароль	
Изменение пароля контейнера		На устройство отправляется команда изменения текущего пароля контейнера на полученный новый пароль	Новый пароль	
Отправка пользовательского соглашения		На устройство отправляется пользовательское соглашение по управлению МСК «UEM SafeMobile»	Отсутствуют	Порядковый номер пользовательского соглашения
Перезагрузка устройства		На устройство оправляется команда перезагрузки устройства. Если устройство находится в состоянии звонка, то перезагрузка произойдет: • после его окончания (для Android и iOS); • во время звонка (для Аврора). Для Android – устройство должно удовлетворять требования: • Android 7+ и наличие привилегии Device Owner или NKOX.	Отсутствуют	

Команда	Плат-форма	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Удаление контейнера		На устройство отправляется команда удаления изолированной области с корпоративными приложениями и данными.	Отсутствуют	
Синхронизация настроек		На устройство отправляются актуальные настройки ОС и приложений, заданные в профилях и конфигурациях	Отсутствуют	
Повторный запрос номера телефона		МСК, получив команду, отправляет сообщение на номер телефона, заданный в профиле настроек монитора. По полученному сообщению, автоматически определяется номер телефона. На МСК, определяющий номер телефона, должен быть назначен профиль настроек монитора с политикой "Регистрировать SMS" = Да.	Отсутствуют	
Отправить файл		На устройство отправляется файл. По получении пользователь уведомляется и файл выкладывается в папку «Загрузки».	Файл, предназначенный для отправки.	
Установить последнее обновление ОС		Команда позволяет установить последнее доступное для устройства обновление ОС. ***Примечание***. *Для устройств **IOS,** работающих в режиме **unsupervised,** нормальным результатом работы команды является оповещение "Команда не поддерживается".*	Отсутствуют	

2.6.8 Раздел «Профили»

Пункт меню **«Профили»** открывает окно (рисунок 2.40), предназначенное для создания, редактирования и удаления профилей, а также осуществления их назначений на МСК, сотрудника или подразделение.

В левой части окна **«Профили»** отображается форма с реестром созданных в системе профилей, таблица реестра содержит следующие столбцы:

- Наименование − название профиля (используется при поиске в таблице);
- Тип − разновидность политик ОС (используется при поиске в таблице);
- Платформа − платформа ОС;
- Сущность – инициатор сущности (собственный/делегированный);
- Владелец –узел ОШС, назначенный владельцем сущности (по умолчанию, не отображается, используется при поиске в таблице).

В правой части окна отображается форма для настройки параметров профиля с вкладками:

- Политики - содержит набор правил или настроек, в соответствии с которыми производится настройка рабочей среды устройства.
- Условия/Условия (не заданы) – содержит описание условий, при выполнении которых, политики профиля будут применены к устройству. Если ни одно из условий не задано политики профиля применяются безусловно.
- Назначения – содержит указание подразделения, пользователей или комплекты, на которые будет применен данный профиль. Если в «назначении» ничего не выбрано, профиль не будет применен;
- Владелец – содержит функционал назначения узла ОШС как владельца профиля. Каждый профиль принадлежит одному владельцу. Администратор узла «владельца» (а также, администратор вышестоящего узла ОШС) имеет права на редактирование настроек профиля;
- Делегирование –позволяет делегировать назначение профиля администраторам подчиненных подразделений.

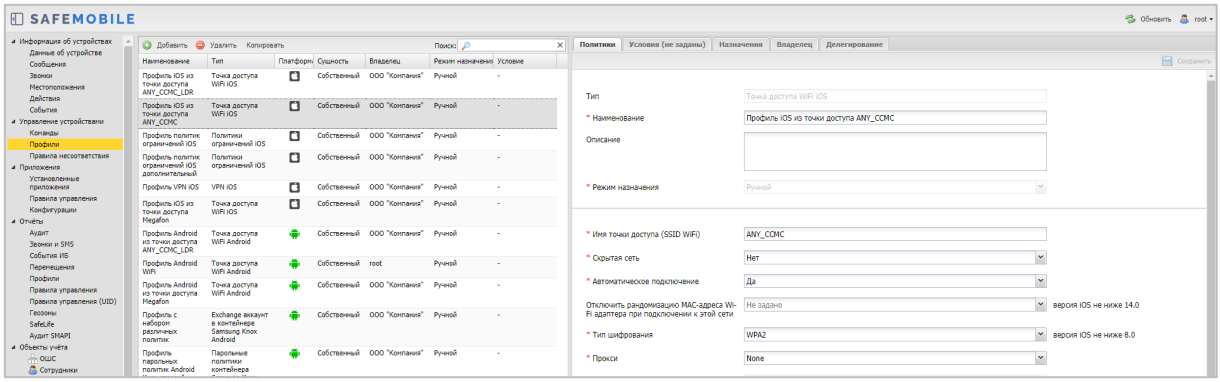


Рисунок 2.40 - Окно «Профили»

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить – предназначена для создания нового профиля;
- Удалить – предназначена для удаления уже созданного профиля;
- Копировать – предназначена для создания копии существующего профиля.

2.6.8.1 Создание профиля

Копирование существующего профиля

Для копирования существующего профиля необходимо выделить в списке профиль для копирования и нажать кнопку «Копировать», после чего будет создан идентичный профиль, кроме следующих изменений:

- Новый профиль будет иметь наименование исходного профиля, с добавлением слова «Копия» в начале наименования (Например «Копия Профиль iOS из точки доступа»);
- Копия не содержащий параметры «Условия» и «Назначения» исходного профиля.

Создание профиля с помощью кнопки «Добавить»

Для добавления нового профиля в реестр нажмите кнопку **«Добавить»**, после чего появится всплывающее окно **«Создание профиля»** с перечнем типов профилей и иконками платформ в соответствии с рисунком 2.41.

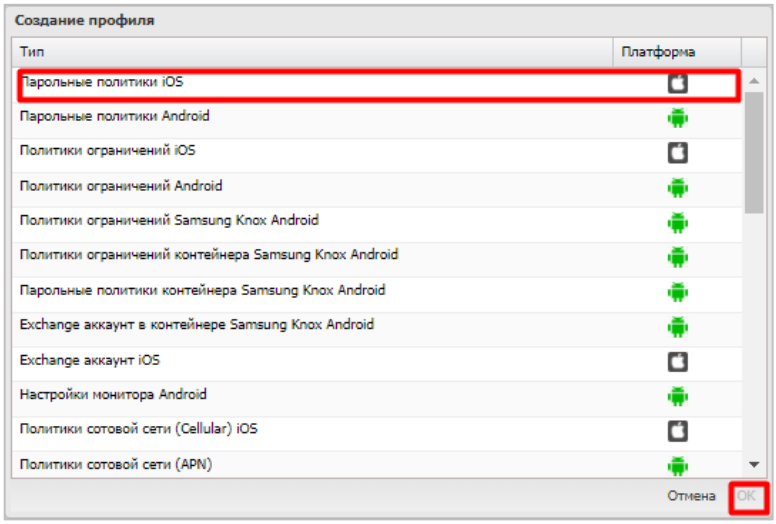


Рисунок 2.41 - Создание профиля

В системе поддерживаются следующие типы профилей:

- **Платформа iOS:**
  - Парольные политики. Требования к паролю доступа к МСК;
  - Политики ограничений. Ограничение возможностей ОС и встроенных приложений;
  - Exchange аккаунт;
  - Политики сотовой сети (Cellular). Настройка мобильного интернета;
  - Режим киоска;
  - Управляемые домены;
  - Точка доступа WiFi;
  - Доверенный сертификат;
  - Настройки монитора;
  - Ярлык рабочего стола iOS;
  - VPN iOS;
  - VPN для приложений (Per-App VPN) iOS;
  - Фильтр web контента iOS.

Примечание.

Политика «Управлять копированием и вставкой через буфер обмена» (1) (для профиля ограничений) работает только совместно с политиками «Разрешить от-

крытие в неуправляемых приложениях документов, ранее открытых в управляемых приложениях» (2) и/или «Разрешить открытие в управляемых приложениях документов, ранее открытых в неуправляемых приложениях» (3).

Значение политики (1)	Значение политики (2)	Копирование данных через буфер обмена из управляемых в неуправляемые
Да	Нет	Запрещено
Да	Да	Разрешено
Да	Не задано	
Нет	Любое	
Не задано	Любое	

Значение политики (1)	Значение политики (3)	Копирование данных через буфер обмена из неуправляемых в управляемые
Да	Нет	Запрещено
Да	Да	Разрешено
Да	Не задано	
Нет	Любое	
Не задано	Любое	

- **Платформа Android:**
  - Exchange аккаунт в контейнере Samsung Knox Android - (работает с ЛРП и КРП);
  - Доверенный сертификат Android - (работает с ЛРП и КРП);

- Настройки монитора Android - (работает с ЛРП и КРП);
- Настройки сбора местоположений Android - (работает с КРП);

Примечание.

Информация об источнике получения данных:

- *Точность и стабильность доставки координат монитору зависят от вендора устройства.*
- *"Только GPS" данные будут передаваться как в режиме низкого энергопотребления, так и в других режимах. Если на устройстве нет датчика GPS (физически), никакой ошибки возникать не будет, но БД не будет получать информацию о перемещении.*
- *В режиме работы стандартного api (не GMS) на версии 12+ в профиль можно передать показатель точности, но гарантия того, что координаты будут возвращены при вызове Монитору, есть только при выборе режима «высокого энергопотребления».*
- *В режиме работы, который использует стандартный api (не GMS) на версиях 11 и ниже, гарантию доставки параметром в профиле задать нельзя. На этой версии единственный способ получать данные местоположения - выбрать "Только GPS" или "... по нескольким источникам и GMS".*
- *Местоположения могут не передаваться, если интервал запроса задан очень маленький. Чтобы повысить шанс приложению «Монитор» получить местоположение при вызове api (при любом источнике) – следует увеличить интервал в "Промежуток времени между попытками получения координат...".*

- Парольные политики Android - (работает с ЛРП и КРП);
- Парольные политики контейнера Samsung Knox Android;
- Политики обновления ОС Android - (работает с КРП, см. «примечание ****»);
- Политики ограничений Android - (работает с ЛРП и КРП);
- Политики ограничений Samsung Knox Android;

- Политики ограничений контейнера Samsung Knox Android;
- Политики сотовой сети (APN);
- Политики управления датой и временем Android;
- Режим киоска Android;
- Режим киоска Android (устарел);
- Режим киоска Samsung Knox Android (устарел);
- Сетевые подключения Android;
- Точка доступа WiFi Android - (работает с ЛРП и КРП);
- Ярлык рабочего стола Android - (работает с ЛРП и КРП).

Примечание

**Для включения возможности входа и выхода из режима «киоск» необходимо:*

1. *Назначить устройству профиль «Режим киоска Android»;*
2. *В настройках профиля «Режим киоска Android» разрешить «Выход из режима киоска по паролю»;*
3. *Установить пароль для выхода из режима «киоск».*

***Для корректной работы ярлыков в режиме киоска, добавленных профилем "Ярлык рабочего стола Android" необходимо учитывать следующее:*

1. *Если в профиле ярлыка **задан** "UID веб браузера, в котором необходимо открывать URL...", то этот же UID должен быть добавлен в политику "Список UID'ов отображаемых приложений" профиля "Режим киоска Android", примененного к данному устройству.*
2. *Если в профиле ярлыка **не задан** «UID веб-браузера, в котором необходимо открывать URL...», то ярлык будет открываться браузером «по умолчанию». Соответственно UID «браузера по умолчанию» должен быть добавлен в политику «Список UID'ов отображаемых приложений» профиля «Режим киоска Android», примененного к данному устройству.*

****Если на устройство назначен профиль парольных политик и текущий пароль устройства не соответствует этим политикам, то устройство блокируется окном смены пароля на пароль, соответствующий назначенным на устройство политикам. Для обеспечения безопасности в этом режиме так же блокируется обмен файлами с устройством и отладка по USB, даже если они не были запрещены политиками ограничений.*

***** Профиль «Политики обновления ОС Android» позволяет настроить отсрочку обновления системы. Обновления могут устанавливаться:*

- *Сразу по получении,*
- *В день получения, но в указанные часы,*
- *Через 30 дней после получения обновления.*

Помимо этого, профиль позволяет задать до 5-ти периодов "заморозки" обновлений в год. Если устройство получит обновление в период заморозки, то обновление будет отложено до завершения периода заморозки. Подобное поведение может быть востребовано для того, чтобы обновление не происходило бесконтрольно в праздничные дни. ОС позволяет отложить обновление не более чем на 90 дней.

Пример: Задана политика отсрочки на 30 дней и получено обновление. До завершения 30-дней, начался 90-дневный период заморозки. Обновление будет установлено ОС через 90 дней с момента получения обновления. То, что период заморозки еще не завершен будет проигнорировано. Так же есть ограничение на минимальный промежуток времени между двумя периодами заморозки - 60 дней.

- **Платформа Аврора**
  - Политики ограничений;
  - Настройки монитора;
  - Парольные политики;
  - Политики обновления ОС Аврора;
  - Доверенный сертификат ОС Аврора.
- **Платформа Windows**
  - Парольные политики;
  - Настройки bluetooth;
  - Политики сетевых подключений;
  - Политики ограничений;
  - Политики использования камеры;
  - Политики доступа к настройкам;
  - Политики Defender;
  - Настройки BitLocker.
- **Платформа SafeLife**
  - Настройки браслета.

Примечание

На устройствах производства Samsung следует применять политики ограничений Samsung Knox, а политики ограничений Android, следовательно, применять на МСК платформы Android производства других компаний.

Для продолжения работы следует сделать выбор и нажать на кнопку **"ОК"** или **"Отмена"**. При нажатии на кнопку "**ОК**" откроется новая форма с настройками политик профиля − вкладка **"Политики",** а созданный профиль отобразится в реестре профилей. При нажатии на кнопку **"Отмена"** окно создания профиля закроется без сохранения изменений.

2.6.8.2 Настройка параметров профиля

В форме настроек политик профиля (рисунок 2.42), следует указать требуемые значения.

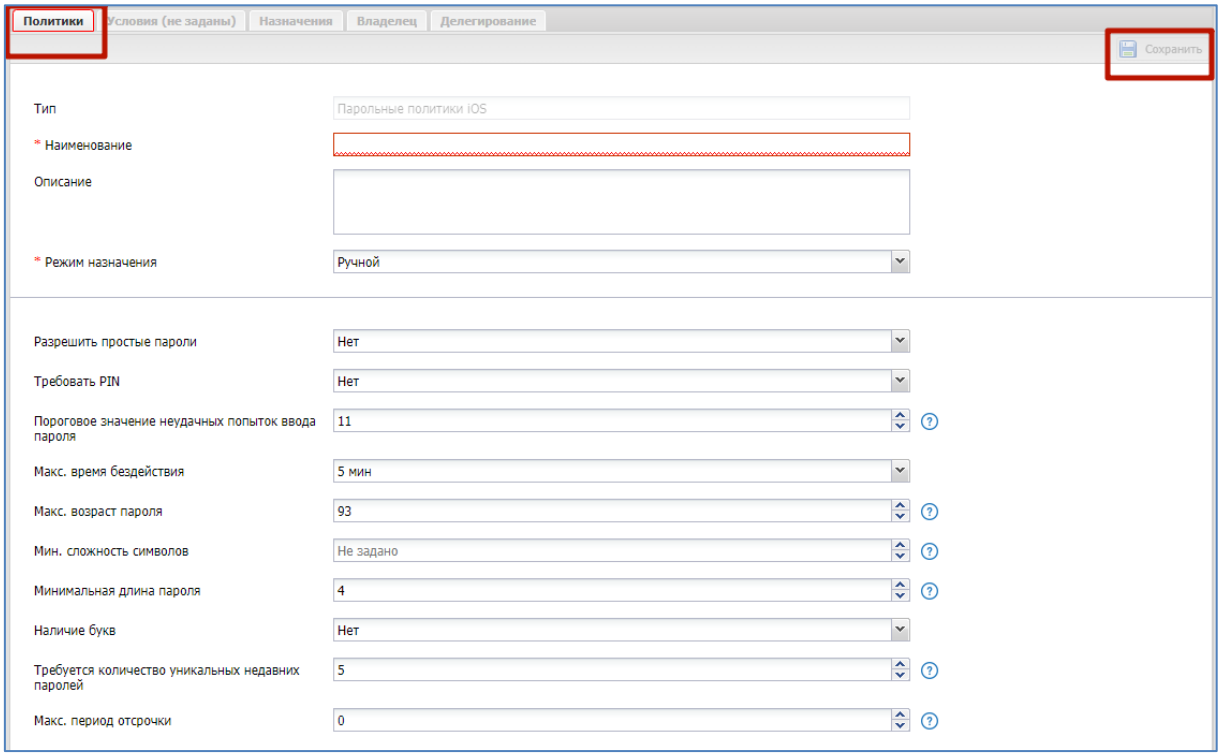


Рисунок 2.42 - Форма с настройками политик профиля

Подстановки

В качестве значений строковых параметров можно использовать подстановки. Подстановки – строки специального вида, вместо которых перед применением подставляются персонифицированные данные.

В каждом строковом параметре допускается использование одной или нескольких подстановок.

Ключ подстановки в тексте должен начинаться с префикса "{{" без кавычек, а заканчиваться постфиксом "}}" без кавычек.

Например, для того чтобы значение параметра содержало домен\логин пользователя, нужно указать следующую строку:

{{employee.exchange.emp_email_domain}}\{{employee.exchange.emp_email_login}}

Список ключей подстановок:

- {{employee.surname}} - фамилия сотрудника.
- {{employee.name}} - имя сотрудника.
- {{employee.patronymic}} - отчество сотрудника.
- {{employee.exchange.emp_email}} - email сотрудника.
- {{employee.exchange.emp_email_login}} - логин сотрудника.
- {{employee.exchange.emp_email_domain}} - домен сотрудника.
- {{noncompliance_rule.name}} - наименование правила несоответствия.
- Импортированные атрибуты из AD:
    - {{company}},
    - {{department}},
    - {{displayname}},
    - {{distinguishedName}},
    - {{employeeID}},
    - {{givenName}},
    - {{mail}},
    - {{mailNickName}},
    - {{middleName}},
    - {{mobile}},
    - {{name}},
    - {{objectCategory}},
    - {{objectGuid}},
    - {{sAMAccountName}},
    - {{sn}},
    - {{telephoneNumber}},
    - {{title}},
    - {{userPrincipalName}}.

Примечание.

- *Подстановки могут быть использованы только в политиках типа «Строка» или «Массив строк».*
- *При отсутствии значения подстановки в необязательной политике подстановка заменяется на пустую строку удаляется из политики, после чего политика обрабатывается как валидная.*
- *Для обязательных политик отсутствие подстановки интерпретируется как сознательное действие администратора (например, в случае exchange, как отключение пользователя от корпоративной почты) и приводит к следующим действиям:*
  - *Отмену установки профиля.*
  - *Событие "Отсутствие значения обязательной политики".*

Добавление идентификаторов приложений

Для ряда параметров профилей требуется указать идентификатор(ы) одного или нескольких приложений.

- Политики профиля **«Политики ограничений iOS»**
  - Список идентификаторов приложений, запуск которых разрешен;
  - Список идентификаторов приложений, запуск которых запрещен;

- Условия
  - На устройстве установлено одно из приложений;
  - На устройстве отсутствует одно из приложений.

Узнать идентификатор для конкретного приложения можно в столбце **«UID»** таблицы установленных приложений раздела **«Приложения / Установленные приложения»**.

Узнать идентификатор системного приложения для МСК производства iOS можно в столбце **«iOS Bundle ID»** приложения В.

2.6.8.3 Задание условий применения профиля

После заполнения формы профиля нажать кнопку **«Сохранить»** и, после подтверждения действия, выбрать вкладку **«Условия»** в соответствии с рисунком 2.43.

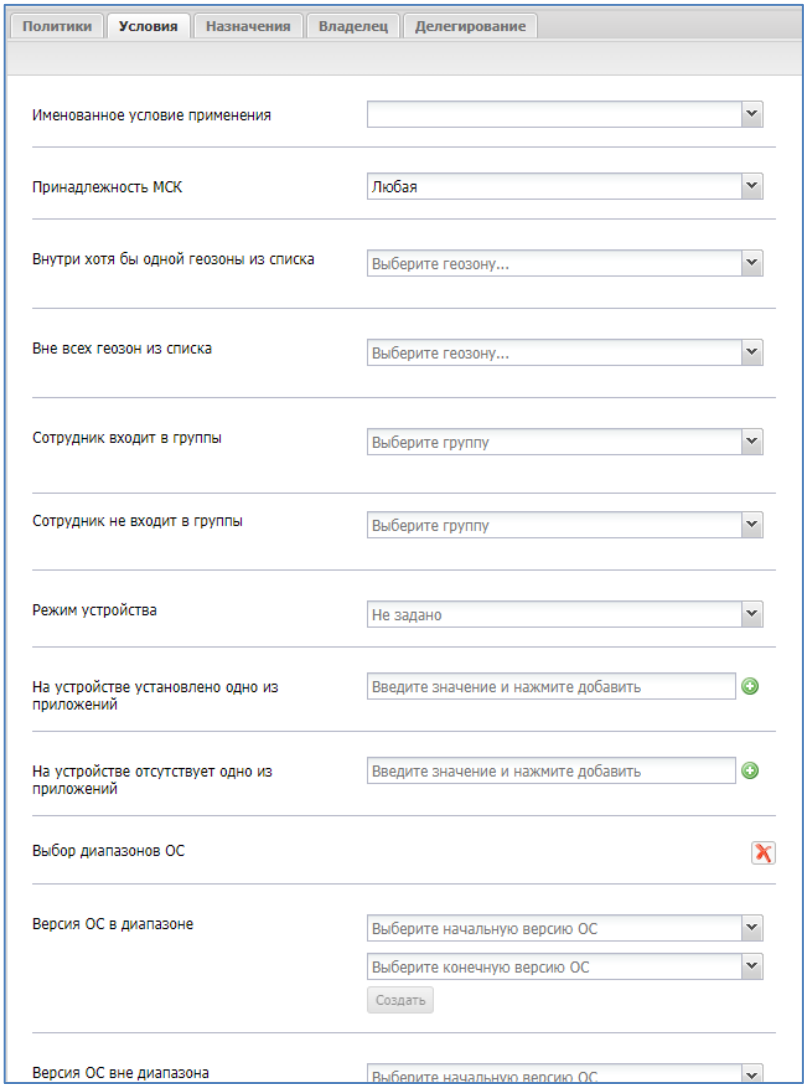


Рисунок 2.43 - Условия применения профиля

По умолчанию условия не заданы, после задания условий название закладки измениться на «Условия». Для задания условий применения следует в раскрывающемся списке выбрать параметр со значением:

- Именованное условие применения – применяет именованное условие применения, заданное в разделе «Объекты учета - Условия применения». После выбора условия из списка все остальные параметры в блоке становятся не доступны для изменения. Чтобы параметры стали доступны для редактирования необходимо в поле «Именованное условие применения» выбрать «Не заданно»;

- Принадлежность МСК (любая/личная/корпоративная);
- Стратегия (только устройство/устройство и контейнер KNOX/личный рабочий профиль/корпоративный рабочий профиль) – **только для Android**;
- Внутри хотя бы одной геозоны (название геозоны);
  Для возможности применения геозона должна быть активирована. Описание работы с геозонами приведено в 2.8.11.
- Вне всех геозон из списка (название геозоны);
  Для возможности применения геозона должна быть активирована. Описание работы с геозонами приведено в 2.8.11.

> ***Примечание.***
> *Если к устройствам Android применяются «условия применения» по геозонам, то необходимо выполнить следующие действия:*
> *1. На устройство Android должен быть назначен профиль "Настройки сбора местоположений Android", который должен применятся безусловно.*
> *2. В профиле должны быть включены политики "Собирать информацию о местоположении (в рабочее время)" и "Системный сервис определения местоположения должен быть всегда включен".*

- Сотрудник входит в группы (DN группы);
- Сотрудник не входит в группы (DN группы);
- Режим устройства (supervised/unsupervised) – **только для iOS**;
- На устройстве установлено одно из приложений (UID приложения);
- На устройстве отсутствует одно из приложений (UID приложения);

Выбор диапазонов ОС

- Выбор диапазона разрешенных ОС: (Выберите начальную версию ОС / Выберите конечную версию ОС);
- Выбор диапазона запрещенных ОС: (Выберите начальную версию ОС / Выберите конечную версию ОС);

После выбора значений диапазона ОС следует нажать кнопку **«Создать».**
Для сохранения внесенных изменений нажать кнопку **«Сохранить»**.

- Устройство имеет все перечисленные метки;
- У устройства есть хотя бы одна метка из перечисленных;
- У устройства нет ни одной из перечисленных меток;

- Модель устройства входит в список;
- Модель устройства отсутствует в списке;
- Тип устройства;
- Монитор имеет все перечисленные привилегии - **только для Android**;
- Монитор имеет хотя бы одну из перечисленных привилегий - **только для Android**;
- Монитор не имеет ни одной из перечисленных привилегий - **только для Android**.

2.6.8.4 Назначение профиля

Для назначения профиля во вкладке **«Назначения»** (рисунок 2.44) в окне ОШС выбрать подразделение(я)/сотрудника(ов) или в главной таблице выбрать одно или несколько МСК сотрудников. Для удобства можно использовать поиск по следующим параметрам таблицы:

- id,
- Телефон,
- Сотрудник,
- Пользователь домена,
- Отдел/группа,
- Метка.

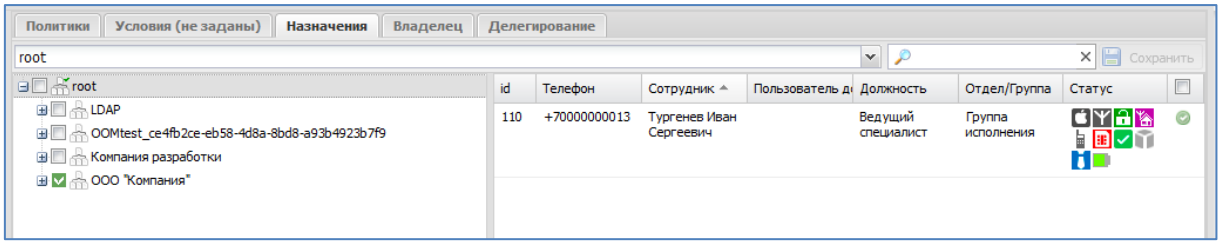


Рисунок 2.44 - Назначение профиля

Назначение сущности имеет два состояния:

- – назначено;
- – исключено.

Для сохранения назначения профиля в системе нажать на кнопку **"Сохранить"**.

2.6.8.5 Смена владельца сущности

Во вкладке **«Владелец»** администратор может сменить владельца сущности для подчиненного подразделения. Для этого следует выбрать требуемый узел ОШС в соответствии с рисунком 2.45 и нажать «Сохранить». После подтверждения изменения владельцем сущности будет назначен указанный объект ОШС. Если сущность имеет назначения за пределами области управления нового владельца, то в интерфейсе отобразится ошибка в соответствии с рисунком 2.46. У объекта ОШС может быть только один владелец для управления сущностями.

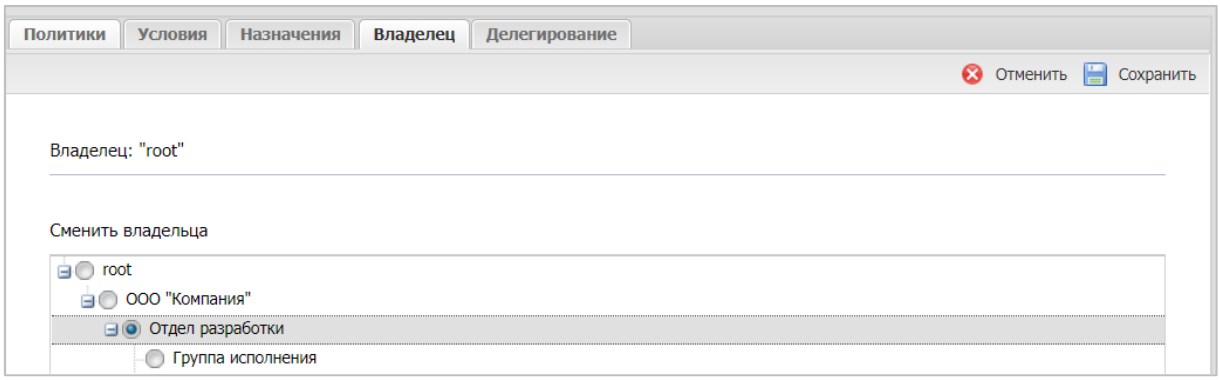


Рисунок 2.45 - Смена владельца сущности

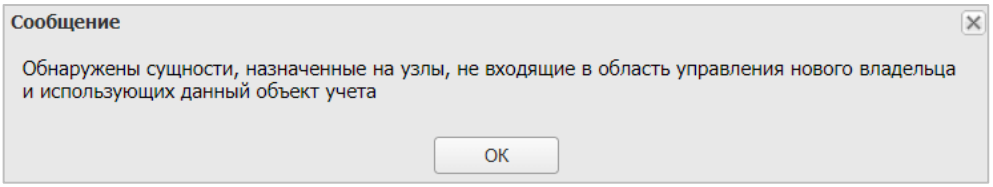


Рисунок 2.46 - Сообщение об ошибке при смене владельца сущности

Для отмены действия смены владельца сущности следует нажать **«Отменить»**, после чего кнопка «Сохранить» станет не активной.

2.6.8.6 Делегирование сущности

Во вкладке **«Делегирование»**, для передачи прав на управление назначением сущности администраторам узла ОШС (на рисунке 2.47), владельцем является «root» требуется выбрать один или несколько объектов ОШС, нажать **«Сохранить»** и подтвердить действие. В этом случае, для администратора выбранного объекта ОШС данная сущность в АРМе в окне с реестром профилей будет отображаться как «Делегированная» в столбце «Сущность».

Для отмены делегирования следует нажать **«Отменить»**.

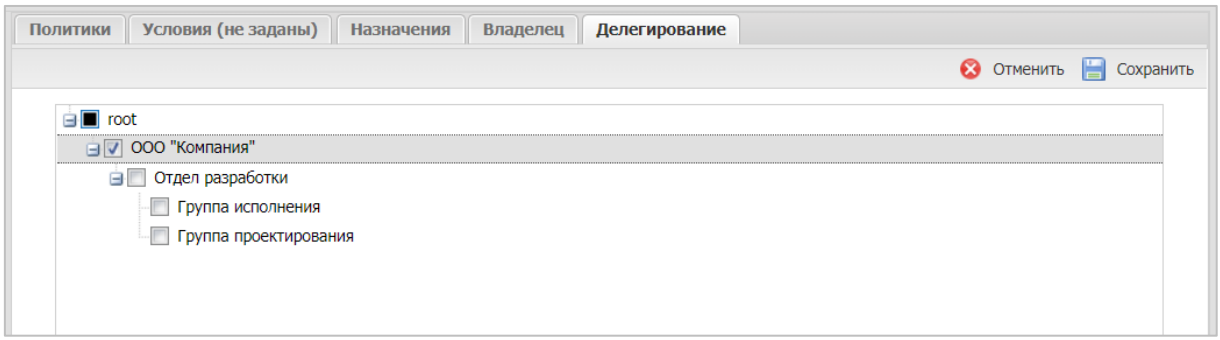


Рисунок 2.47 - Делегирование сущности

2.6.8.7 Применение профиля

Особенности применения на МСК платформы Android профилей парольные политики

Начиная с 10 версии Android, для управления парольными политиками устройства, Монитору **обязательно** нужны права Device Owner. Таким образом, если монитор был установлен на Android 9 без прав Device Owner (например, с правами Device Admin или лицензией KNOX), то после обновления устройства до Android 10 возможность управлять парольными политиками будет утрачена.

Особенности применения на МСК профилей различных типов

При добавлении профиля следует учитывать следующие особенности:

- При назначении нескольких профилей будут применяться политики назначенные на ближайшие к МСК родительские узлы в дереве ОШС. Для следующих типов профилей:
    - Парольные политики iOS,
    - Парольные политики Android,

- Политики ограничений iOS,
- Политики ограничений Android,
- Политики ограничений Samsung Knox Android,
- Политики ограничений контейнера Samsung Knox Android,
- Парольные политики контейнера Samsung Knox Android,

- При назначении нескольких профилей на МСК будет применено то количество аккаунтов, которое было назначено. Для следующих типов профилей:
  - Exchange аккаунт в контейнере Samsung Knox Android,
  - Exchange аккаунт iOS,
  - доверенный сертификат iOS,
  - доверенный сертификат Android,
  - доверенный сертификат ОС Аврора,
  - точка доступа WiFi iOS,
  - точка доступа WiF Android,
  - политики Cellular iOS;
- При назначении нескольких профилей на МСК эти профили будут применены, но пользователю следует самостоятельно выбрать значения, которые будут действовать. Для профилей типа:
  - Политики сотовой сети (APN) Samsung Knox Android.

Особенности применения на МСК профилей одного типа

При назначении нескольких профилей одного типа непосредственно на МСК, пользователя или узел будут применяться политики из профиля, назначенного последним. Под **«последним»** понимается назначение, сделанное последним по времени.

Особенности применения профилей «Режим киоска…»

При добавлении профиля «Режим киоска…» для МСК будут применены следующие ограничения:

−Пользователю МСК доступно только одно приложение (только для МСК на платформе iOS);

−На устройстве применяются другие профили, кроме;

- Профиль парольных политик контейнера knox.

−На устройстве выполняются команды, кроме:

- Установка пароля контейнера;

Для того чтобы в режиме киоска была возможность принимать и совершать звонки, а также получать и отправлять SMS, необходимо добавить в политику "Список UID'ов отображаемых приложений" следующие приложения:

- com.google.android.dialer;
- com.google.android.contacts,
- com.google.android.apps.messaging.

В зависимости от производителя и модели устройства состав приложений может отличаться. В частности, для устройств производителя Samsung необходимо добавлять приложения:

- com.samsung.android.dialer;
- com.samsung.android.app.contacts;
- com.samsung.android.incallui;
- com.samsung.android.messaging;
- com.android.server.telecom.

Состав необходимых приложений для конкретного устройства необходимо определять экспериментально.

Примечание:

В текущей версии (7.0) поддерживается работа устаревших типов профилей на Android:

- *Режим киоска Android (устарел)*
- *Режим киоска Samsung Knox Android (устарел)*

Следует отказаться от их использования в дальнейшем и произвести миграцию на другие типы профилей.

Особенность применения профиля «Политики ограничений Samsung Knox Android»

Одновременное назначение запрета на использование всех сетевых интерфейсов, перепрошивку устройства и сброс к заводским настройкам приведет **к нерабочему состоянию МСК без возможности восстановления его работоспособности**.

Пример такого назначения приведен ниже:

Разрешить перепрошивку устройства − Нет.

Разрешить сброс устройства к заводским настройкам − Нет.

Разрешить Wi-Fi (при запрете недоступны Wi-Fi Direct и S Beam) − Нет.

Разрешить мобильную передачу данных − Нет.

Разрешить использование Bluetooth − Нет.

Особенность применения профилей на МСК при его блокировке

Если МСК на платформе Android было заблокировано, то после его разблокировки для применения назначенных профилей следует повторно отправить команду синхронизации настроек.

Условия создания контейнера Knox

При добавлении профиля Настройки монитора Android на МСК производства Samsung одной из задач является создание контейнера Knox. Но для достижения этой цели должны быть выполнены следующие условия:

− в параметрах профиля назначен действительный ключ Samsung Knox License (SKL);

− на МСК не был установлен Knox warranty bit в результате проведения незаводской прошивки;

− пользователь МСК согласился с созданием контейнера;

− на момент активации лицензий Knox были доступны серверы Samsung.

Если указанные условия не выполнены, в системе воспроизведется ошибка (ошибка активации Knox ключей, ошибка создания контейнера) в соответствии с описанием в таблице 2.2.

Особенности системы при обновлении с версии 2.8.X

При обновлении с версии 2.8.X до текущей в системе создаются и назначаются на корневые объекты ОШС (компании) следующие профили, с учётом уже установленного ПО:

−Парольные политики Android со значениями ранее назначенных политик;

−Парольные политики iOS со значениями ранее назначенных политик;

−Политики ограничений Samsung Knox Android, в которых значения блокировки доступа к Bluetooth, браузеру и камере назначаются в соответствии с установленными значениями по умолчанию в конфигурации комплектов (описание в 2.8.9). В профиле устанавливаются ограничения, которые ранее были недоступны для управления;

−Настройки монитора Android, в которых задаются значения в соответствии с установленными значениями по умолчанию в конфигурации комплектов. В профиле

также устанавливается управление регистрацией звонков и SMS;

−Политики ограничений iOS, в которых значения блокировки доступа к Bluetooth, и камере назначаются в соответствии с установленными значениями по умолчанию в конфигурации комплектов.

При обновлении системы после первой синхронизации настроек МСК с веб-сервером осуществятся следующие действия:

1. Конфигурация всех МСК Android будет приведена к значениям конфигурации комплектов, установленных по умолчанию, в том числе уровень будут унифицированы параметры: уровень логирования, политики блокировки SIM-карт и период опроса GPS;
2. Блокировки доступа к камере, браузеру и Bluetooth будут сняты, если не были заданы в конфигурации комплектов по умолчанию.

С окончательными применёнными значениями назначенных на МСК профилей можно ознакомиться в отчёте «Профили» раздела 2.7.5.

Особенности системы при обновлении с версии 4.1

При обновлении с версии 4.1 до текущей в системе создаются и назначаются следующие профили с учётом уже установленного ПО:

- Парольные политики Android со значениями ранее назначенных политик;
- Профили парольных политик.
- Профили ограничений.
- Профили режима киоска.
- Профиль настроек монитора Android.
- Профиль управления датой и временем Samsung Knox.

Перед обновлением до текущей версии следует проверить содержимое вышеперечисленных профилей. В профилях одного типа следует установить самое строгое значение политики для верхнего объекта ОШС, а для остальных объектов ОШС указать значение «Не задано».
Если существуют профили одного типа, назначенные на один и тот же объект ОШС (подразделение, сотрудника), необходимо оставить только один профиль.

2.6.8.8 Удаление профиля

Для удаления следует выбрать в реестре профиль и нажать кнопку **«Удалить»**. Данный профиль будет удален из подраздела **«Профили»**. Если удаленный профиль был назначен на МСК, то в подразделе **«Отчёты/Профили»** он отобразится в применённых профилях с записью **«удален»**. После синхронизации устройства с системой и удаления настроек с МСК профиль будет окончательно удален из интерфейса.

> ***Примечание.***
>
> *На устройствах iOS, при удалении корпоративного профиля, приложение «Монитор» должно автоматически удаляться с устройства. Если этого не произошло, то устройство необходимо сбросить до заводских настроек.*

2.6.9 Раздел «Правила несоответствия»

«Правила несоответствия» позволяет создавать, редактировать или удалять набор действий, которые система автоматически произведет при выполнении заданных условий (рисунок 2.48). Для каждого действия в правиле существует возможность указать задержку между выполнением условий и действием.

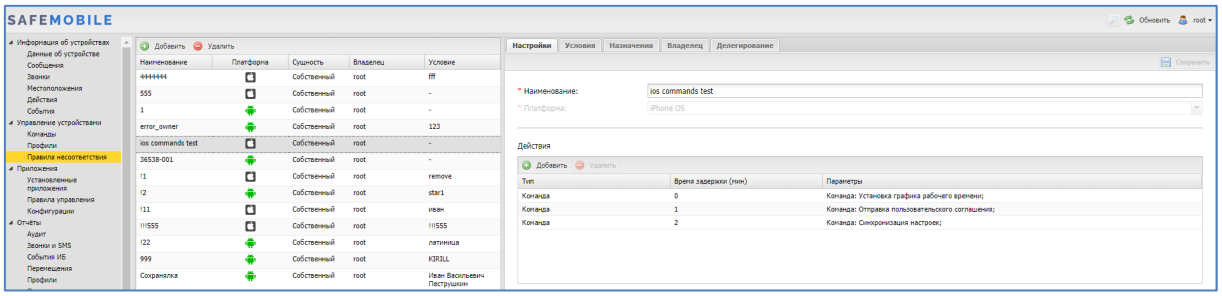


Рисунок 2.48 - Список правил несоответствия

В центральной части рабочего экрана отображается список правил, в котором каждая строка запись одного правила и содержит следующую информацию:

- Наименование – наименование правила;
- Платформа – iOS или Android;
- Сущность – тип сущности;
- Владелец – владелец правила в ОШС.

В боковом экране, рабочей области раздела отображаются параметры правила, выделенного в списке.

- Настройки – описание действия над МСК, при соответствии условий;
  - Наименование – наименование правила;
  - Платформа – платформа МСК, для которой назначается правило;
  - Действия – блок содержит список действий над устройством, выполняемых над МСК;

- Условия/Условия (не заданы) – содержит описание условий, при выполнении которых, настройки правила будут применены к устройству. Список условий идентичен условиям применения профилей (см. 2.6.8.3);
- Назначения – содержит указание подразделения, пользователей или комплекты, на которые будет применено данное правило;
- Владелец – содержит функционал назначения узла ОШС как владельца правила. Каждое правило принадлежит одному владельцу. Администратор узла «владельца» (а также администратор вышестоящего узла ОШС) имеет права на редактирование настроек правила;
- Делегирование – позволяет делегировать назначение правила администраторам подчиненных подразделений.

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить – предназначена для создания нового правила;
- Удалить – предназначена для удаления уже созданного правила.

2.6.9.1 Добавление нового правила несоответствия

Чтобы добавить новое правило несоответствия, необходимо выполнить следующие действия:

1. Перейти в раздел «Правила несоответствия»;
2. Нажать кнопку «Добавить»
3. В боковом блоке, рабочего экрана заполнить следующие поля:
   - Наименование
   - Платформа
4. В блоке «Действия» нажать кнопку «Добавить», после чего откроется модальное окно настройки действия правила.
5. Выбрать тип действия, после чего откроются дополнительные поля настроек:

- Отправка e-mail – отправка e-mail сообщения (рисунок 2.49);
  - Получатель – список адресов email. Разделитель - точка с запятой;
  - Копия - список адресов email. Разделитель - точка с запятой;
  - Шаблон – шаблон письма. Выбирается из шаблонов писем в объектах учета;
  - Время задержки (мин) – время задержки выполнения действия.

Примечание.

При заполнении полей «Получатель» и «Копия» допускается использование подстановок, описанных в разделе 2.6.8.2 Настройка параметров профиля».

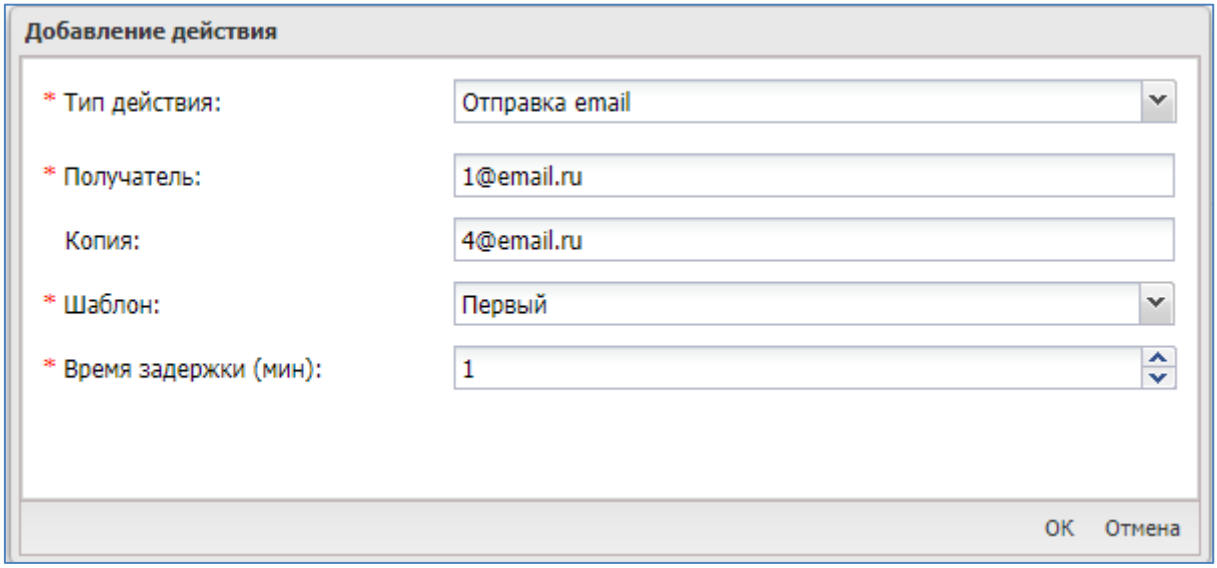


Рисунок 2.49 - Параметры действия «Отправка email»

- Команда – назначает выполнение заданной команды (рисунок 2.50);
  - Команда – выбор команды
    - Отключение от управления со сбросом к заводским настройкам;
    - Отключение от управления с удалением только корпоративных данных;
  - Время задержки (мин) - время задержки выполнения действия.

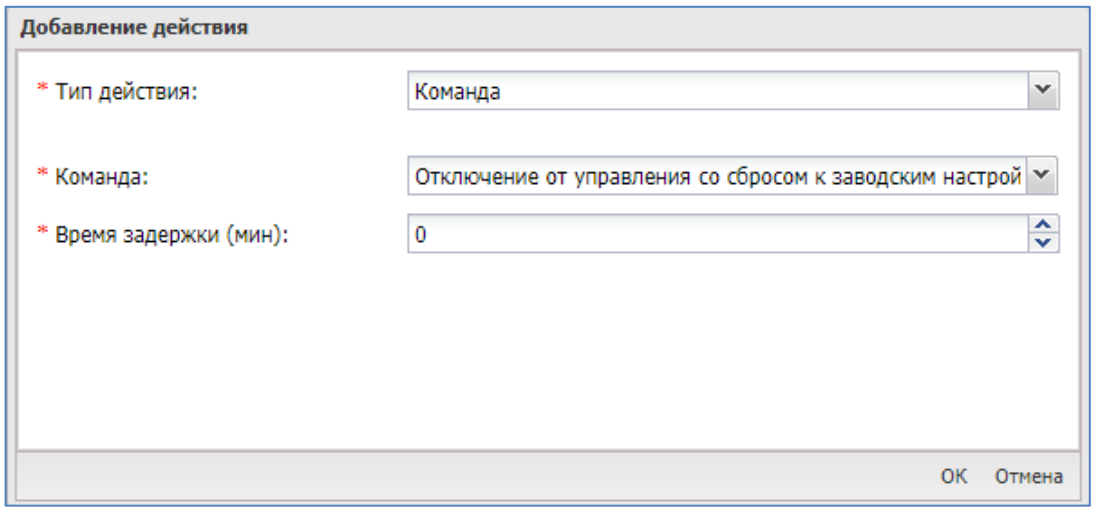


Рисунок 2.50 - Параметры действия «Команда»

- Профиль – назначение на устройство профиля (рисунок 2.51);
  - Тип профиля – выпадающий список выбора назначаемого типа профиля. В списке отображаются только типы профилей с режимом назначения «автоматический»;
  - Выбор – выбор профиля, соответствующего выбранному типу профиля;
  - Время задержки (мин) - время задержки выполнения действия.

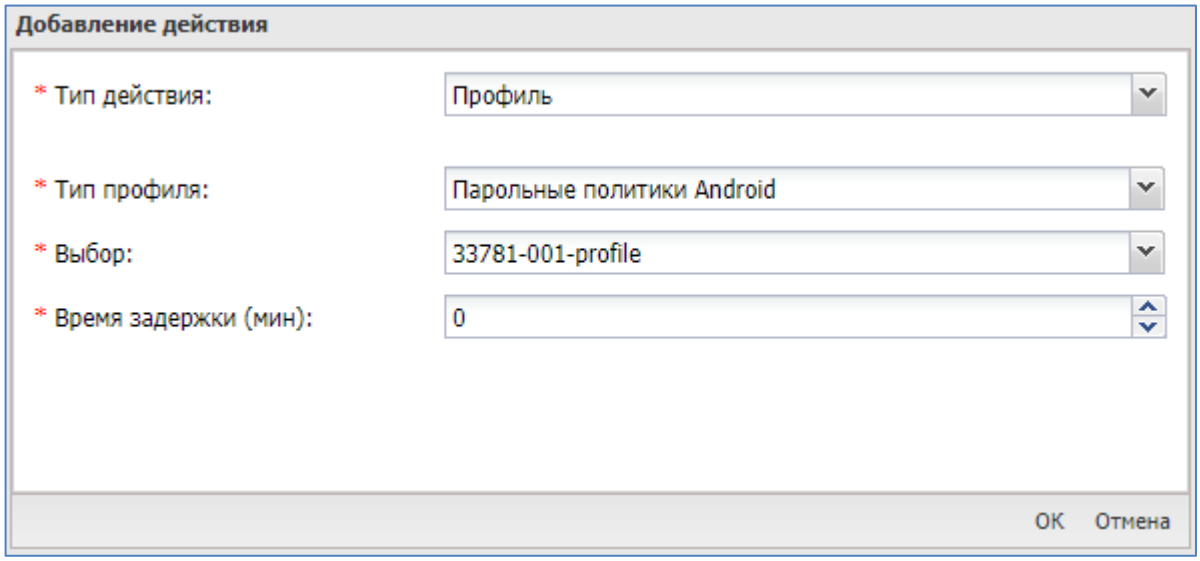


Рисунок 2.51 - Параметры действия «Профиль»

6. Нажать кнопку «Ок», после чего действие будет добавлено в список действий правила;
7. Нажать кнопку «Сохранить» (рисунок 2.52);

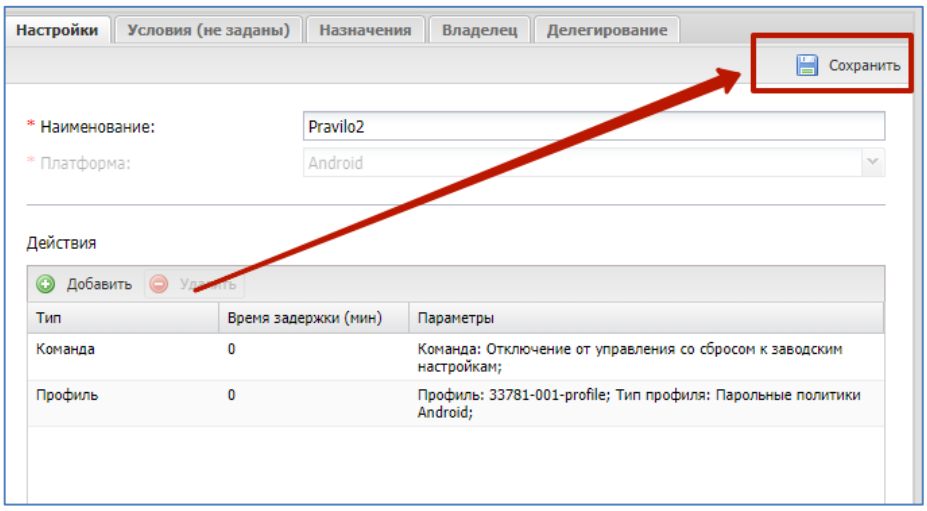


Рисунок 2.52 - Расположение кнопки «Сохранить»

8. Нажать кнопку «Да», в модальном окне подтверждения действия, после чего новое правило будет добавлено в список.

Примечание.

- *Если в «назначении» ничего не выбрано, то правило не будет применено;*
- *Если в период задержки устройство перестало удовлетворять условиям, то действие произведено не будет;*
- *Если ни одно из условий не задано, то правило применяется безусловно;*
- *Настройки правила во вкладках «Условия», «Назначения», «Владелец», «Делегирование» доступны после завершения создания правила.*
- *Если в качестве действия задано применение профилей, то все профили, указанные в правиле несоответствия:*

  1. Будут назначены непосредственно на устройство.

  2. Будут иметь более высокий приоритет по отношению к профилям назначенным администратором.

  3. В остальном будут подчиняться общим правилам применения профилей.

2.6.9.2 Редактирование существующего правила несоответствия

Чтобы внести изменения в существующее правило несоответствия, необходимо выполнить следующие действия:

1. В списке правил выделить правило подлежащее редактированию;
2. В блоке настроек внести изменения в параметры правила;
   (Изменить уже заданное действие, в блоке «Действия» нельзя. Допускается только удаление существующего и создание нового);
3. Нажать кнопку «Сохранить».

2.6.9.3 Удаление существующего правила несоответствия

Чтобы удалить существующее правило несоответствия, необходимо выполнить следующие действия:

1. В списке правил выделить правило подлежащее редактированию;
2. Нажать кнопку «Удалить» на центральном рабочем экране раздела;
3. В модальном окне подтверждения действия нажать кнопку «Да», после чего правило будет удалено.

2.6.10 Раздел «Установленные приложения»

Раздел **«Установленные приложения»** (рисунок 2.53) предназначен для осуществления контроля за приложениями, установленными на МСК пользователя, в том числе, установленными в контейнер, позволяет Администратору зарегистрировать приложение в «UEM SafeMobile», а также осуществить удаленный запуск выбранного приложения.

В информационной таблице раздела **«Управление приложениями»** отображаются две таблицы:

Установленные приложения;

Приложения, установленные в контейнере.

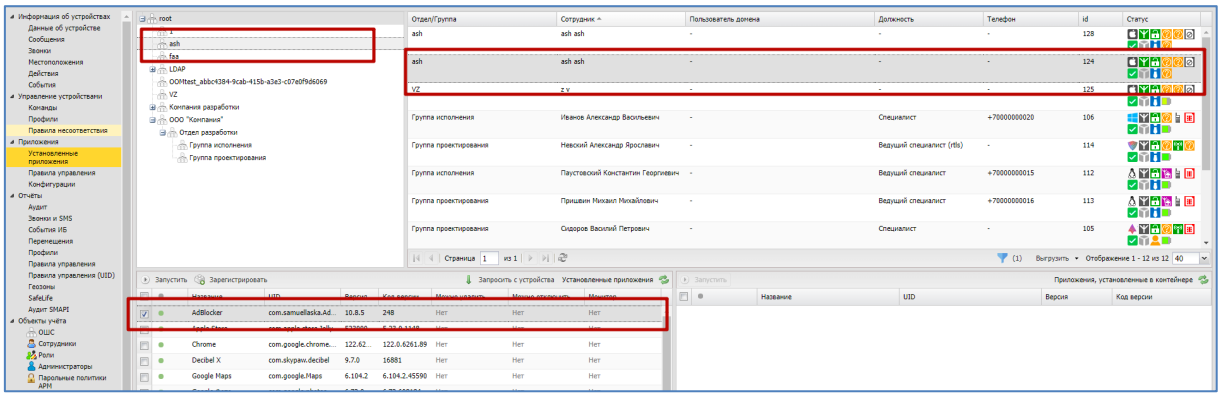


Рисунок 2.53 - Раздел «Установленные приложения»

В таблице **«Установленные приложения»** отображаются приложения, установленные на выбранном МСК.

Таблица **«Установленные приложения»** содержит следующие столбцы:

- Признак угрозы – индикатор наличия угрозы;
- – Состояние установленного приложения (− включено, − выключено);
- Название – название установленного приложения;
- UID – уникальный идентификатор приложения;
- Версия – версия установленного приложения;
- Код версии – код установленной версии приложения;
- Можно удалить − возможность удаления приложения с МСК (Да/Нет);
- Можно отключить − возможность отключения приложения на МСК на платформе Android (Да/Нет);
- Монитор − мобильный клиент SafeMobile «Да/Нет».;

- Репутация приложения (по умолчанию, не отображается в форме).

Отключение и удаление приложения осуществляется посредством создания ПУП в соответствии с 2.6.11.

Кнопки, расположенные на панели таблицы **«Установленные приложения»**, позволяют Администратору отправить с АРМ на МСК команды, после чего будет выполнено следующее действие, а именно:

Запустить – нажатие кнопки приводит к запуску выбранного приложения на устройстве. На МСК платформы Android нельзя удаленно запустить отключенное пользователем **системное** приложение. Если системное приложение было отключено на устройстве в разделе **«Настройки»**, то включить его можно только в **«Настройках»** устройства;

Запросить с устройства – нажатие кнопки приводит к отправке команды-запроса на формирование списка всех установленных приложений на МСК, включая приложения, установленные до подключения устройства к системе.

При нажатии на кнопку **«Зарегистрировать»** выбранное некорпоративное приложение, установленное на МСК пользователя, зарегистрируется в «UEM SafeMobile» и будет доступно при назначении ПУП Администратором.

В таблице **«Приложения, установленные в контейнере»** отображается список всех приложений, установленных в контейнере Knox на МСК платформы Android производства Samsung. Таблица содержит столбцы:

- – Состояние установленного приложения (− включено, − выключено);
- Признак угрозы – индикатор наличия угрозы;
- Название – название установленного приложения;
- UID – уникальный идентификатор приложения;
- Версия – версия установленного приложения.
- Код версии – код установленной версии приложения.
- Репутация приложения (по умолчанию, не отображается в форме).

На панели таблицы **«Приложения, установленные в контейнере»** находится кнопка **«Запустить»**, которая выполняет удалённый запуск выбранного приложения из контейнера на МСК пользователя.

2.6.11 Раздел «Правила управления»

Раздел **«Правила управления»** предназначен для управления приложениями на МСК, а именно:

- Автоматическая установка, обновление и удаление приложений;
- Установка приложений из Google Play и App Store;
- Автоматическое перемещение приложений в контейнер Knox;
- Настройка режима киоска: пользователю доступно только одно приложение на МСК;
- Взятие под управление «UEM SafeMobile» некорпоративных приложений пользователя;
- Ограничение доступа пользователя к приложению посредством «черного» списка.

ПУП назначается на выбранное приложение, установленное на МСК пользователя и зарегистрированное в «UEM SafeMobile». Список зарегистрированных приложений отображается в разделе **«Объекты учёта/Приложения»**.

В левой части окна **«Правила управления»** (рисунок 2.54) отображается список созданных в системе ПУП, оформленный в виде таблицы.

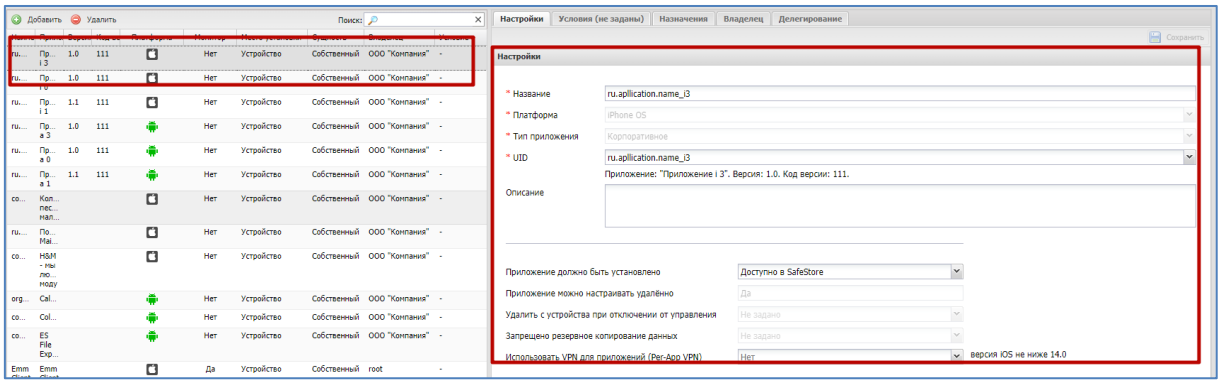


Рисунок 2.54 - Раздел «Правила управления»

Каждая строка списка содержит информацию об одном правиле для одного приложения. Таблица содержит следующие колонки данных:

- Колонки данных, отображающиеся по умолчанию:
  - Наименование − название правила;
  - Приложение − название приложения;
  - Версия − версия приложения;

- Платформа − платформа ОС;
- Монитор − мобильный клиент SafeMobile (Да/Нет);
- Место установки − Выбор места установки приложения доступен только для платформы Android. Для прочих платформ место установки всегда – «устройство». (устройство / контейнер).
- Сущность – инициатор сущности (собственный/делегированный);
- Владелец – администратор узла ОШС, назначенный владельцем сущности.

- Колонки данных опционального отображения:
  - UID – UID приложения;
  - Тип приложения − зависит от наличия дистрибутива в «UEM SafeMobile» (корпоративное/некорпоративное);
  - Приложение должно быть установлено − (Да/Нет/Не задано/Доступно в SafeStore);
  - Удалить с устройства при отключении от управления − (Да/Нет/Не задано)
  - Приложение должно быть включено – только для МСК на платформе Android (Да/Нет/Не задано);

Примечание *Если для системного приложения задано значение «Нет», то на устройстве кнопка «Остановить» (в разделе настроек «Сведения о приложениях») будет оставаться активной несмотря на то, что приложение не запущено.* *Если системное приложение отключено на устройстве через настройки пользователем, то оно не может быть включено средствами MDM.*

  - Приложение можно настраивать удалённо − только для МСК на платформе iOS (Да/Нет/Не задано);
  - Запрещено резервное копирование данных − только для МСК на платформе iOS (Да/Нет/Не задано);
  - Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении − только для МСК на платформе Android (Да/Нет);
  - Использовать VPN для приложений (Per-App VPN) – только для МСК на платформе iOS (Название профиля Per-App VPN соединения/Нет).

В верхней части таблицы находится панель инструментов с кнопками:

- Добавить – предназначена для создания нового ПУП;
- Удалить – предназначена для удаления, уже созданного ПУП.

Примечание

Единовременно на устройстве в контейнере и не в контейнере устройства может быть установлена только одна версия приложения.
Приложения, установленные пользователем на личном устройстве с рабочим профилем, могут влиять на управление приложениями в рабочем профиле через монитор и наоборот.
Таким образом, если на устройстве или в контейнере уже установлено целевое приложение, то при установке в другую управляемую область существуют следующие ограничения:

- *Подписи приложений должны совпадать;*
- *Версии приложений должны совпадать, либо версия устанавливаемого приложения должна быть выше, чем у установленного.*

2.6.11.1 Создание нового Правила управления приложениями

Чтобы создать новое «правило управления приложениями», необходимо выполнить следующие действия:

1. Перейти в раздел «Правила управления»;
2. Нажать кнопку «Добавить», после чего откроется форма создания нового правила (рисунок 2.55);

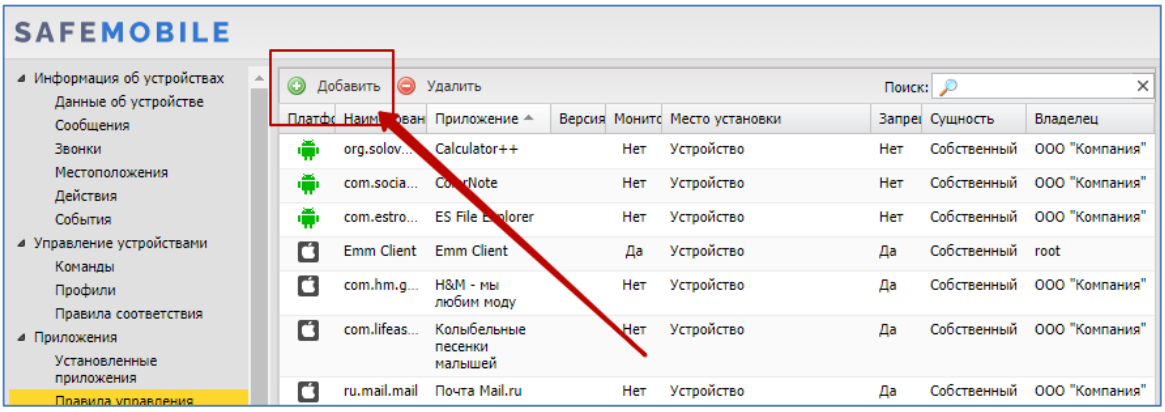


Рисунок 2.55 - Кнопка «Добавить» правило

3. Во вкладке «Настройки», заполнить все необходимые поля ввода данных;
4. Нажать кнопку «Сохранить», после чего новое правило будет сохранено в системе;
5. Перейти во вкладку «Назначение»;
6. Выбрать пользователей, к которым будет применено новое правило;
7. Нажать кнопку «Сохранить», после чего новое правило становится действующим
   (см. 2.6.11.6. «Применение ПУП»).

В зависимости от того какие будут выбраны значения в полях «Платформа» и «Тип приложения» становятся доступны дополнительные поля ввода данных:

Поля ввода данных для платформы iPhone OS

- Приложение должно быть установлено;
- Приложение можно настраивать удаленно (всегда «ДА»);
- Удалить с устройства при отключении от управления;
  Доступно для ввода, если:
  - Значение поля «Тип приложения» является «Не корпоративное»;
  - Значение поля «Приложение должно быть установлено» является «Да»;

- Запрещено резервное копирование данных - (доступно для ввода, если «Тип приложения» - Не корпоративное);
- Использовать VPN для приложений (Per-App VPN).

Поля ввода данных для платформы Android

- Приложение должно быть установлено;
- Удалить с устройства при отключении от управления.
  Доступно для ввода, если:
  - Значение поля «Тип приложения» является «Не корпоративное»;
  - Значение поля «Приложение должно быть установлено» является «Да» или «Не задано»;
- Приложение должно быть включено;
  Доступно для ввода, если:
  - Значение поля «Тип приложения» является «Не корпоративное»;
- Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении.

Поля ввода данных для платформы Windows

- Приложение должно быть установлено.

Поля ввода данных для платформы AuroraOS

- Приложение должно быть установлено.

Поля ввода данных для платформ Linux (Altlinux, Astra, Debian)

- Приложение должно быть установлено;
- Автоматически обновлять приложение;

  Доступно для ввода, если:
  - Значение поля «Тип приложения» является «Не корпоративное».

2.6.11.2 Задание условий применения ПУП

После заполнения формы ПУП и сохранения настроек выбрать условия применения ПУП во вкладке **«Условия»** в соответствии с описанием задания условий применения профиля раздел 2.6.8.3.

2.6.11.3 Назначение ПУП

Для назначения ПУП во вкладке **«Назначения»** (рисунок 2.56) в окне ОШС выбрать подразделение(я)/сотрудника(ов) или в главной таблице выбрать одно или несколько МСК сотрудников в соответствии с 2.6.8.4.

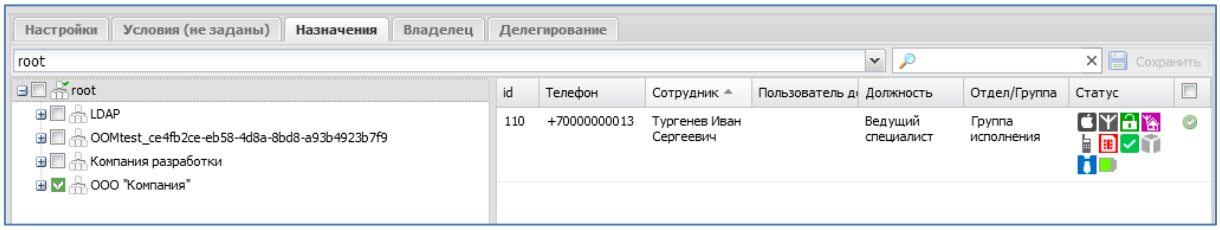


Рисунок 2.56 - Назначение ПУП

2.6.11.4 Смена владельца сущности

Для смены владельца сущности, во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.57) в окне ОШС в соответствии с 2.6.8.5.

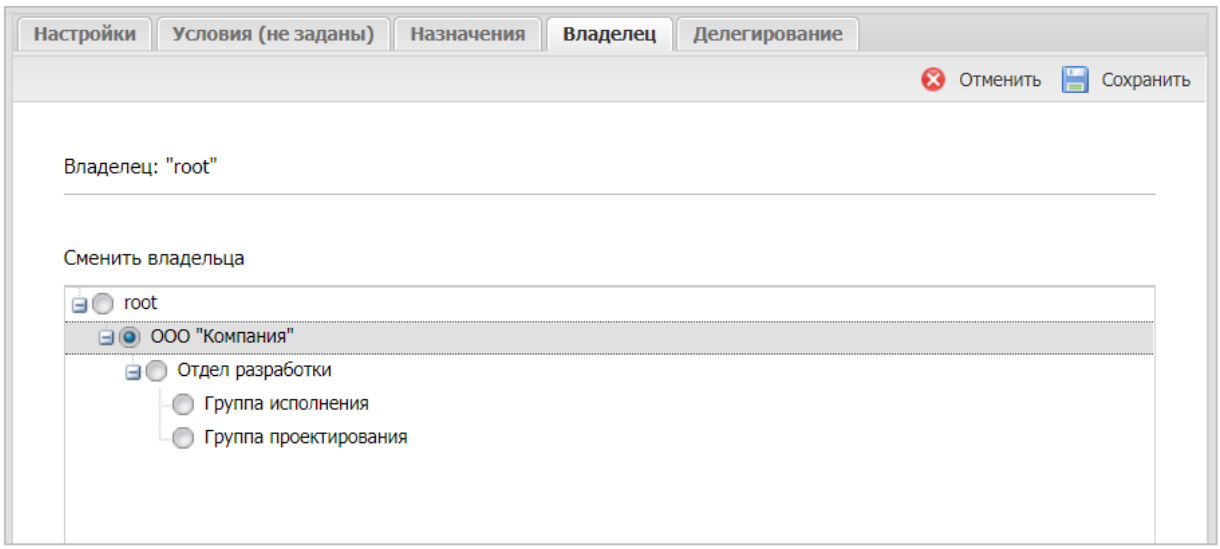


Рисунок 2.57 - Смена владельца сущности

2.6.11.5 Делегирование сущности

Для делегирования сущности, во вкладке **«Делегирование»** следует выбрать один или несколько объектов ОШС (рисунок 2.58) в окне ОШС в соответствии с 2.6.8.6.

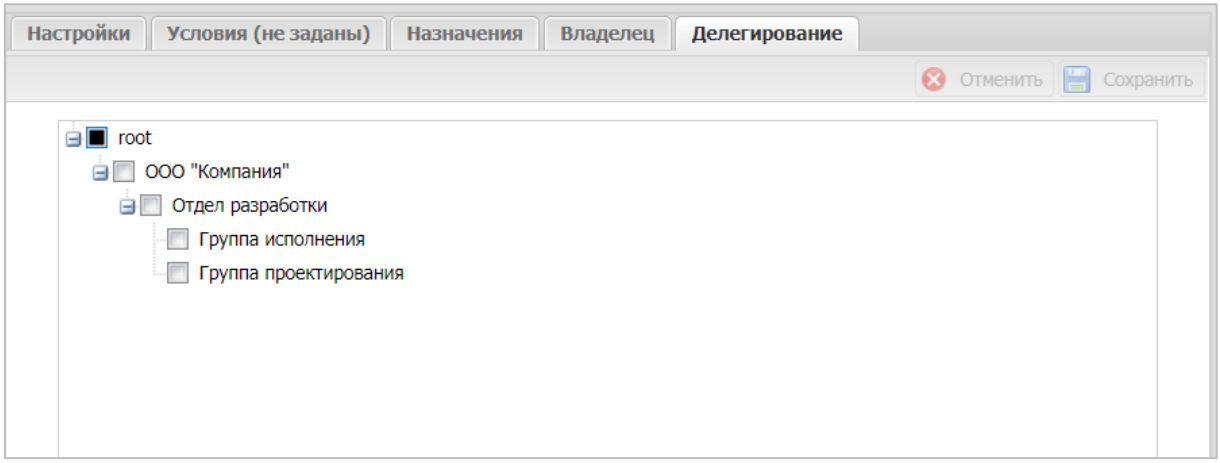


Рисунок 2.58 - Делегирование сущности

2.6.11.6 Применение ПУП

При создании и использовании ПУП необходимо учитывать следующую информацию:

Для всех платформ:

- Если при создании правила, в поле «Приложение должно быть установлено» стоит значение «Нет», то приложение, **установленное пользователем**, будет автоматически удалено с устройства, а при невозможности удаления − отключено;
- При добавлении ПУП следует учитывать, что профили имеют больший приоритет перед ПУП. Например, если в примененном профиле присутствуют политики, запрещающие отдельные приложения, а ПУП эти приложения разрешает, то в этом случае приложение будет запрещено.
- При изменении значения параметра ПУП **«Удалить с устройства при отключении от управления»** с «Да» на «Нет», а синхронизация настроек задержалась, например, из-за нахождения МСК в статусе «Не в сети», тогда будет применено первое значение и приложение удалится с устройства.

Для iPhone OS:

- Если при создании правила, в поле «Приложение должно быть установлено» стоит «ДА», при этом МСК не находится в режиме «supervised» (см. данные об устройстве), то для действия с ним будет запрошено подтверждение пользователя;
- Для исключения несанкционированного распространения корпоративных данных через некорпоративные приложения, при создании ПУП следует установить значения «Да» для параметров:
  - «Приложение можно настраивать удалённо»,
  - «Удалить с устройства при отключении от управления»,
  - «Запрещено резервное копирование данных».
- На МСК в режиме «supervised» версии iOS 14.0 и выше пользователь не сможет удалить приложение, установленное системой. На МСК без «supervised» пользователь может удалить приложение, но система будет пытаться повторно установить приложение, запрашивая у пользователя подтверждение.
- Для приложений на МСК платформы iOS после применения ПУП с пара-

метром «**Приложение можно настраивать удалённо»**, невозможно обратное действие: сделать приложение неуправляемым.

Для Android:

- При установке корпоративных приложений на МСК платформы Android следует учитывать, что на время установки снимается блокировка установки из недоверенных источников.
- При установке корпоративного приложения на МСК платформы Android, приложение проверяется сервисом ОС **«Play Protect»**. Если сервис посчитает приложение вредоносным, он может приостановить установку приложения и предложить пользователю удалить данное приложение. Монитор не может повлиять на статус приложения в сервисе. Так как сервис **«Play Protect»** является частью приложения **«Google Play»**, то отключение магазина приложений позволяет отключать проверку приложений сервисом **«Play Protect»**.
- В связи с тем, что платформа Android не допускает установку двух разных версий одного приложения и в контейнер, и на устройство, то в случае, если на МСК Android назначены два правила одного корпоративного приложения с разными местами установки, а версии приложения различаются, то будет произведена установка только в одно место: или в контейнер или на устройство.

2.6.11.7 Особенности при удалении ПУП

Для платформы Android.

Особенность корпоративного ПУП, предназначенного для обновления системного приложения (встроенного приложения от производителя устройства). Если удалить данное ПУП, то системное приложение удалено не будет. Но если монитор установлен с правами Device Owner в соответствии с разделом 2.6.8, в этом случае будет удалено обновление системного приложения.

2.6.11.8 Особенности обновления приложений

При необходимости обновить корпоративное приложение на устройствах, необходимо загрузить новую версию в раздел **«Приложения»** и определиться с ПУП.

1) Если новую версию необходимо сначала протестировать на ограниченном

списке сотрудников, рекомендуется создать новое правило и назначить его на тестовые устройства. Произойдет обновление до новой версии приложения только на тестовых устройствах. После проведения всех проверок и подтверждения готовности новой версии к распространению, необходимо внести правки в основное правило для этого приложения, а временное правило потом можно будет удалить.

2) Если сразу или после тестирования новая версия готова к распространению, необходимо внести изменение в правило управления, созданное ранее для предыдущей версии. Тогда все **Назначения** сохранятся и произойдет автоматическое обновление приложения на всех целевых устройствах. Для внесения исправления в правило управления, необходимо через поле **UID** вызвать список доступных версий и выбрать новую в соответствии с рисунком 2.59.

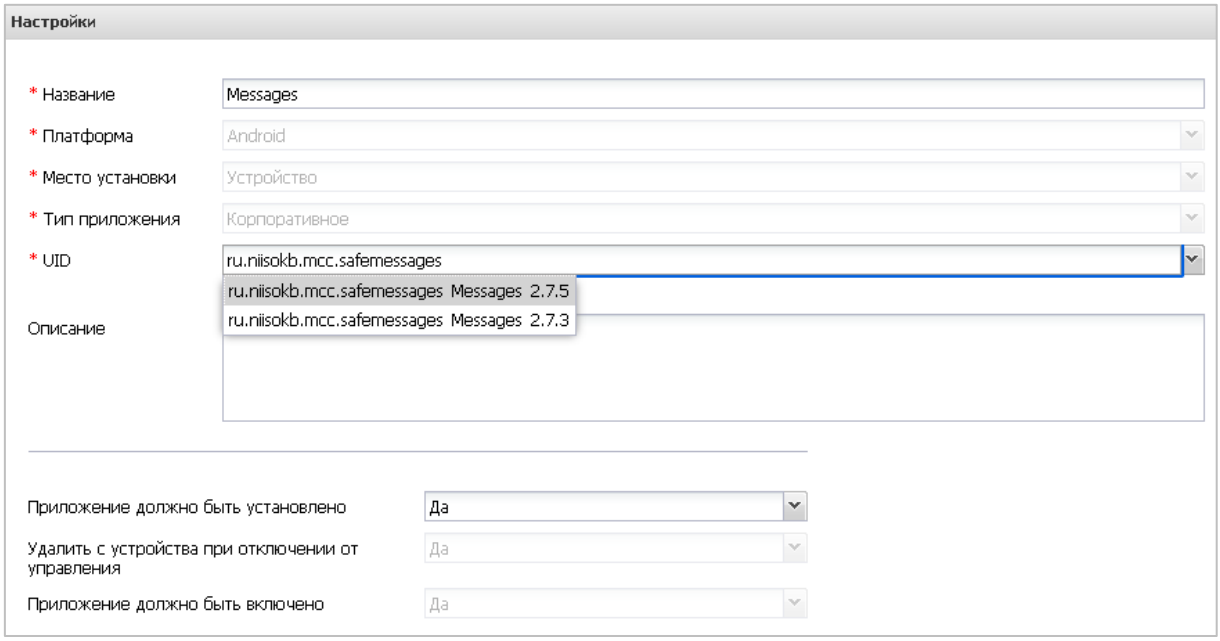


Рисунок 2.59 - Выбор версии приложения

3) Для приложений на МСК платформе Windows не поддерживается обновление приложений. При назначении новой версии возникнет ошибка установки. Для установки новой версии приложения необходимо снять назначение ранее установленной версии приложения.

Таблица 2.4 – Параметры ПУП

Платформа	Тип приложения	Параметры ПУП					
		Приложение должно быть установлено	**Приложение можно настраивать удалённо**	**Удалить с устройства при отключении от управления**	**Запрещено резервное копирование данных**	**Приложение должно быть включено**	**Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении**
	Корпоративное	Да (по умолчанию) Не задано Доступно в SafeStore	Да	Да	Да	–	–
		Нет	Да	Нет	Нет		
	Некорпоративное	Да (по умолчанию) Не задано	Да	Да (по умолчанию) Нет	Да (по умолчанию) Нет		
		Нет	Да	Нет	Нет		
	Корпоративное	Да (по умолчанию) Не задано Доступно в SafeStore	–	Да	–	Да	Да
		Нет		Нет		Нет	Нет
	Некорпоративное	Да (по умолчанию) Не задано		Да (по умолчанию) Нет		Да (по умолчанию) Нет Не задано	Да Нет (по умолчанию)
		Нет		Нет		Нет	Нет
	Корпоративное	Да (по умолчанию)	-	-	-	-	-

2.6.12 Раздел «Конфигурации»

Пункт меню **«Конфигурации»** открывает окно (рисунок 2.60), предназначенное для управления настройками приложений на МСК посредством созданных конфигураций. В данном окне доступно создание, редактирование и удаление конфигураций, а также осуществление их назначений на МСК, сотрудника или подразделение.

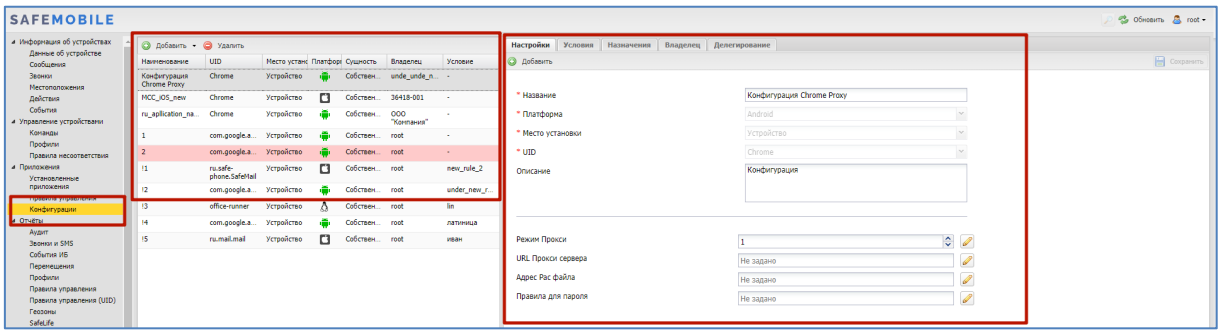


Рисунок 2.60 - Окно «Конфигурации»

Управление конфигурациями приложений осуществляется для МСК:

- на платформе iOS версий 10 и выше;
- на платформе Android для устройств Samsung с Knox версии 2.7, версия Android 5.0 и выше;
- на платформе Android для устройств других производителей, отличных от Samsung, версия Android 6.0 и выше"

В левой части окна **«Конфигурации»** отображается форма с реестром созданных в системе конфигураций приложений, таблица реестра содержит следующие столбцы:

- Наименование − название конфигурации приложения;
- UID − уникальный идентификатор приложения, к которому относится конфигурация;
- Место установки − контейнер (для МСК на платформе Android) или устройство;
- Платформа − платформа ОС;
- Сущность – инициатор сущности (собственный/делегированный);
- Владелец – администратор узла ОШС, назначенный владельцем сущности; по умолчанию, не отображается в форме.

В правой части окна отображается форма для настройки параметров конфигурации с вкладками:

- Настройки;
- Условия;
- Назначения;
- Владелец;
- Делегирование.

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить – предназначена для создания новой конфигурации;
- Удалить – предназначена для удаления уже созданной конфигурации.

2.6.12.1 Добавление конфигурации

Для добавления новой конфигурации раскройте выпадающий список справа от кнопки **«Добавить»** и выберите один из вариантов:

−Создать пустую конфигурацию;
−Создать конфигурацию из шаблона.

При выборе параметра **«Создать пустую конфигурацию»** откроется новая форма во вкладке **«Настройки»** в соответствии с рисунком 2.61. Поля, отмеченные * обязательные для заполнения.

В поле «Место установки» необходимо указать:

- "Устройство", если нужно применить Конфигурацию к приложению, размещенному на устройстве. Устройство должно быть подключено по стратегиям "Только устройство (Android)", либо "Устройство и контейнер KNOX (Samsung 5.0 - 9)";
- "Контейнер", если нужно применить Конфигурацию к приложению, размещенному в контейнере KNOX (Samsung 5.0 - 9) или рабочем профиле Android. Доступно только для МСК, подключенным по стратегиям "Устройство и контейнер KNOX (Samsung 5.0 - 9)", либо "Личный рабочий профиль (Android 7.0+)", либо "Корпоративный рабочий профиль (Android 11.0+)".

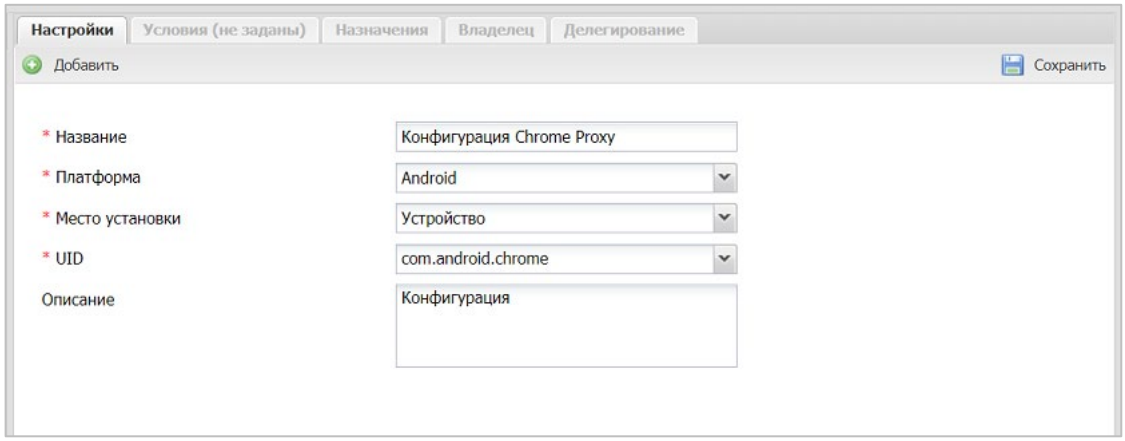


Рисунок 2.61 - Форма новой конфигурации

Для добавления параметров настройки приложения нажать кнопку **«Добавить»**, после чего отобразится форма (рисунок 2.62).

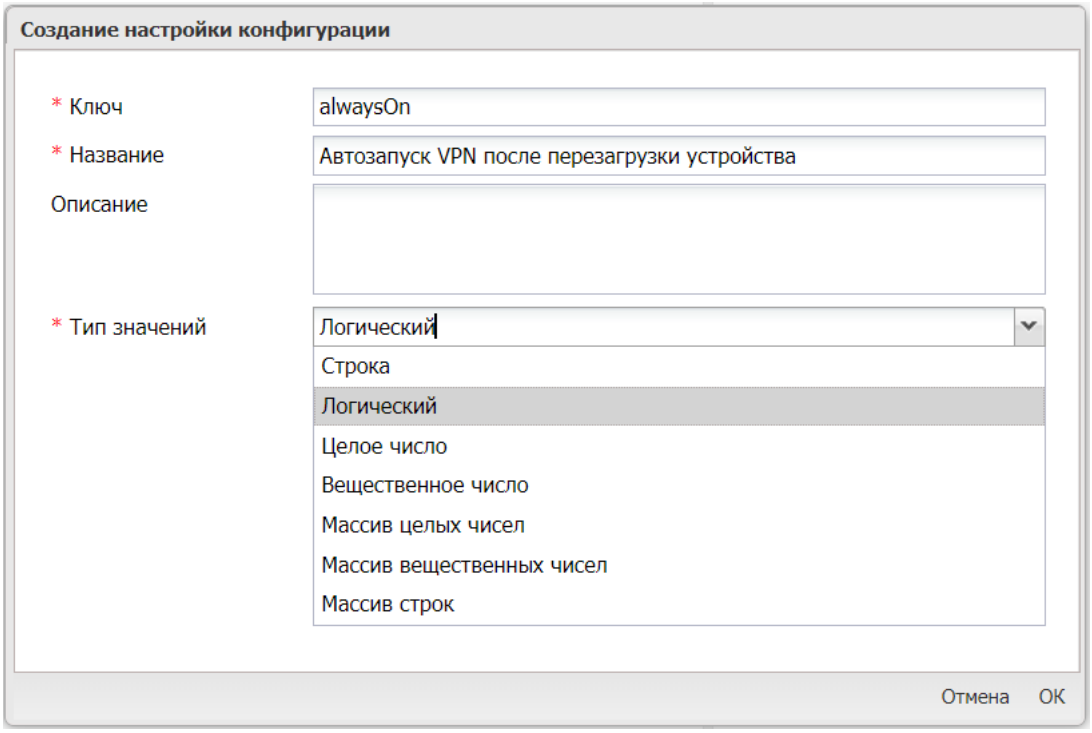


Рисунок 2.62 - Создание настройки конфигурации

Форма создания настройки конфигурации состоит из следующих полей:

- Ключ − обозначение настройки конфигурации, заданное разработчиком приложения МСК;
- Название − обозначение настройки в системе;
- Описание − краткое описание настройки;
- Тип значений − Строка / Логический / Целое число / Вещественное число /

Массив целых чисел / Массив вещественных чисел / Массив строк.

В конфигурациях могут быть использованы подстановки, описанные в «2.6.8.2 Настройка параметров профиля».

Поля **«Ключ»**, **«Название»** и **«Тип значений»** обязательные для заполнения. После заполнения полей следует нажать кнопку **«ОК»**. Конфигурация может включать в себя одну или несколько настроек приложения.

При выборе параметра **«Создать конфигурацию из шаблона»** в окне (рисунок 2.63) доступен список с уже созданными шаблонами настроек.

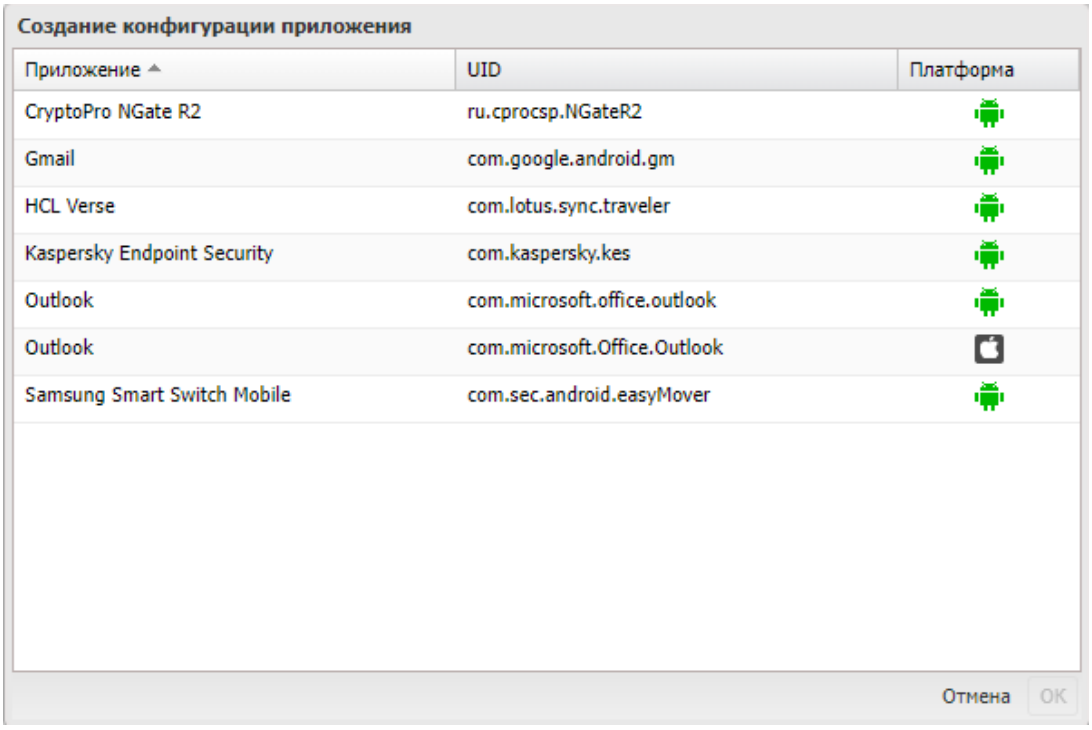


Рисунок 2.63 - Создание конфигурации приложения

В системе представлены следующие шаблоны с настройками приложений:

- ru.cprocsp.NGate – VPN (android);
- com.google.android.gm − Gmail (android);
- com.lotus.sync.traveler – Клиент Lotus (android);
- com.kaspersky.kes – Антивирус Касперского (android);
- com.microsoft.office.outlook – Microsoft Outlook (android);
- com.microsoft.Office.Outlook – Microsoft Outlook (iOS);
- com.sec.android.easyMover - Samsung Smart Switch Mobile (android).

В списке следует выбрать требуемый шаблон, нажать кнопку **«ОК»** для продолжения настроек конфигурации в форме (рисунок 2.63) и возможности редактирования параметров. Параметры конфигурации в форме будут зависеть от выбранного шаблона

Пример шаблона КП **SafeMail** с параметрами приведен на рисунке 2.64.

После заполнения всех необходимых полей для сохранения настроек конфигурации нажать кнопку **«Сохранить».**

После заполнения формы и сохранения настроек (опционально) следует задать условия применения конфигурации во вкладке **«Условия»** в соответствии с описанием задания условий применения профиля раздел 2.6.8.3.

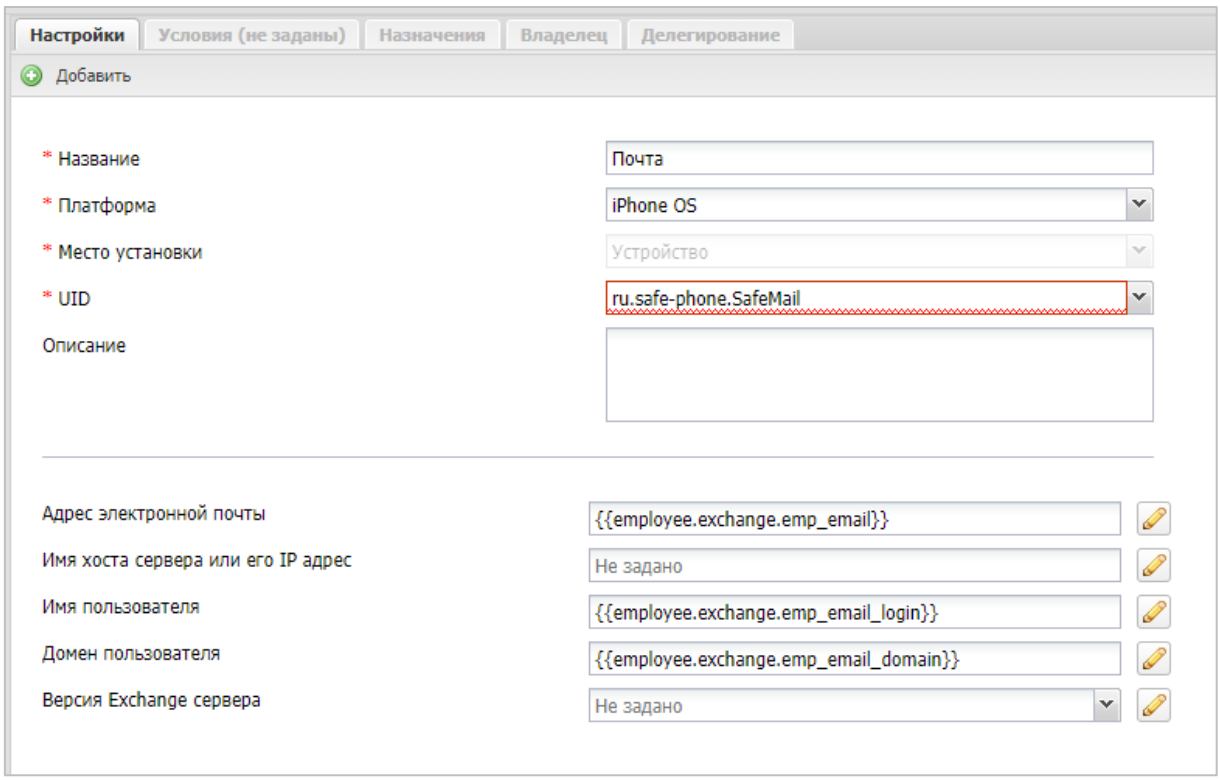


Рисунок 2.64 - Шаблон КП SafeMail

2.6.12.2 Назначение конфигурации

Чтобы назначить конфигурацию, необходимо выполнить следующие действия:

1. Выбрать конфигурацию в списке, после чего в блоке настроек будут отображены параметры конфигурации;
2. Во вкладке «Назначения», выбрать объект назначения (рисунок 2.65):
   - В окне ОШС - подразделение, сотрудник;
   - В окне устройств выбрать одно или несколько МСК сотрудников в соответствии с 2.6.8.4;

     Для удобства можно использовать поиск по следующим параметрам таблицы:
     - id,
     - Телефон,
     - Сотрудник,
     - Пользователь домена,
     - Отдел/группа,
     - Метка.
3. Нажать кнопку «Сохранить».

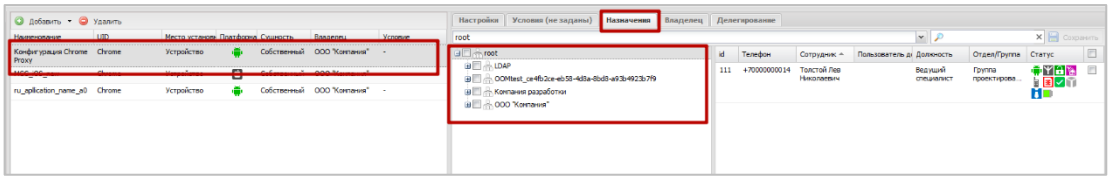


Рисунок 2.65 - Назначение конфигурации

2.6.12.3 Смена владельца сущности

Для смены владельца сущности во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.66) в окне ОШС в соответствии с 2.6.8.5.

Для сохранения изменений в системе следует нажать на кнопку **«Сохранить».**

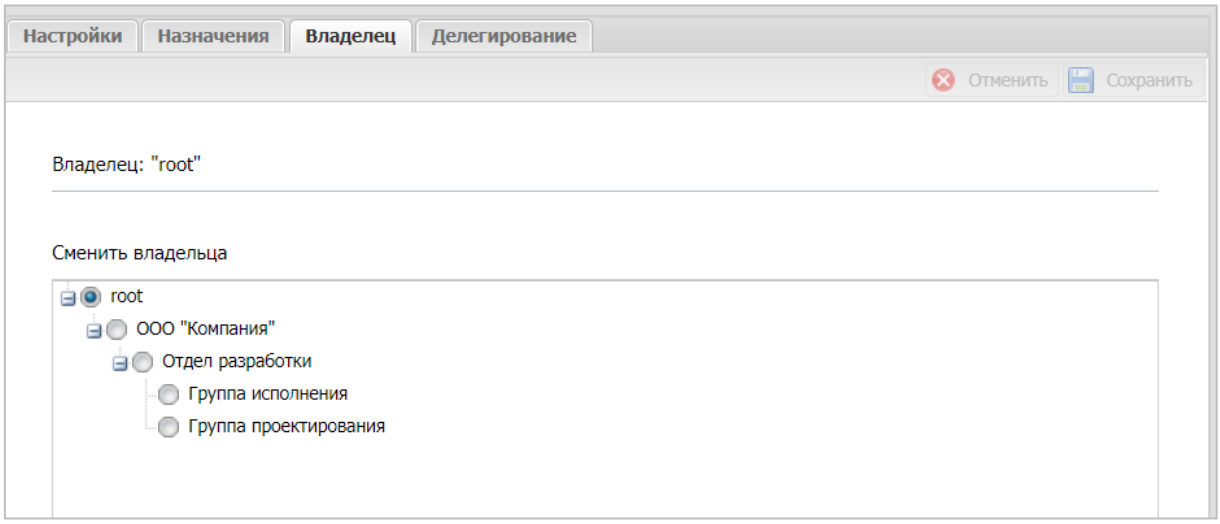


Рисунок 2.66 - Смена владельца сущности

2.6.12.4 Делегирование сущности

Для делегирования сущности во вкладке **«Делегирование»** следует выбрать один или несколько объектов ОШС (рисунок 2.67) в окне ОШС в соответствии с 2.6.8.6.

Для сохранения изменений в системе следует нажать на кнопку **«Сохранить».**

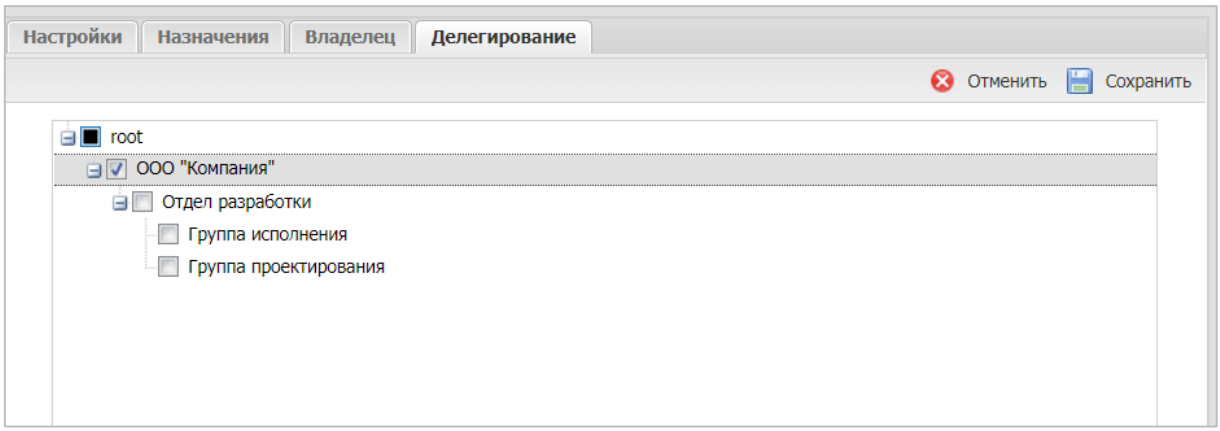


Рисунок 2.67 - Делегирование сущности

2.7 Построение отчётов (пункт меню «Отчёты»)

В разделе главного меню «Отчёты» формируются следующие отчёты:

- Аудит;
- Звонки и SMS,
- События ИБ,
- Перемещения,
- Профили,
- Правила управления,
- Правила управления (UID),
- Геозоны,
- SafeLife.

2.7.1 Отчёт «Аудит»

Для формирования отчёта выберите пункт главного меню **«Аудит»**. В открывшемся окне отображается таблица с перечнем действий администраторов в АРМ «UEM SafeMobile», произошедших в заданном интервале времени, и их результатов в соответствии с рисунком 2.68.

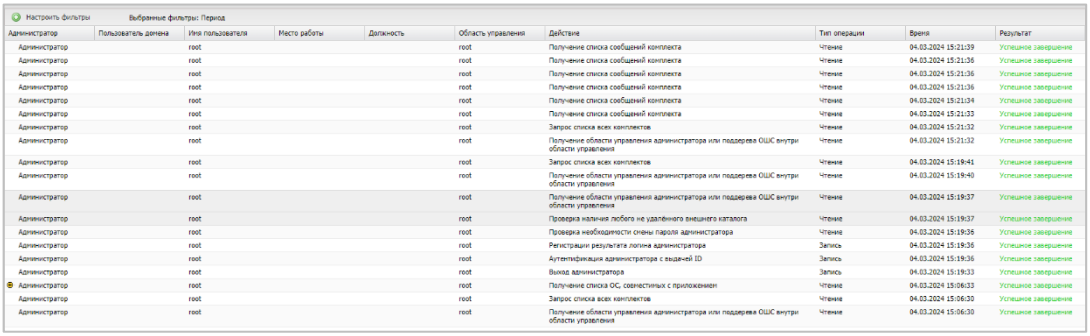


Рисунок 2.68 - Окно отчёта «Аудит»

Сформированный отчёт содержит следующие столбцы:

- Транзакция – номер операции в системе (по умолчанию, в таблице не отображается);
- Администратор – ФИО администратора, выполнившего действие в системе;
- Пользователь домена - Отображает ФИО администратора (отображает e-mail, если ФИО не было импортировано)
- Имя пользователя – имя пользователя (логин) администратора, выполнившего действие в системе;
- Место работы – место работы по штатному расписанию;

- Должность – должность по штатному расписанию;
- Область управления – узел поддерева ОШС, на который назначен администратор;
- Действие – действие, выполненное администратором в системе;
- Тип операции − вид операции с данными (чтение/запись);
- Время – дата и время выполнения действия;
- Параметры – параметры выполненного действия (по умолчанию, в таблице не отображается);
- Результат – результат выполнения действия, инициированного администратором;
- Код завершения – 0 − успешное завершение, 1 – ошибка (по умолчанию, в таблице не отображается).

Положительные результаты выполненных действий воспроизводятся зеленым цветом, а отрицательные − красным.

Для просмотра дополнительной информации по действию следует в столбце **«Администратор»** нажать значок (при его наличии).

Для настройки отображаемых в отчёте сведений используется окно настроек (рисунок 2.69), открывающееся нажатием кнопки **«Настроить фильтры»** в верхней панели инструментов.

В окне настроек параметров отчёта можно выбрать период, для которого создается отчёт. Для этого используются поля ввода даты/времени «**Отчёт за период с**», «**по**» (для начальной и конечной даты соответственно) в верхней части окна настроек. После нажатия на кнопку со значком календаря, выберите год, месяц, день и время начала и конца отчёта по аудиту действий администраторов в системе.

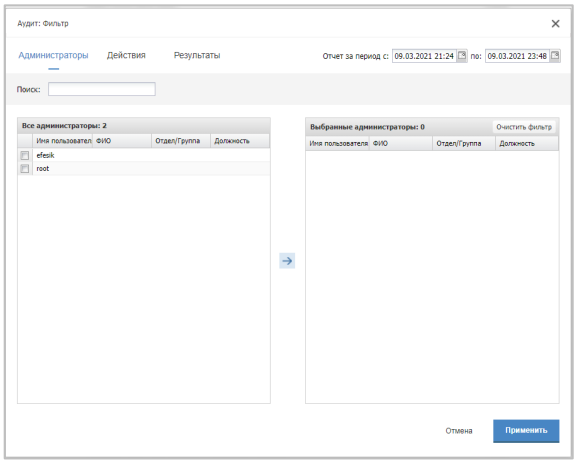


Рисунок 2.69 - Окно настроек параметров отчёта «Аудит»

Кроме того, в окне настроек отчёта можно настроить фильтры выводимых результатов на следующих вкладках:

Администраторы – позволяет выбрать администраторов, действия которых будут отображены в отчёте;

Действия – позволяет выбрать действия администраторов в системе, которые будут отображены в отчёте;

Результаты – позволяет выбрать результаты действий администраторов в системе, которые будут отображены в отчёте.

Чтобы выбрать требуемые позиции в реестрах **«Администраторы»**, **«Действия»** и **«Результаты»**, установите флажки в перечне слева и нажмите кнопку со стрелкой, после чего выбранные элементы появятся в перечне справа. Можно также просто перенести элемент из левого перечня в правый с помощью мыши. При выборе верхней строки в раскрывающихся реестрах, будут выделены все перечисления.

Окно настроек **«Действия»** (рисунок 2.70) содержит флажки **«Чтение»** и **«Запись»**. При установке флажка **«Запись»** в перечне отображаются действия администраторов с возможным редактированием данных, при установке флажка **«Чтение»** отображаются действия только с просмотром данных. Если установлены оба флажка, список содержит перечень всех имеющихся в системе действий администраторов.

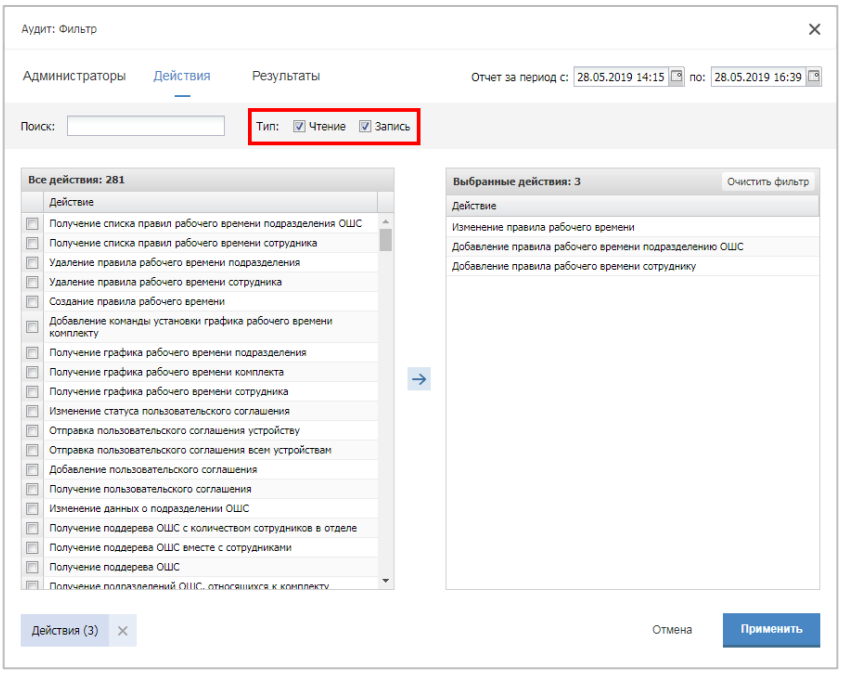


Рисунок 2.70 - Окно «Действия» в настройках параметров отчёта «Аудит»

Для осуществления поиска по ключевому слову в реестрах параметров отчёта «Аудит» предназначено окно **«Поиск»** (рисунок 2.71).

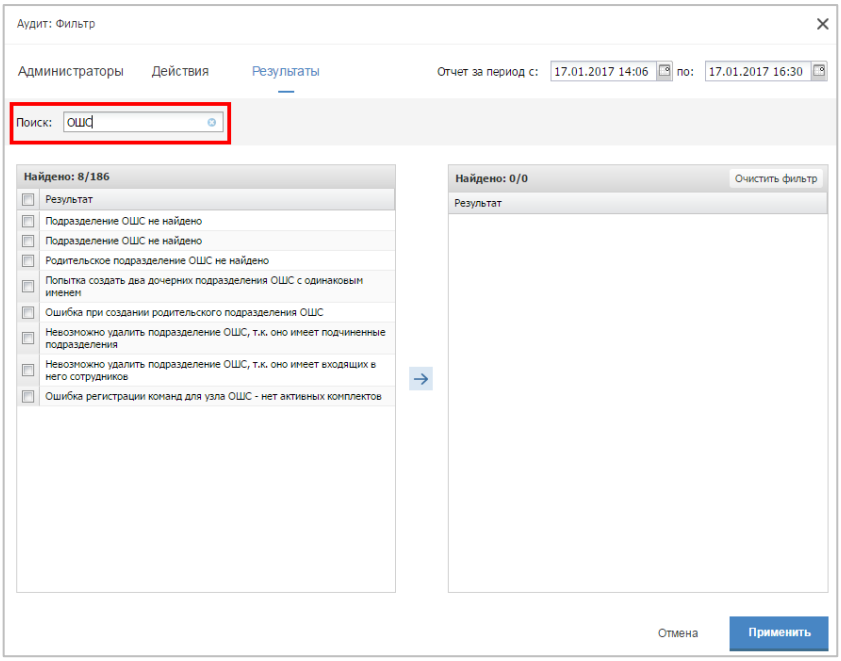


Рисунок 2.71 - Окно «Поиск» в настройках параметров отчёта «Аудит»

После настройки параметров отчёта по действиям Администраторов в «UEM SafeMobile» необходимо нажать кнопку **«Применить»** в нижней части окна настроек для перехода к сформированному отчёту согласно установленным фильтрам.

2.7.2 Отчёт «Звонки и SMS»

Для формирования отчёта выберите пункт главного меню **«Звонки и SMS»**. В открывшемся окне (рисунок 2.71) отображается таблица с перечнем звонков и SMS-сообщений за заданный период времени.

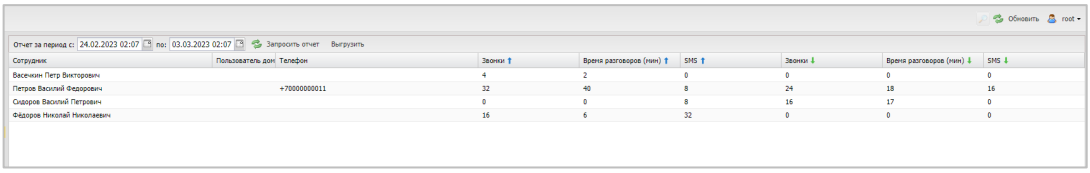


Рисунок 2.72 - Окно «Звонки и SMS»

Для выбора периода построения отчёта используются поля ввода даты/времени «**Отчёт за период с**», «**по**» (для начальной и конечной даты соответственно) в верхней

панели инструментов. После нажатия на кнопку со значком календаря выберите год, месяц, день и время начала и завершения периода отчёта. После задания периода отчета нажмите кнопку «Запросить отчет».

Сформированный отчёт содержит следующие столбцы:

- id – номер устройства в системе (по умолчанию, в таблице не отображается);
- Сотрудник – фамилия, имя и отчество сотрудника-владельца устройства;
- Пользователь домена – ФИО сотрудника или e-mail, если ФИО не было импортировано;
- Телефон – номер телефона SIM-карты устройства;
- Звонки входящие – количество входящих звонков;
- Время разговоров (мин) – общая продолжительность входящих соединений;
- SMS – количество входящих SMS.
- Звонки входящие – количество исходящих звонков;
- Время разговоров (мин) – общая продолжительность исходящих соединений;
- SMS – количество исходящих SMS.

2.7.3 Отчёт «События ИБ»

Для формирования отчёта выберите пункт главного меню **«События ИБ»**. В открывшемся окне отображается таблица с перечнем событий информационной безопасности «UEM SafeMobile», произошедших в интервале времени, заданном Администратором в соответствии с рисунком 2.73.

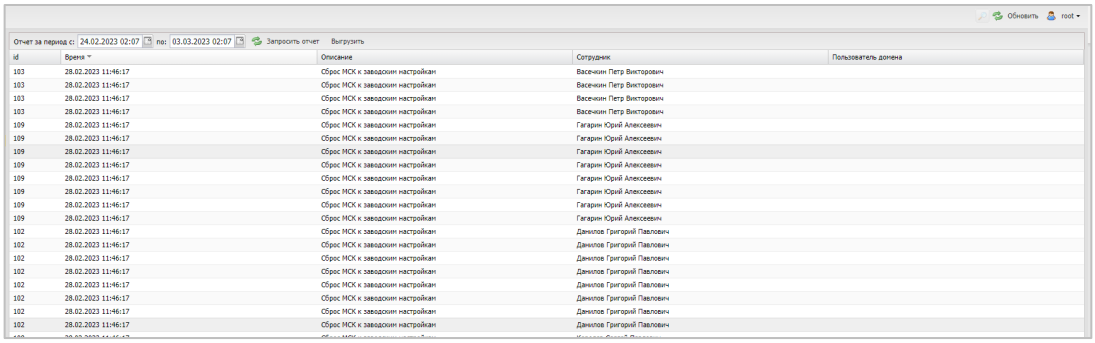


Рисунок 2.73 - Окно «События ИБ»

Для выбора периода построения отчёта используются поля ввода даты/времени **«Отчёт за период с»**, **«по»** (для начальной и конечной даты соответственно) в верхней панели инструментов. Нажмите на кнопку со значком календаря в требуемом поле и в открывшемся календаре выберите год, месяц, день и время. После задания периода отчета нажмите кнопку «Запросить отчет».

Сформированный отчёт содержит следующие столбцы:

- id – номер устройства в системе;
- Время – время наступления события;
- Описание – название события;
- Сотрудник – фамилия, имя и отчество сотрудника, на устройстве которого это событие наступило;
- Пользователь домена – ФИО сотрудника или e-mail, если ФИО не было импортировано.

В отчёт попадают события ИБ, указанные в таблице 2.2.

2.7.4 Отчёт «Перемещения»

В отчёте отображается информация о перемещении абонентов «UEM SafeMobile» (в виде ломаных линий на карте) за указанный Администратором интервал времени. Для формирования отчёта следует выбрать пункт главного меню **«Перемещения»**.

Для выбора периода построения отчёта используются поля ввода даты/времени **«Отчёт за период с»**, **«по»** (для начальной и конечной даты соответственно), для этого следует нажать на кнопку со значком календаря и выбрать год, месяц, день и время.

В поле **«Интервал (с)»** следует ввести интервал времени, на основе которого будут запрашиваться данные по координатам абонентов из базы данных.

В главной таблице необходимо выбрать сотрудника (сотрудников), отчёт о перемещении которых требуется сформировать. Затем нажать кнопку **«Запросить отчёт»**, чтобы отобразить линию перемещения абонента на карте, расположенную в информационной таблице, в соответствии с рисунком 2.74.

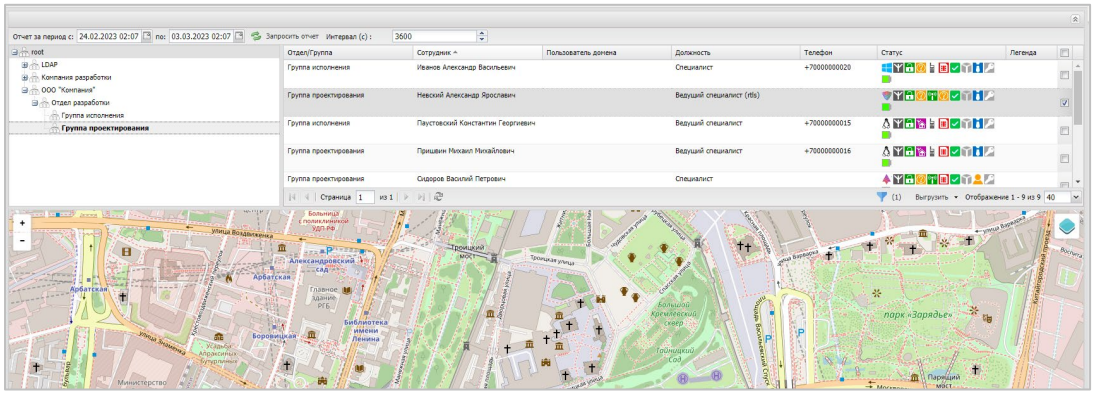


Рисунок 2.74 - Окно «Перемещения»

Если в таблице выбрано несколько сотрудников, траектории их перемещения отображаются разными цветами. Цвет траектории показывается в столбце **«Легенда»** главной таблицы.

Более подробные сведения об инструментах работы с картой приведены в разделе 2.6.4.

2.7.5 Отчёт «Профили»

В отчёте отображается информация о профилях, примененных на подключенных к системе МСК. Отчёт состоит из двух таблиц: верхняя таблица с реестром назначенных и применённых профилей; а в нижней таблице воспроизводятся установленные и примененные на МСК значения параметров политик выбранного профиля в соответствии с рисунком 2.75.

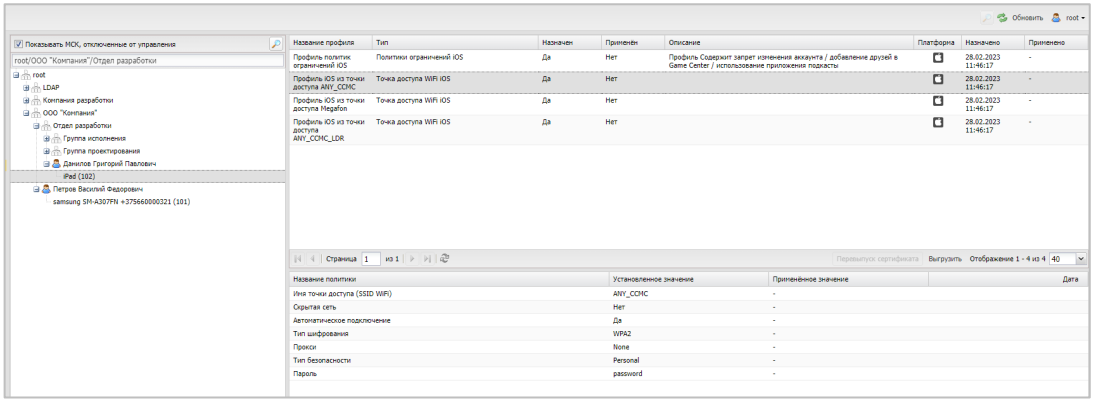


Рисунок 2.75 - Окно отчёта «Профили»

Верхняя таблица отчёта содержит следующие столбцы:

- Название профиля − название созданного в системе профиля;
- Тип − разновидность политик ОС;
- Назначен − «Да/Нет»;
- Применен − «Да/Нет»;
- Описание − описание настроек ОС, заданных в профиле;
- Платформа - значок платформы МСК, на которое назначен профиль;
- Назначено – время назначения;
- Применено – время применения.

Нижняя таблица отчёта содержит следующие столбцы (данные отображаются при выборе МСК в верхней таблице):

- Название политики − название политики профиля;
- Установленное значение − значение параметра установленной на МСК политики;
- Примененное значение − значение параметра политики, которое было применено на МСК;
- Дата − дата/время, когда значение политики было применено на МСК.

Для просмотра отчёта необходимо в панели ОШС выбрать МСК сотрудника, а затем в верхней таблице интересующий профиль. В нижней таблице отобразится информация с установленными и применёнными на МСК значениями параметров политики назначенного профиля.

Сертификаты, выписанные через сервер SCEP, могут быть принудительно перевыпущены по команде администратора. Кнопка «перевыпуск сертификата» располагается в блоке отображения списка профилей, назначенных на МСК. Кнопка становится активной при следующих условиях:

- В дереве ОШС выбран МСК;
- Доступна для следующих типов профилей:
  - VPN iOS,
  - VPN для приложений (Per-App VPN) iOS,
  - Точка доступа WiFi iOS,
  - Точка доступа WiFi Android,
  - Exchange аккаунт iOS,
- В качестве учетных данных, в профиле выбраны настройки SCEP.

При нажатии кнопки начинается процесс перевыпуска сертификата.

2.7.6 Отчёт «Правила управления»

В отчёте отображается информация о ПУП, примененных на подключенных к системе МСК. Отчёт состоит из двух таблиц: верхняя таблица с реестром назначенных и применённых правил управления; а в нижней таблице воспроизводятся установленные и примененные на МСК значения параметров ПУП в соответствии с рисунком 2.76.

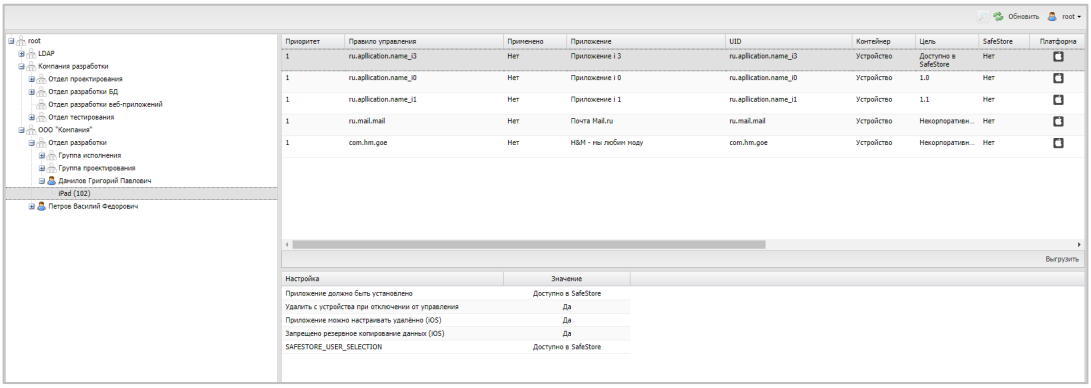


Рисунок 2.76 - Окно отчёта «Правила управления»

Верхняя таблица отчёта содержит следующие столбцы:

- Приоритет – если назначено несколько правил с одинаковым приложением, то применяется правило с приоритетом равным единице;
- Правило управления − название созданного в системе ПУП;
- Применено – Да / Нет;
- Приложение – название приложения;
- UID;
- Контейнер – приложение установлено в контейнере;
- Цель – цель назначения ПУП;
- Платформа − платформа МСК, на котором установлено приложение и назначен ПУП;
- Описание − описание настроек ОС;
- Условия – выполнено/не выполнено;
- На устройстве – версия приложения, установленного на устройстве.
- Включено – Включено / Заблокировано;
- Выбор пользователя – отображается при выборе МСК в ОШС;
- Статус – применено / не применено;
- Дата назначения;
- Дата применения.

Нижняя таблица отчёта содержит следующие столбцы:

- Настройка – описание параметров ПУП;
- Значение – Да / Нет.

Для просмотра отчёта необходимо в панели ОШС выбрать МСК сотрудника, а затем в верхней таблице интересующий ПУП. В нижней таблице отобразится информация с установленными и применёнными на МСК значениями параметров назначенного ПУП.

2.7.7 Отчет «Правила управления (UID)»

В отчёте отображается информация о ПУП одного приложения, примененного на подключенных к системе МСК. Страница отчета состоит из следующих блоков (рисунок 2.77):

- Блок поиска приложения, по которому будет сформирован отчет;
- Блок указания подразделения (дерево ОШС), к комплектам которого будет применен отчет;
- Блок со списком комплектов, на которых установлено заданное приложение;
- Блок вывода отчета о настройках ПУП, в выбранном комплекте.

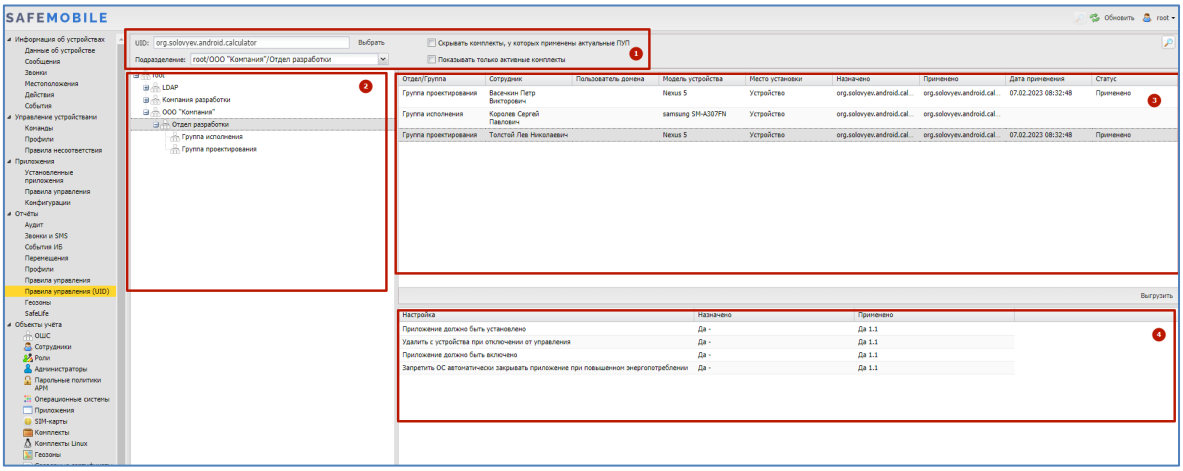


Рисунок 2.77 - Расположение блоков в разделе «Отчеты – Правила управления (UID)»

Блок поиска приложения состоит из следующих элементов:

- UID – Поле отображения UID выбранного приложения;

- Кнопка «Выбрать» - Открывает список приложений, установленных в комплектах системы и позволяет выбрать приложение для формирования отчета;
- Скрыть комплекты, у которых применены актуальные ПУП – фильтр (чекбокс). Если флаг фильтра включен, то из отчета будут исключены комплекты, на которые применен актуальный ПУП приложения;
- Показывать только активные комплекты – фильтр (чекбокс);
- Подразделение – поле отображения выбранного подразделения в структуре ОШС;

Блок списка комплектов представлен в виде таблицы, в которой каждая строка списка является информацией об одном комплекте, сгруппированной по следующим колонкам данных:

- Колонки таблицы, включенные по умолчанию;
    - Отдел/Группа – название группы в структуре ОШС, которой принадлежит пользователь (владелец МСК);
    - Сотрудник – ФИО сотрудника
    - Пользователь домена – ФИО сотрудника (или e-mail, если ФИО не было импортировано из AD);
    - Модель устройства;
    - Место установки – устройство или контейнер;
    - Назначено – наименование назначенного ПУП;
    - Применено – наименование примененного ПУП;
    - Дата применения – дата и время применения ПУП на комплект;
    - Статус - состояние или ошибка применения ПУП;
- Колонки таблицы, не включенные по умолчанию;
    - Должность,
    - SIM: Принадлежность,
    - Состояние роуминга,
    - IMSI,
    - ICCID,
    - Телефон,
    - Id,
    - Состояние блокировки,
    - Управление устройствами,
    - Последняя активность,
    - Тип соединения,
    - IP адрес,
    - Тип устройства,

    - IMEI,
    - UDID,
    - Серийный номер,
    - Тип контейнера,
    - Заряд аккумулятора,
    - Устройство: Принадлежность,
    - Монитор,
    - Платформа,
    - Версия,
    - Статус,
    - Условия,
    - Стратегия.
- Кнопка «Выгрузить» - выгрузка отчета (excel).

Блок отображения списка ПУП, выбранного комплекта представлен в виде таблицы, в которой каждая строка списка содержит информацию об одном «правиле управления приложениями» и распределена по следующим колонкам:

- Настройка – название настройки ПУП;
- Назначено – назначенное значение настройки ПУП;
- Применено – назначенное значение настройки ПУП, примененное на устройстве.

Чтобы сформировать отчет по ПУП, необходимо выполнить следующие действия:

1. В блоке выбора приложения нажать кнопку «Выбрать», после чего откроется список UID приложений, зарегистрированных в системе;

2. Выбрать в списке приложение, по которому необходимо сформировать отчет;

3. Установить фильтрам поиска необходимые значения (по умолчанию они включены);

4. В структуре ОШС указать подразделение, по комплектам которого будет сформирован отчет. Если ПУП с указанным приложением назначен или применен хотя бы на одном устройстве выбранного подразделения, то в соответствующем блоке будет отображен список комплектов, на которых установлено указанное приложение.

5. Выбрать в списке комплектов необходимый для просмотра значений настроек ПУП, после чего в соответствующем блоке будет отображен список значений назначенного и примененного на комплект ПУП.

Если у комплекта примененный и назначенный ПУП не совпадают, то строка в списке комплектов будет выделена цветом (рисунок 2.78).

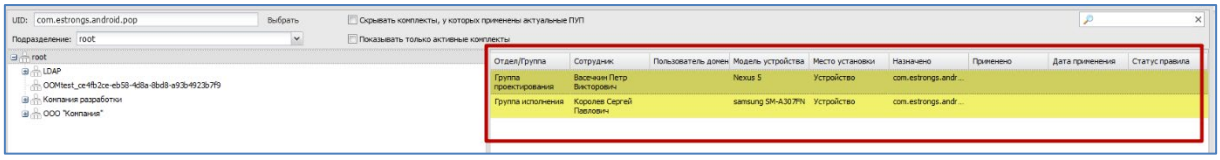


Рисунок 2.78 - Комплект с несовпадающими назначенными и примененными ПУПами

2.7.8 Отчет «Геозоны»

В отчете отображается информация о входе/выходе в/из геозоны абонентов «UEM SafeMobile» за указанный Администратором интервал времени. Для формирования отчёта следует выбрать пункт главного меню **«Геозоны»** (рисунок 2.79).

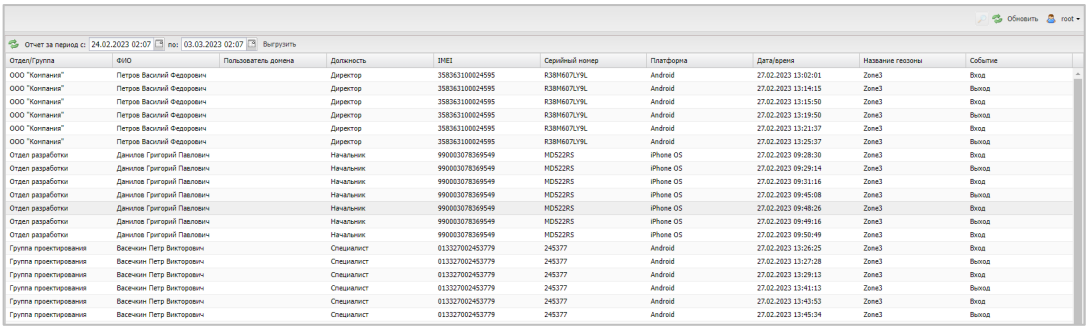


Рисунок 2.79 - Окно «Геозоны»

Для выбора периода построения отчёта используются поля ввода даты/времени **«Отчёт за период с»**, **«по»** (для начальной и конечной даты соответственно) в верхней панели инструментов, для этого следует нажать на кнопку со значком календаря и выбрать год, месяц, день и время. После задания периода отчета нажмите кнопку «Выгрузить». Сформированный отчёт содержит следующие столбцы:

- Отдел/группа − подразделение организации, в котором работает сотрудник;
- ФИО − фамилия, имя и отчество сотрудника;
- Пользователь домена - ФИО сотрудника или e-mail, если ФИО не было импортировано;
- Должность − должность сотрудника;
- Тип устройства − тип МСК, подключенного к системе (по умолчанию, в таблице не отображается);

- Модель устройства – модель МСК, подключенного к системе (по умолчанию, в таблице не отображается);
- IMEI;
- UDID (по умолчанию, в таблице не отображается);
- Серийный номер – для МСК на платформе iOS и Android;
- Платформа – мобильная платформа МСК;
- Принадлежность – признак собственности МСК (по умолчанию, в таблице не отображается);
- Координаты – координаты регистрации события в системе (по умолчанию, в таблице не отображается);
- Дата/время – дата и время регистрации события в системе;
- Название геозоны – название созданной и активированной в системе геозоны;
- Событие – вход/выход в/из геозоны.

2.7.9 Отчет «SafeLife»

Отчет предназначен для отображения информации по сотрудникам, использующим браслеты «SafeLife» за заданный промежуток времени (рисунок 2.80).

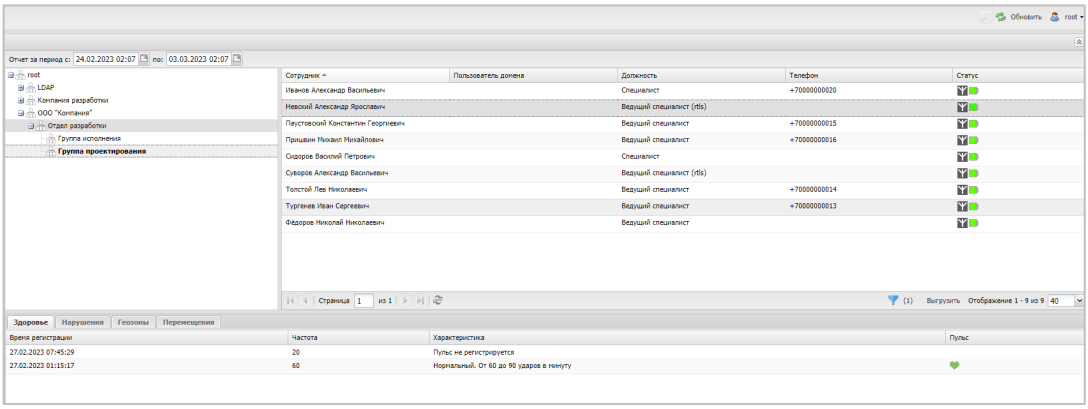


Рисунок 2.80 - Окно «SafeLife»

Для выбора периода построения отчёта используются поля ввода даты/времени **«Отчёт за период с»**, **«по»** (для начальной и конечной даты соответственно) в верхней панели инструментов, для этого следует нажать на кнопку со значком календаря и выбрать год, месяц, день и время.

В дереве ОШС необходимо выбрать подразделение, а в главной таблице необходимо выбрать сотрудника, отчёт по которым требуется сформировать в соответствии с рисунком 2.81.

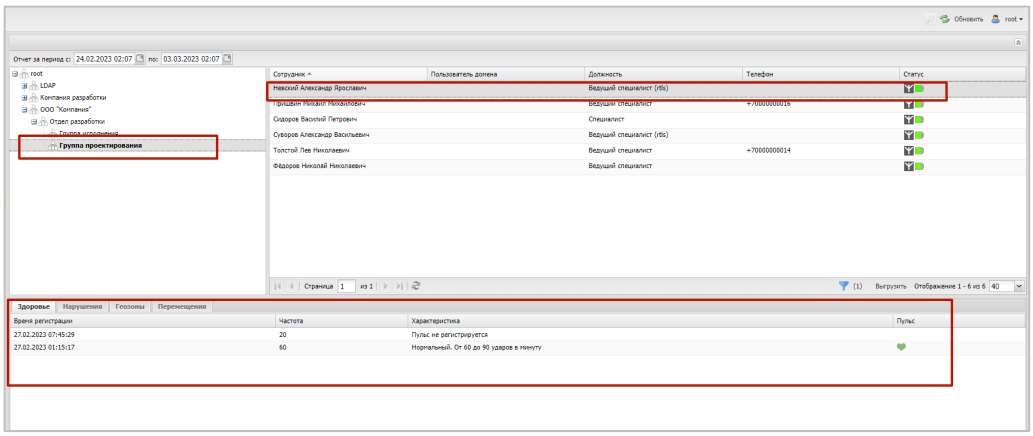


Рисунок 2.81 - Выбор сотрудника для просмотра отчета «SafeLife»

В нижней части расположено окно с отчетами со следующими вкладками:

- Здоровье;
- Нарушения;
- Геозоны;
- Перемещения.

На вкладке **«Здоровье»** отображается таблица с показаниями пульса (рисунок 2.82:

- Время регистрации;
- Частота пульса;
- Характеристика (пониженный/нормальный/повышенный);
- Пульс.

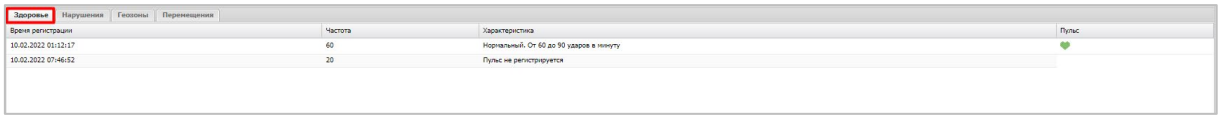


Рисунок 2.82 - Вкладка «Здоровье»

На вкладке **«Нарушения»** отображается таблица со следующими столбцами (рисунок 2.83):

- Время регистрации;
- Нарушения и уведомления − наименование нарушения или уведомления: пульс не регистрируется/нет движения/пульс и движение не регистрируется/зафиксировано падение/нажатие тревожной кнопки/изменение высоты (события, которое регистрируется при подъеме или спуске на 10 метров менее, чем за 10 минут);
- Геозоны, в которых произошло нарушение или уведомление.

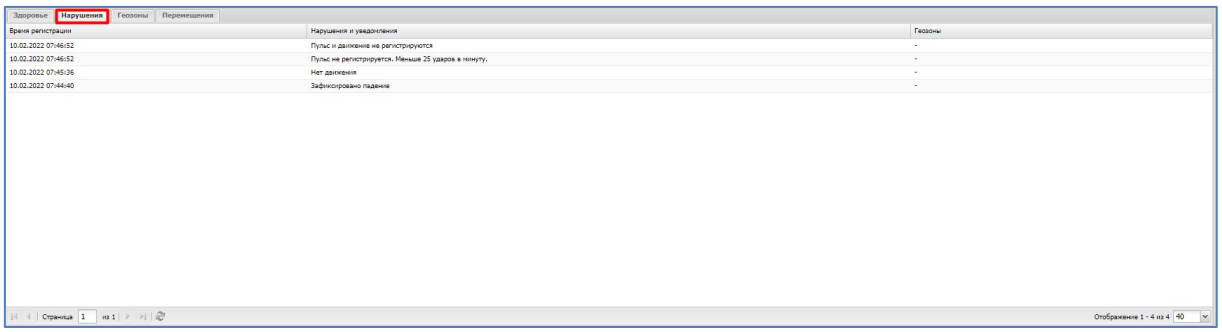


Рисунок 2.83 - Вкладка «Нарушения»

На вкладке **«Геозоны»** отображается таблица учета времени пребывания в геозонах и карта с геозонами. Таблица содержит следующие столбцы (рисунок 2.84):

- Время – время входа в геозону;
- Наименование – наименование геозоны;
- Выход – время выхода из геозоны;
- Время пребывания – время пребывания в геозоне.

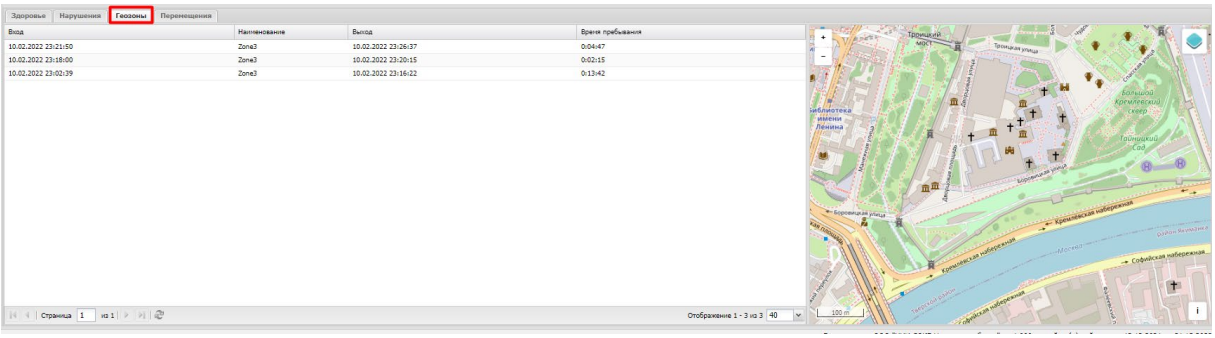


Рисунок 2.84 - Вкладка «Геозоны»

На вкладке **«Перемещения»** отображаются координаты точек маршрута перемещений сотрудника и фрагмент карты, на которой в виде ломаной линии отображена информация о местоположении и перемещении абонента. Таблица содержит следующие столбцы (рисунок 2.85):

- Время регистрации координат;
- Широта;
- Долгота;
- Геозона.

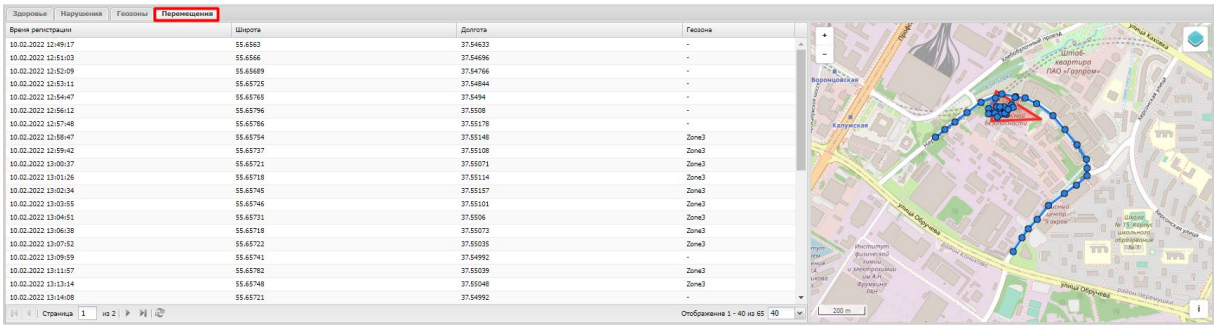


Рисунок 2.85 - Вкладка «Перемещения»

2.7.10 Аудит SMAPI

Раздел отображает журнал данных по работе SMAPI через сервисные учетные записи. Доступ к журналу имеют администраторы назначенные на корень дерева ОШС и определяется полномочием на просмотр.

Данные отображаются в виде списке, каждая строка которого содержит информацию о подключениях через сервисные учетные записи (рисунок 2.86). Каждая строка содержит:

- Служебная запись - наименование сервисной учетной записи;
- Метод,
- URL,
- Область управления,
- Параметры - входные параметры запроса;
- Время - время регистрации обращения в БД;
- Результат.

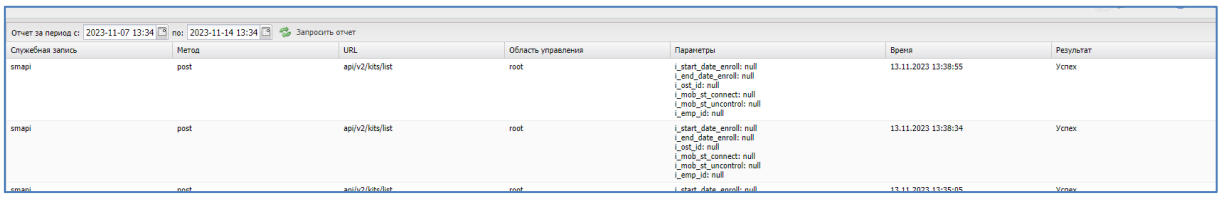


Рисунок 2.86 - раздел «Аудит SMAPI»

По умолчанию журнал отображает данные за последние 7 календарных дней. Задать период отображения можно в фильтре по дате и времени над списком записей раздела. Для этого следует задать «дату и время начала - конца периода» и нажать кнопку «Запросить отчет», после чего данные в разделе будут сформированы в соответствии с установками фильтра.

2.8 Управление объектами учёта (пункт меню «Объекты учёта»)

Пункт главного меню «Объекты учёта» предназначен для управления объектами учёта «UEM SafeMobile»:

- ОШС;
- Сотрудники;
- Роли;
- Администраторы;
- Парольные политики АРМ;
- Операционные системы;
- Приложения;
- SIM-карты;
- Комплекты;
- Комплекты Linux;
- Геозоны;
- Серверные сертификаты;
- Подключения к серверам;
- Настройки SCEP;
- Клиентские сертификаты;
- Группы;
- Шаблоны писем.

2.8.1 Организационно-штатная структура

Пункт меню **«ОШС»** открывает окно в соответствии с рисунком 2.87, в котором отображаются подразделения организации в виде иерархической структуры.

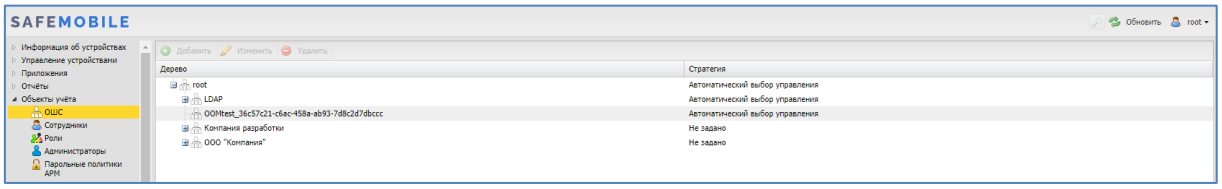


Рисунок 2.87 - Окно «ОШС»

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- Добавить – предназначена для добавления нового подразделения в структуру организации;

- Изменить – предназначена для изменения параметров подразделения, имеющегося в структуре организации;
- Удалить – предназначена для удаления подразделения, имеющегося в структуре организации.

Для добавления нового подразделения в структуру организации следует выбрать родительское подразделение и нажать кнопку **«Добавить»**, после чего появится окно в соответствии с рисунком 2.88.

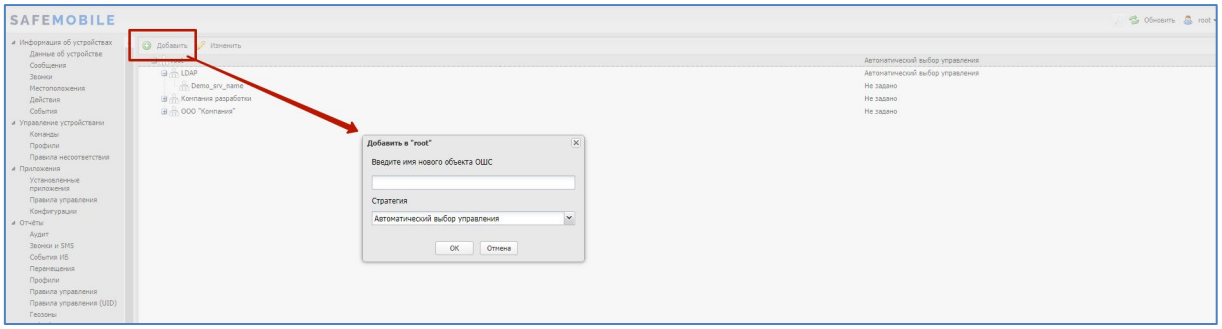


Рисунок 2.88 - Добавление подразделения в ОШС

В этом окне необходимо ввести название создаваемого подразделения. Опционально можно выбрать стратегию управления устройства Android по умолчанию. Если стратегию не выбрать, то будет использоваться стратегия, заданная в родительских подразделениях. Затем нажать кнопку **«OK»**. Для отмены создания подразделения необходимо нажать кнопку **«Отмена»**.

Стратегия по умолчанию будет автоматически выбираться при создании нового кода приглашения, при подключении МСК с авторизацией пользователя в AD и при подключении с использованием технологии КМЕ.

Если выбрать подразделение и нажать кнопку **«Добавить»**, новое подразделение будет добавлено в выбранное в качестве подчиненного.

Для изменения названия выбранного подразделения или стратегии по умолчанию нажмите кнопку **«Изменить»**, после чего появится окно в соответствии с рисунком 2.89. Для узлов ОШС, синхронизированных с AD, изменение названия подразделения недоступно.

Нажмите кнопку **«OK»**, чтобы подтвердить изменение или кнопку **«Отмена»**, чтобы отменить его.

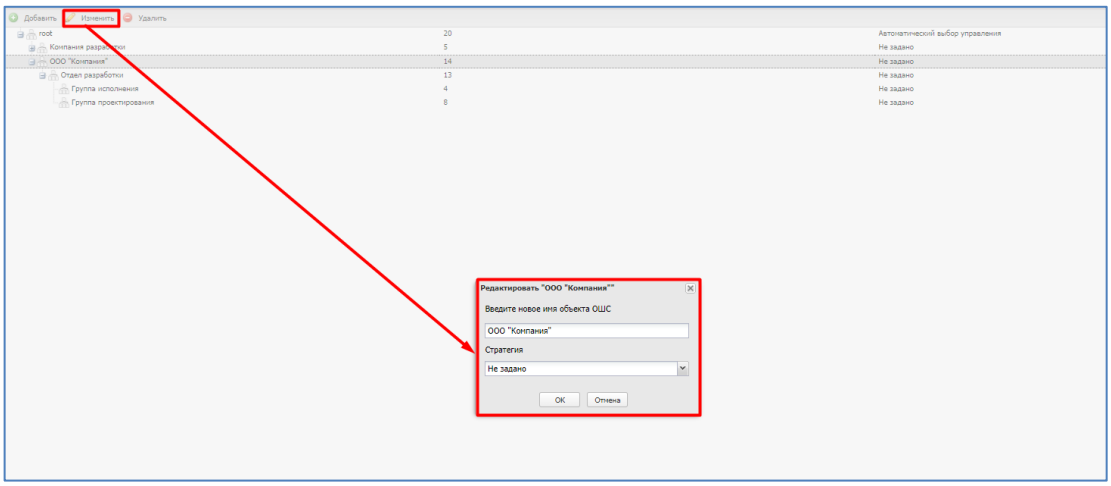


Рисунок 2.89 0 Изменение подразделения в ОШС

Для удаления выбранного подразделения из структуры организации нажмите кнопку **«Удалить»**, после чего появится окно в соответствии с рисунком 2.90.

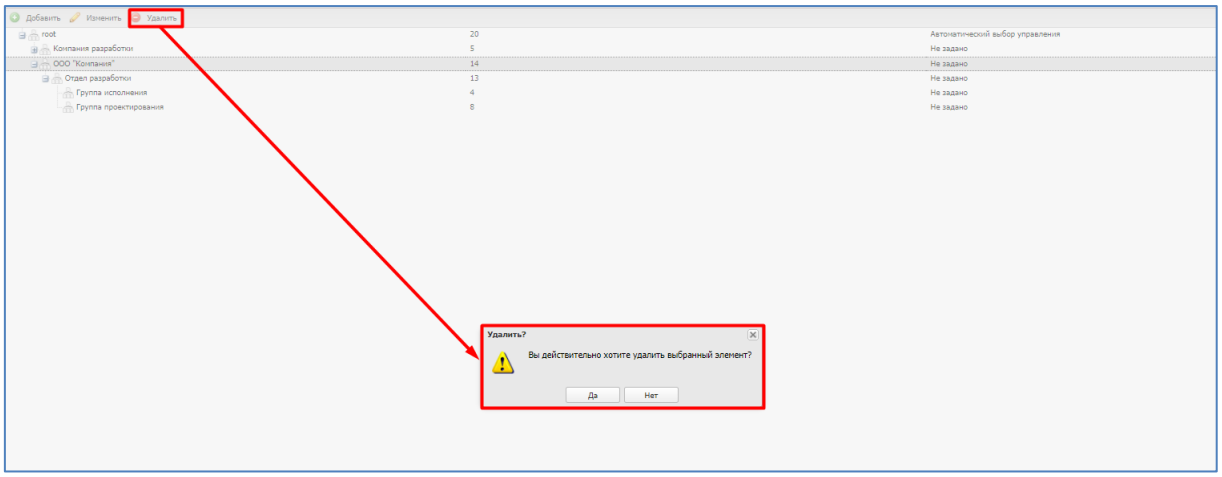


Рисунок 2.90 - Удаление подразделения в ОШС

Нажмите кнопку **«Да»**, чтобы подтвердить удаление или кнопку **«Нет»**, чтобы отменить его.

2.8.2 Сотрудники

Раздел содержит справочник сотрудников и ведется для учёта абонентов МСК. Перед созданием комплектов МСК в «UEM SafeMobile» необходимо внести данные о сотрудниках организации

Страница раздела состоит из дерева ОШС, списка сотрудников подразделения ОШС, информации о сотруднике, выбранного в списке сотрудников подразделения. (рисунок 2.91)

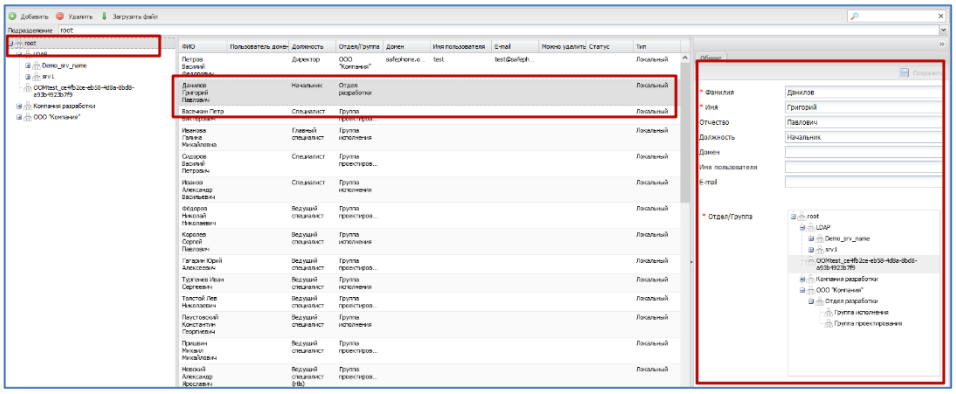


Рисунок 2.91 - Окно «Сотрудник»

Таблица списка сотрудников содержит следующие столбца данных:

- Столбцы, отображаемые по умолчанию:
  - ФИО – фамилия, имя и отчество сотрудника;
  - Пользователь домена - Отображает ФИО сотрудника (или e-mail, если ФИО не было импортировано),
  - Должность – должность сотрудника;
  - Отдел/Группа – подразделение организации, в котором работает сотрудник;
  - Домен – доменное имя организации пользователя;
  - Имя пользователя – имя пользователя (логин) в электронной почте;
  - E-mail – адрес электронной почты;
  - Можно удалить – отметка о том, что импортированного пользователя можно удалить из системы (Да/Не заданно)
  - Статус – статус блокировки пользователя (Заблокирован/Разблокирован/Не заданно)
  - Тип – тип пользователя (локальный/импорт)

- Столбцы, отображаемые опционально:
    - id − номер сотрудника с комплектом в системе;
    - objectGUID;
    - memberOf;
    - name;
    - givenName;
    - middleName;
    - sn;
    - mail;
    - mailNickName;
    - mobile;
    - telephoneNumber;
    - distinguishedName;
    - userPrincipalName;
    - department;
    - userAccountControl;
    - lockoutTime;
    - objectCategory;
    - whenChanged;
    - whenCreated;
    - employeeID
    - manager;
    - title;
    - company;
    - samaccountName.

Блок с информацией о сотруднике отображает следующие данные:

- Общие:
    - Фамилия,
    - Имя,
    - Отчество,
    - Должность,
    - Домен,
    - Имя пользователя,
    - E-mail,
    - Отдел/Группа (подразделение в ОШС).

- Импорт:

  (вкладка отображается только для импортированных пользователей)

  - Поля данных о пользователях, импортированных из внешнего каталога,
    - objectGUID,
    - memberOf,
    - name,
    - displayName,
    - givenName,
    - middleName,
    - sn,
    - mail,
    - mailNickName,
    - mobile,
    - telephoneNumber,
    - distinguishedName,
    - userPrincipalName,
    - department,
    - userAccountControl,
    - lockoutTime,
    - objectCategory,
    - employeeID,
    - manager,
    - title,
    - company,
    - whenChanged,
    - whenCreated,
    - samaccountName.

Для добавления записи используется кнопка **«Добавить»**. Затем в правой части окна следует заполнить форму, содержащую информацию о сотруднике (рисунок 2.92). Для этого необходимо ввести сведения в обязательные поля: **«Фамилия»**, **«Имя»**. После заполнения формы нажать кнопку **«Сохранить»**, и запись о новом сотруднике будет добавлена в систему.

Кроме того, в списке ОШС, расположенном ниже поля «**Отдел/группа»**, выбрать подразделение, в котором работает сотрудник. **Изменение расположения доступно только для уже существующих записей о сотрудниках**.

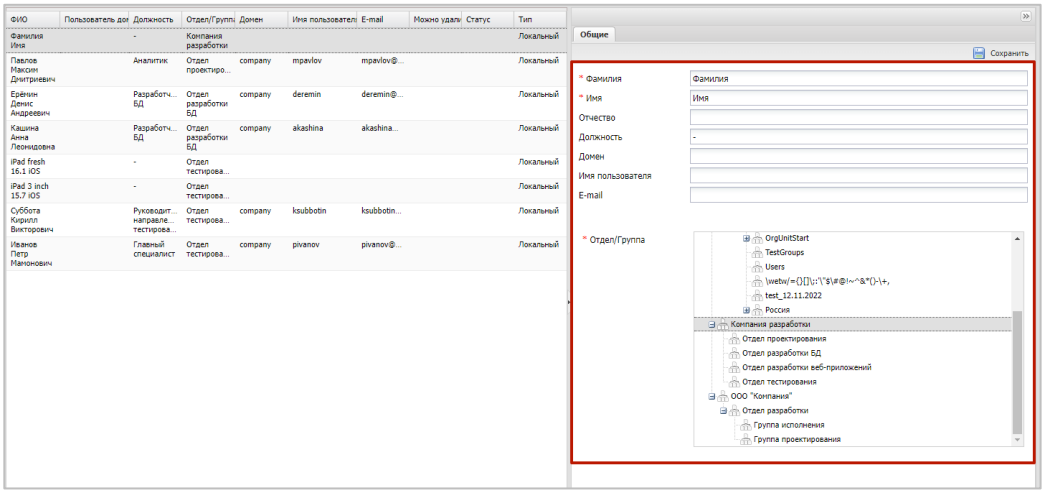


Рисунок 2.92 - Создание записи о сотруднике

После добавления нового сотрудника рекомендуется убедиться в наличии для него календаря рабочего времени в разделе **«Календарь»** (по умолчанию сотрудникам назначается календарь подразделения, если он задан). У Администратора появится возможность получать данные о местоположении сотрудника и его комплекта в рабочее время. Подробнее описание календаря приведено в п. 2.11, а об определении местоположения в п. 2.6.4.

Для редактирования необходимо выбрать в таблице запись о сотруднике и внести изменения в поля в правой части окна. В списке подразделений организации можно выбрать необходимый отдел и группу для перемещения туда редактируемой записи о сотруднике. При нажатии кнопки **«Сохранить»** внесенные изменения сохраняются в БД.

Для удаления объекта учёта необходимо выбрать в таблице (рисунок 2.93) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удаляется из базы при отсутствии связанных объектов учёта.

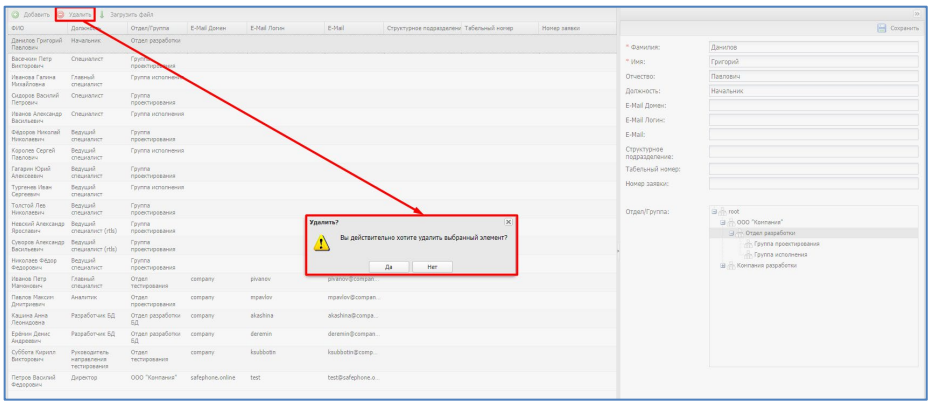


Рисунок 2.93 - Удаление сотрудника

Кнопка **«Загрузить файл»** предназначена для загрузки списка сотрудников из файла формата **«xlsx»** (рисунок 2.94).

	A	B	C	D	E	F	G	H	I
1	Фамилия	Имя	Отчество	Должность	Домен	Имя пользователя	E-mail	Место работы 1	Место работы 2
2				Директор				1.НИИ СОКБ	
3									
4									

Рисунок 2.94 - Список сотрудников в файле формата «xlsx»

Структура колонок в файле должна быть следующая:

- Фамилия (обязательно для заполнения);
- Имя (обязательно для заполнения);
- Отчество;
- Должность (обязательно для заполнения);
- Домен
- E-mail
- Место работы 1 (обязательно для заполнения);
- Место работы 2;
- Место работы …;
- Место работы 10.

2.8.3 Роли

Пункт меню **«Роли»** открывает окно (рисунок 2.95), предназначенное для управления ролями Администраторов «UEM SafeMobile».

В левой части таблицы в столбце **«Роль»** отображается список ролей Администраторов, а в правой части в столбце **«Полномочия»** − список полномочий, которые можно назначить каждой выбранной роли.

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- Добавить – предназначена для создания новой роли;
- Изменить – предназначена для изменения названия существующей роли;
- Удалить – предназначена для удаления выбранной роли.

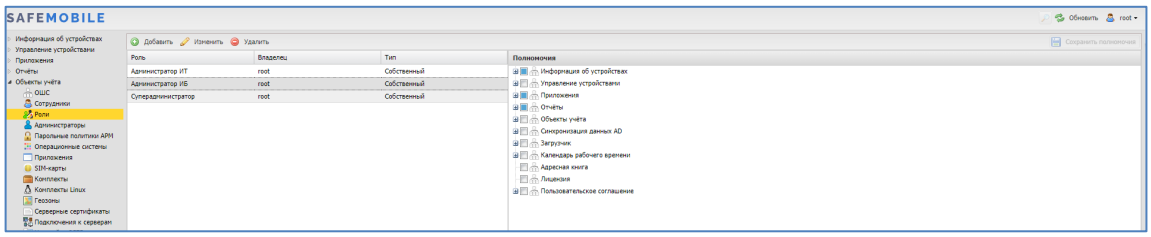


Рисунок 2.95 - Окно «Роли»

Для добавления новой роли в перечень ролей организации нажмите кнопку **«Добавить»** (рисунок 2.96), после чего появится следующее окно:

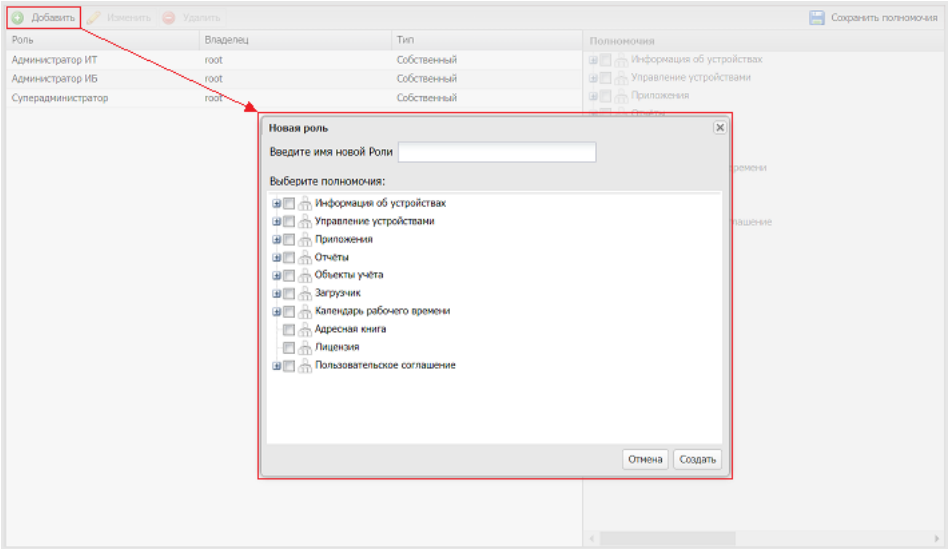


Рисунок 2.96 - Создание роли Администратора

После этого необходимо ввести имя и указать полномочия для новой роли, установив соответствующие флажки.

При добавлении новой роли следует учитывать, что для администраторов, назначенных не на корень дерева ОШС в иерархической структуре подразделений, действуют следующие ограничения:

1. Только администраторам, назначенным на корень дерева ОШС, доступны разделы:
    - Парольные политики АРМ,
    - Объекты учета - Шаблоны писем,
    - Синхронизация данных с AD,
    - Лицензия.

2. Только администраторы, назначенные на корень дерева ОШС, могут редактировать пользовательское соглашение. Прочие администраторы могут только его просматривать и рассылать;
3. Только администраторы, назначенные на корень дерева ОШС, могут редактировать информацию в разделах: «Настройки SCEP», «ОС», «Подключения к серверам».

Для сохранения новой роли и назначенных ей полномочий необходимо нажать кнопку **«Создать»**, после чего она отобразится в списке слева, а также станет доступной для выбора в списке ролей в окне **«Администратор»**.

Для изменения названия роли следует нажать кнопку **«Изменить»** (рисунок 2.97), после чего появится окно в соответствии с рисунком 2.96. После редактирования, для подтверждения изменения, необходимо нажать кнопку **«ОК»**.

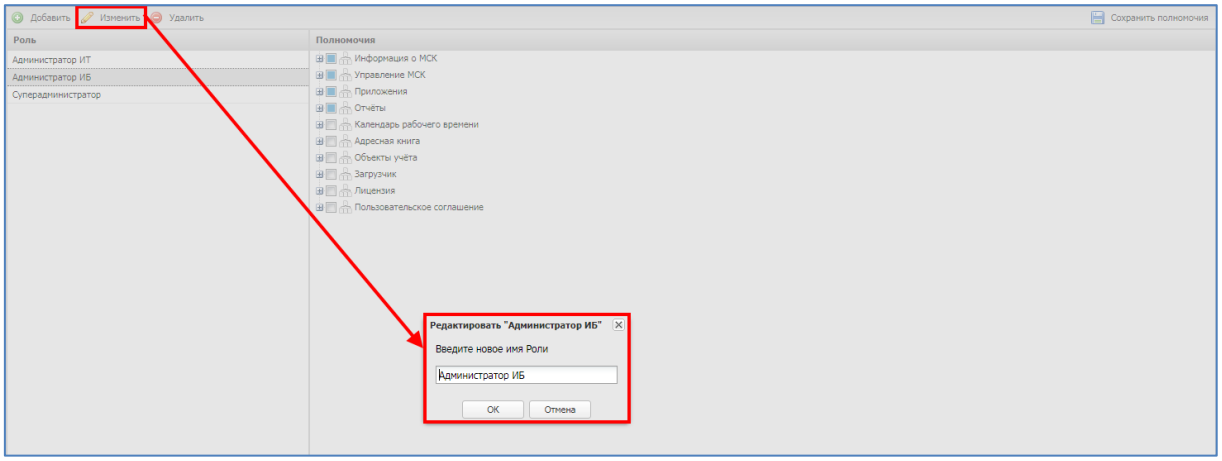


Рисунок 2.97 - Изменение роли Администратора

Для удаления существующей роли требуется нажать кнопку **«Удалить»**. После подтверждения действия (рисунок 2.98) роль будет удалена.

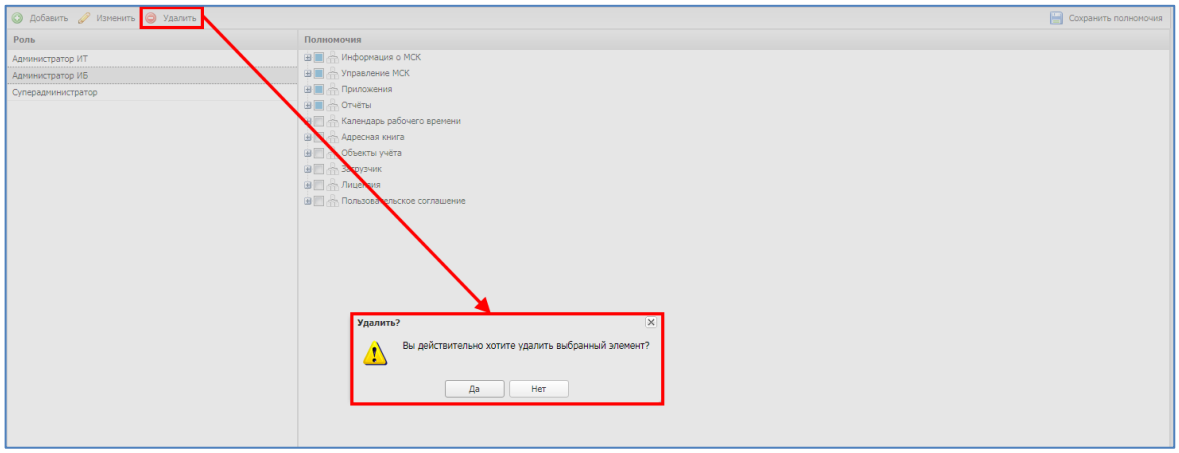


Рисунок 2.98 - Удаление роли Администратора

Примечания.

1. По умолчанию в системе имеется три роли, наделенные соответствующими полномочиями: Администратор ИБ, Администратор ИТ и Суперадминистратор. С полномочиями предустановленных ролей можно ознакомиться в приложении Г.

2. Роль Суперадминистратор обладает максимальными полномочиями и не подлежит редактированию или удалению.

2.8.4 Администраторы

Раздел содержит в себе справочник администраторов «UEM SafeMobile» и функционал по управлению справочником:

- Просмотр списка администраторов;
- Добавить/Удалить/Заблокировать администратора;
- Редактировать данные администратора;

Справочник представлен в виде списка администраторов и блока просмотра информации об администраторе (рисунок 2.99).

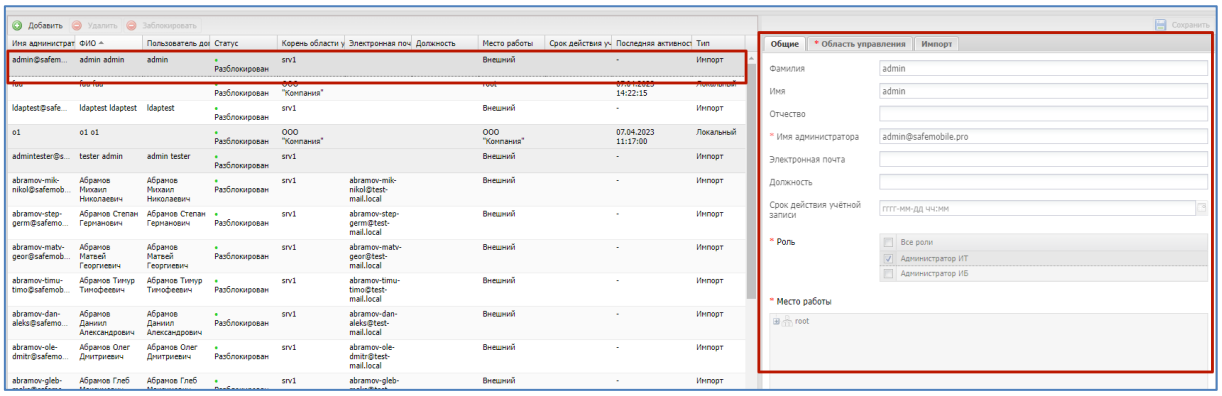


Рисунок 2.99 - Окно «Администратор»

В таблице в левой части окна отображаются следующие столбцы:

- Имя администратора – учетная запись администратора (логин);
- ФИО – фамилия, имя и отчество сотрудника, назначенного администратором;
- Пользователь домена - отображает ФИО администратора (или e-mail, если ФИО не было импортировано),
- Статус – состояние учётной записи администратора (заблокирована или не

заблокирована). Статус администратора можно изменить с помощью кнопок «Заблокировать» и «Разблокировать». Изменение статуса допускается только для локальных администраторов;

- Корень области управления – начальный узел поддерева ОШС, на который назначен администратор;
- Электронная почта;
- Должность;
- Место работы;
- Срок действия учетной записи (дата и время);
- Последняя активность (дата и время);
- Тип – тип записи об администраторе (локальный/импорт).

В блоке просмотра информации об администраторе отображаются следующие данные:

- Общие:
  - Фамилия,
  - Имя,
  - Отчество,
  - Имя администратора,
  - Электронная почта,
  - Должность,
  - Срок действия учетной записи,
  - Кнопка «Изменить пароль»
    (При нажатии открывается диалоговое окно запроса нового пароля для администратора);
  - Роль,
  - Место работы,
- Область управления:
  - Дерево ОШС,
- Импорт:
  (вкладка отображается только для импортированных администраторов)
  - Поля данных об администраторах, импортированных из внешнего каталога.

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- Добавить – предназначена для добавления новой учётной записи Администратора;
- Удалить – предназначена для удаления выбранной учётной записи Администратора; Заблокировать – предназначена для блокирования выбранной учётной записи Адми-нистратора;
- Разблокировать – предназначена для разблокирования выбранной учёт-ной записи Администратора (кнопка доступная только для заблокированных учётных записей).

2.8.4.1 Редактирование данных администратора

Чтобы изменить данные об администраторе, необходимо выполнить следующие действия:

1. Найти строку с записью об администраторе, подлежащего редактированию;
2. В блоке с информацией об администраторе внести необходимые изменения;
3. Нажать кнопку «Сохранить».

Примечание.

1. *Редактирование данных администраторов, импортированных из внешних каталогов не доступно.*
2. *Для администраторов любого типа допустимо изменить «Область управления»*

2.8.4.2 Добавить нового администратора

Для добавления нового администратора нажмите кнопку **«Добавить»**, после чего следует заполнить форму в правой части окна, на вкладке «Администратор» выбрать роль администратора и область управления в соответствии с рисунком 2.100. Область управления – это поддерево ОШС, на которое администратор может влиять, начиная с узла, на который он назначен и заканчивая устройствами. В дальнейшем для admini-

стратора интерфейс будет отображаться только из своей области управления в соответствии с ролью и предоставленным правам. Обязательные для заполнения поля отмечены *.

> ***Примечание.***
>
> *Имя пользователя Администратора должно начинаться с латинского символа. Может содержать латинские символы, цифры, точки, символы подчёркивания и тире. Использование других символов не допускается. Максимальная длина имени пользователя 32 символов.*

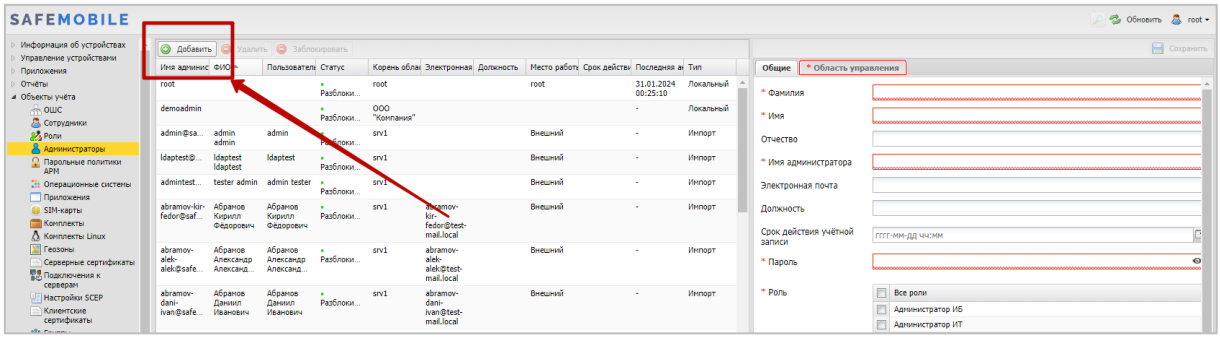


Рисунок 2.100 - Создание Администратора

Для сохранения записи об Администраторе, нажмите кнопку **«Сохранить»**, после чего новая запись отобразится в таблице Администраторов в левой части окна.

Для смены пароля имеющемуся Администратору необходимо выбрать его в списке слева, после чего нажать кнопку **«Изменить пароль»** (рисунок 2.101) в правой части окна на вкладке **«Администратор».** Если пароль, на который осуществляется смена, не соответствует установленной парольной политике, то при первом входе Администратору потребуется его изменить.

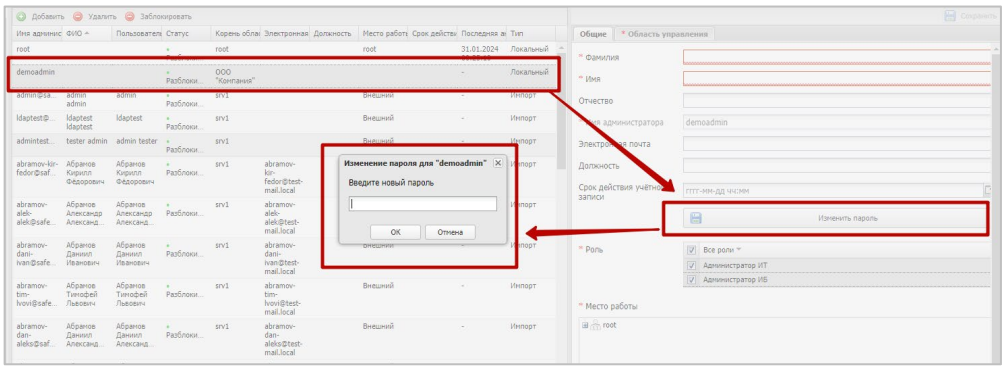


Рисунок 2.101 - Изменение пароля Администратора

2.8.5 Парольные политики АРМ

Для настройки параметров пароля и учетной записи при входе в «UEM SafeMobile» следует открыть пункт меню **«Парольные политики АРМ»** (рисунок 2.102).

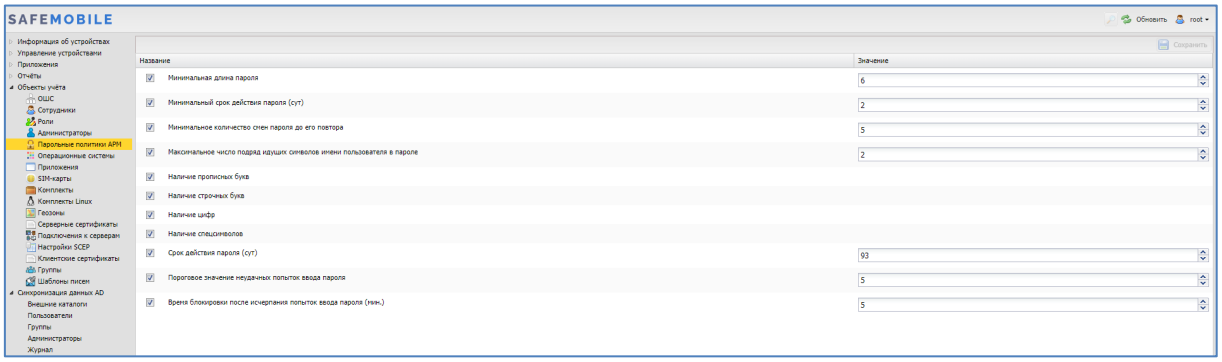


Рисунок 2.102 - Окно «Парольные политики АРМ»

Таблица парольных политик состоит из следующих столбцов:

- Название − название параметра парольной политики, который можно включить или отключить с помощью флажков;
- Значение − значение, которое необходимо для применения параметра парольной политики (при его наличии). После установки системы отображаются рекомендованные величины.

В таблице 2.5 указываются параметры парольных политик АРМ и рекомендованные значения.

Таблица 2.5 − Параметры парольной политики и рекомендованные значения

Название	Значение
Минимальная длина пароля	6
Минимальный срок действия пароля (сут)	2
Минимальное количество смен пароля до его повтора	5
Максимальное количество подряд идущих символов имени пользователя в пароле	2
Наличие прописных букв	Да
Наличие строчных букв	Да
Наличие цифр	Да

Название	Значение
Наличие спецсимволов	Да
Срок действия пароля (сут)	93
Пороговое значение неудачных попыток ввода пароля	5
Время блокировки после исчерпания попыток ввода пароля (мин.)	5

После выбора значений для сохранения параметров парольных политик нажмите кнопку **«Сохранить»**.

Примечание.

- *Парольные политики АРМ действуют только на локальных администраторов. На импортированных администраторов действуют доменные парольные политики.*
- *Спецсимволами являются следующие знаки: !$#%@^&*()~/[]*
  Знаки «+» и «-» спецсимволами на являются.

2.8.6 Операционные системы

Справочник операционных систем ведется для учёта используемых мобильных платформ для связи приложений и ОС. Данные об ОС необходимо внести в соответствующий справочник до начала регистрации МСК в «UEM SafeMobile».

Чтобы открыть окно **«Операционные системы»**, необходимо выбрать соответствующий пункт главного меню АРМ, после чего отобразится таблица с перечнем операционных систем и их версий в соответствии с рисунком 2.103. Поле **«id»** с номером операционной системы (по умолчанию, в таблице не отображается).

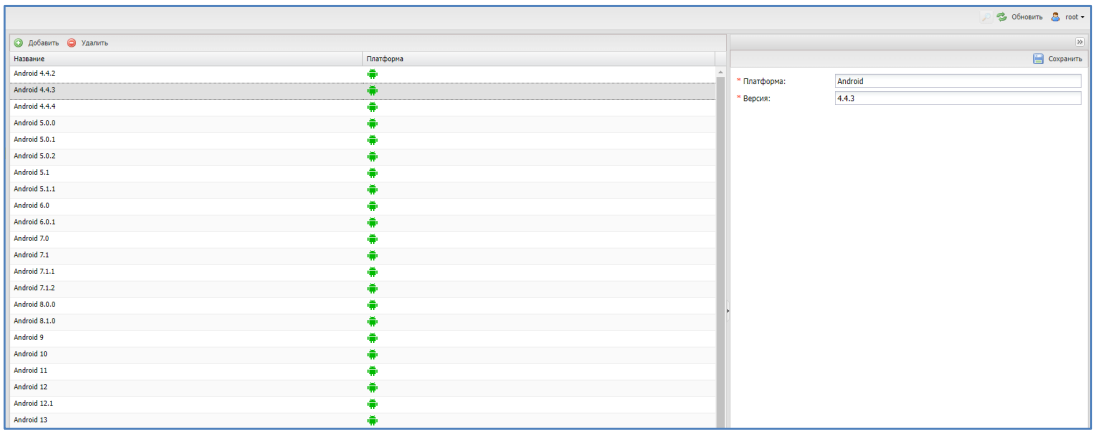


Рисунок 2.103 - Окно «Операционные системы»

Для добавления новой ОС в «UEM SafeMobile» используется кнопка **«Добавить»** в панели инструментов окна (рисунок 2.104), которая позволяет в правой части окна выбрать мобильную платформу в поле **«Платформа»** и указать версию добавляемой ОС в поле **«Версия»**.

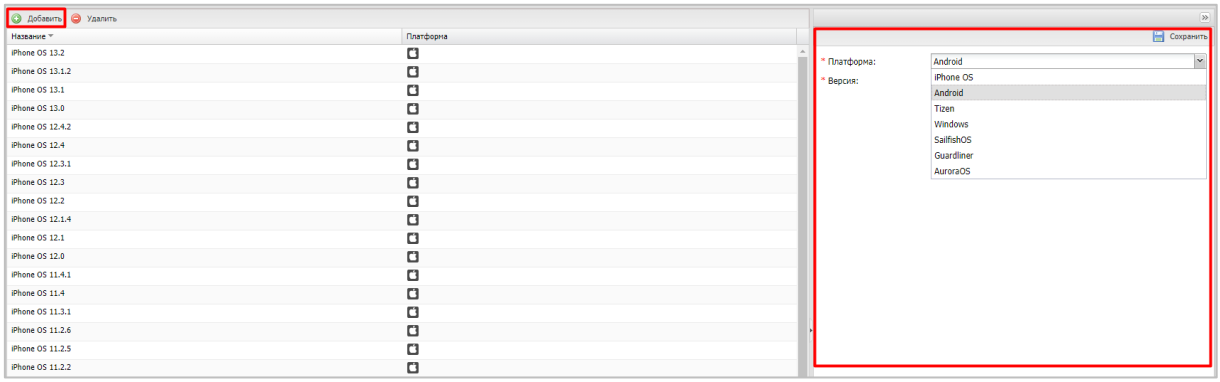


Рисунок 2.104 - Добавление ОС

После нажатия кнопки **«Сохранить»** (рисунок 2.105) созданная запись об ОС будет сохранена в системе. Для удаления записи об ОС используется кнопка **«Удалить»**.

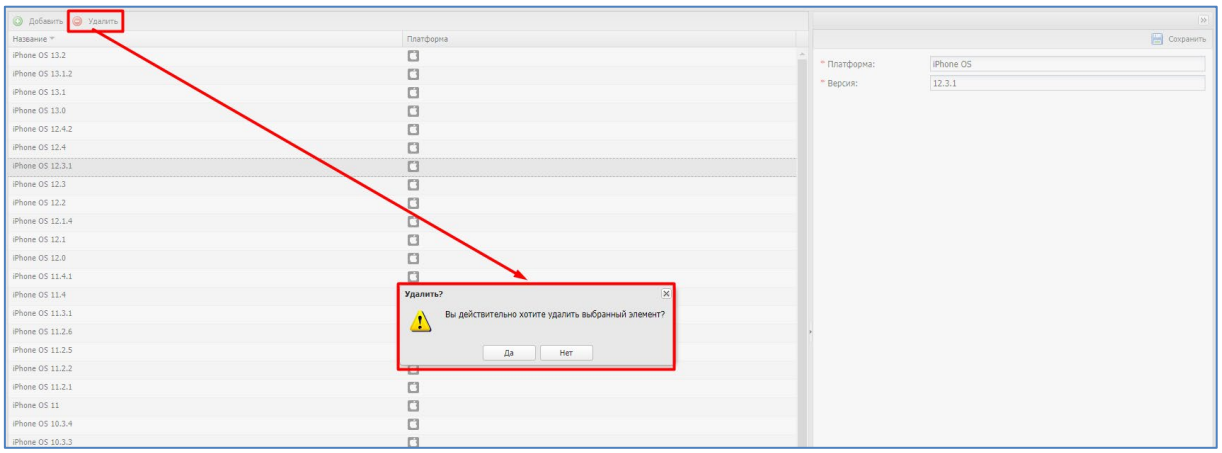


Рисунок 2.105 - Удаление ОС

При нажатии кнопки **«Удалить»** (рисунок 2.105) запрашивается подтверждение выполняемого действия, и выбранная запись об ОС удаляется из базы при отсутствии связанных объектов учёта.

2.8.7 Приложения

Репозиторий приложений ведется для учёта и распространения приложений. Перечень приложений, зарегистрированных в «UEM SafeMobile», отображается в окне **«Приложения»** раздела **«Объекты учёта»** в соответствии с рисунком 2.106.

Таблица приложений содержит следующие столбцы:

- id – номер приложения в системе (по умолчанию, в таблице не отображается);
- Имя – наименование приложения;
- UID – уникальный идентификатор приложения;
- Монитор – флаг отображает является ли приложение мобильным клиентом SafeMobile или нет. Определяется системой автоматически, изменить вручную нельзя;
- Тип – тип приложения: корпоративное (приложение, для которого загружен дистрибутив) /некорпоративное (любое другое приложение);
- Версия – версия приложения;
- Код версии– код версии приложения;

- Загружено – дата загрузки приложения в систему;
- Описание – текстовое описание приложения;
- Платформа – отображает значок платформы, на которой работает приложение;
- Владелец – администратор узла ОШС, назначенный владельцем сущности.

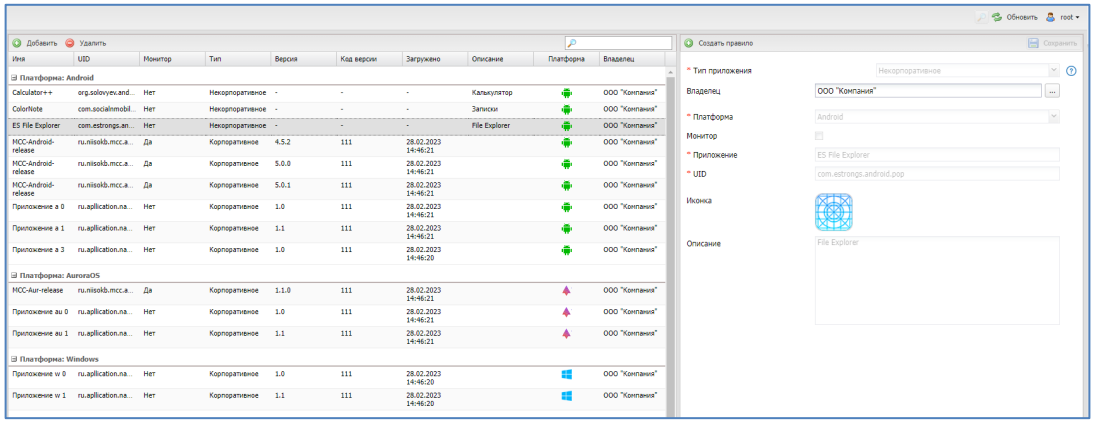


Рисунок 2.106 - Окно «Приложения»

По умолчанию, записи в реестре приложений группируются по платформам. Возможна также группировка по заданному полю. Сгруппировать по этому полю Для этого следует выбрать необходимый столбец и, при сортировке записей в раскрывающемся меню, нажать на строку в соответствии с рисунком 2.107. В этом случае записи сгруппируются по версии приложений. Для разгруппировки записей приложений необходимо в раскрывающемся меню снять флажок в строке **«Группировать»**.

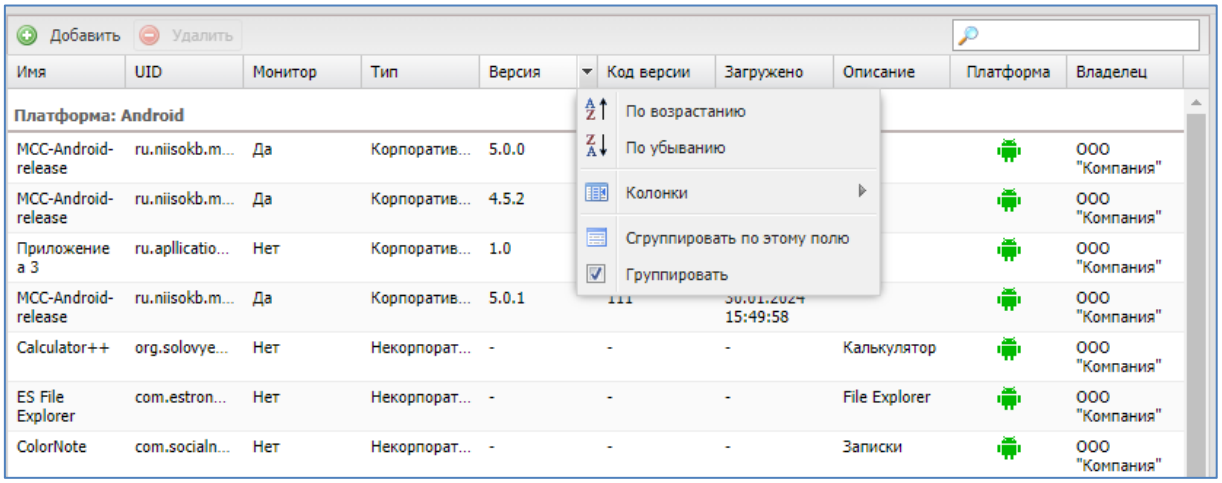


Рисунок 2.107 - Группировка приложений

2.8.7.1 Добавление записи о приложении в систему

Для добавления в систему записи о приложении используется кнопка **«Добавить»** в верхней панели инструментов окна. Затем в правой части окна (рисунок 2.108) следует выбрать **«Тип приложения»**.

Формы для корпоративных и некорпоративных приложений различны.

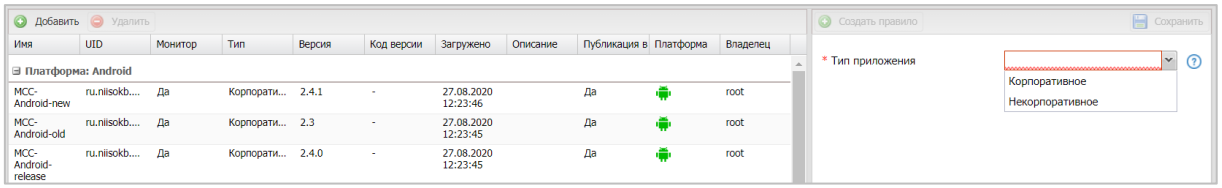


Рисунок 2.108 - Добавление приложения

2.8.7.1.1 Некорпоративное приложение

При добавлении ***некорпоративного*** приложения необходимо заполнить форму в соответствии с рисунком 2.109, содержащую перечень параметров добавляемого приложения. Поля, обозначенные * − обязательные для заполнения.

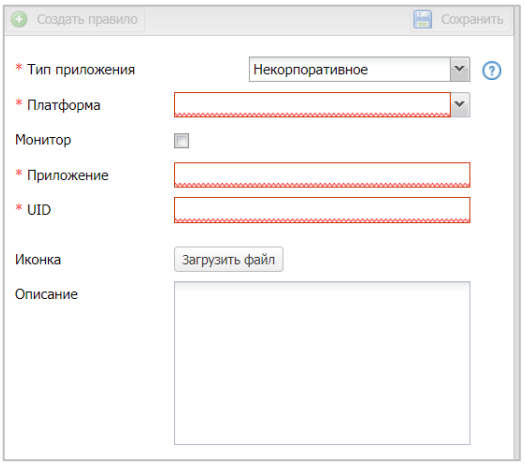


Рисунок 2.109 - Форма некорпоративного приложения

Если при заполнении формы поля не заполнились автоматически, то их нужно ввести вручную.

При добавлении приложения для МСК на платформе Android из Google Play UID приложения следует выбрать из адресной строки в соответствии с рисунком 2.110.

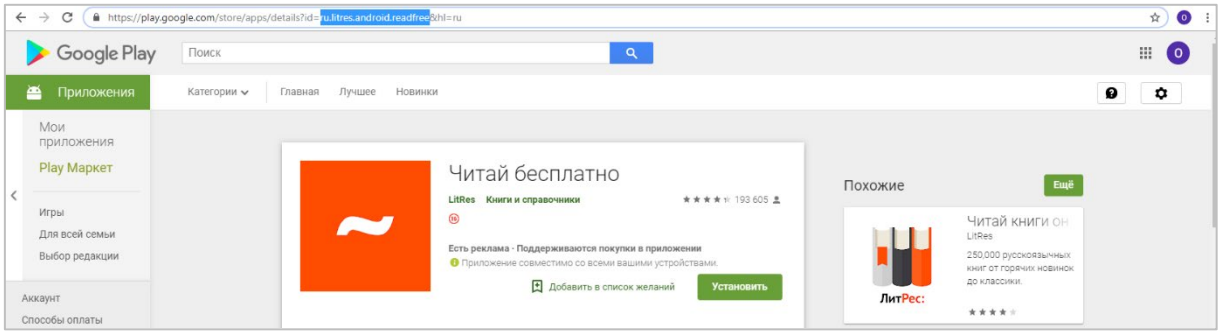


Рисунок 2.110 - Добавление приложения из Google Play

Для загрузки иконки нажать кнопку **«Загрузить файл»** и выбрать файл рисунка для приложения. Для продолжения работы нажать кнопку **«Сохранить»**.

После этого осуществляется запись в БД введенной информации, и запись о добавленном приложении воспроизведется в таблице в левой части окна. Приложение будет доступно для назначения ПУП, для этого следует нажать кнопку **«Создать правило»** и выполнить действия согласно описанию в 2.6.11.

Особенности создания записи о приложении для платформы Windows

Приложения на МСК платформы Windows загружаются в 2 этапа:

1. Необходимо подготовить файл с метаинформацией. На ПК с ОС Windows 10+ запустить **PowerShell** и выполнить команду:
   - ./msi-info.ps1 ./<приложение>.msi
   - После выполнения команды, в той же папке появится файл <приложение>.msi.meta.json.
2. Загрузить msi-файл в соответствии с описанием, приведенном в данном разделе, как Корпоративное приложение: нажать кнопку **«Загрузить файл»** и загрузить файл с метаинформацией <приложение>.msi.meta.json, затем нажать кнопку **«Сохранить»**.

Сам скрипт **msi-info.ps1** можно скачать при загрузке первого msi-приложения (появится кнопка **«Скачать скрипт»**) и использовать в дальнейшем для последующих приложений.

Примечание.

Если при первом выполнении скрипта возникает ошибка, извещающая об отсутствии у пользователя прав на выполнение ps-скриптов, необходимо один раз выполнить команду:

Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser

Если некорпоративное приложение уже было установлено на МСК пользователя, то процедура добавления записи в систему аналогична процедуре в разделе **«Приложения/Управления приложениями»** при нажатии кнопки **«Зарегистрировать»**.

2.8.7.1.2 Корпоративное приложение

При добавлении ***корпоративного*** приложения необходимо в строке **«Файл»** нажать кнопку **«Загрузить файл»**, после чего в появившемся окне выбрать файл дистрибутива приложения. Загружаемые приложения имеют следующий формат:

- для устройств на платформе **iOS** − **IPA**;
- для устройств на платформе **Android** − **APK**;
- для устройств на платформе **Windows** − **MSI** (только приложения в режиме автоматической установки)
- для устройств на платформе **Аврора** − **RPM**.
- для устройств на платформе **Linux** − **RPM**

После загрузки дистрибутива его название, версия, код версии, UID, описание определятся автоматически и отразятся в соответствующих полях формы. Если поля не были заполнены автоматически, то их нужно ввести вручную. Поля, обозначенные * − обязательные для заполнения.

Примечание.

- *Для платформ Linux и Аврора необходимо указать платформу, вручную.*
- *Для платформ Linux необходимо указать «дистибутив»*

- *Некорректное (ошибочное) заполнение поля UID приведет к воспроизведению ошибочных действий при установке приложения на МСК. Для МСК платформы Windows такие действия приведут к невозможности удаления приложения средствами SafeMobile, т.к. регистрация установки была произведена для другого UID приложения.*

Для завершения процесса создания в системе записи о приложении следует нажать кнопку **«Сохранить»**. После этого осуществляется запись в БД введенной информации и запись о добавленном корпоративном приложении воспроизведется в таблице в левой части окна. Приложение будет доступно для назначения ПУП, для этого следует нажать кнопку **«Создать правило»** и выполнить действия согласно описанию в 2.6.11.

2.8.7.2 Редактирование записи о приложении

Для приложения, выбранного в левой части окна, можно изменить в соответствии с рисунком 2.111. После нажатия кнопки **«Сохранить»** внесенные изменения сохранятся в БД.

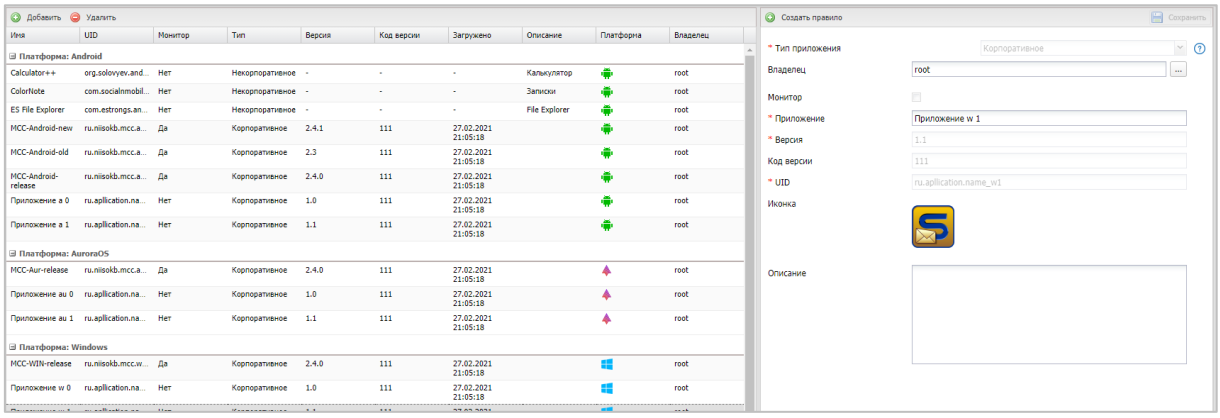


Рисунок 2.111 - Редактирование приложения

2.8.7.3 Удаление записи о приложении

Для удаления приложения необходимо выбрать в таблице соответствующую ему запись в соответствии с рисунком 2.112 и нажать кнопку **«Удалить»**.

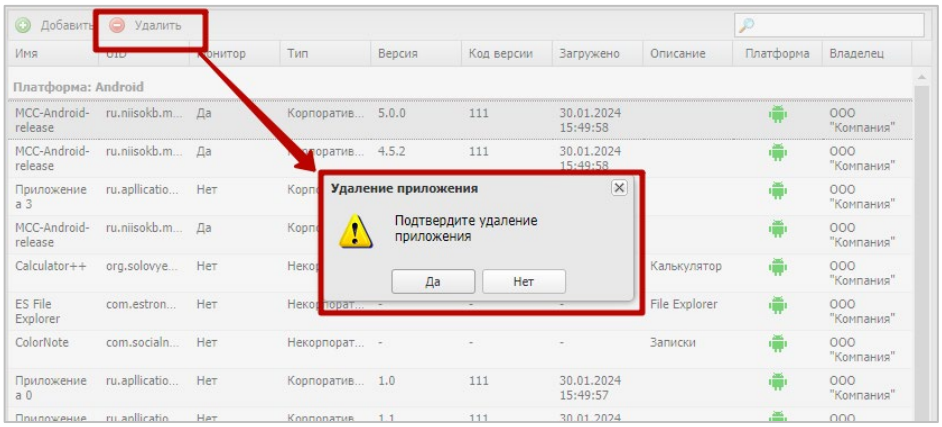


Рисунок 2.112 - Удаление приложения

После подтверждение выполняемого действия выбранная запись удалится из БД при отсутствии связанных объектов учёта.

2.8.8 SIM-карты

Окно **«SIM-карты»** предназначено для управления записями о SIM-картах, используемых на устройствах. Чтобы открыть окно, выберите пункт **«SIM-карты»** в главном меню АРМ Администратора SafeMobile в соответствии с рисунком 2.113.

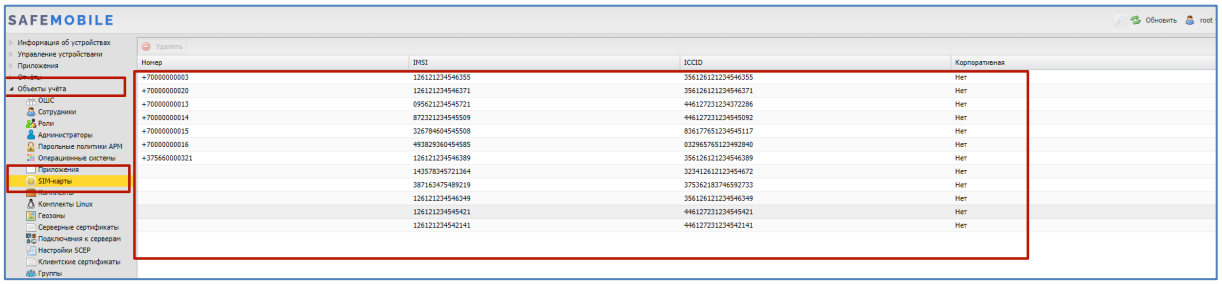


Рисунок 2.113 - Окно SIM-карты

Таблица зарегистрированных SIM-карт содержит следующие столбцы:

- id – номер SIM-карты в системе (по умолчанию, в таблице не отображается);
- Номер;
- IMSI;
- ICCID;
- Корпоративная.

SIM-карты регистрируются в системе по данным МСК, добавление их Администратором невозможно.

Администратор может назначить SIM-карте номер телефона или изменить признак её корпоративности при помощи соответствующего флажка (рисунок 2.114). Изменение полей IMSI и ICCID недоступно. После изменения параметров SIM-карты нажмите кнопку **«Сохранить»**, в результате чего изменения будут сохранены в системе.

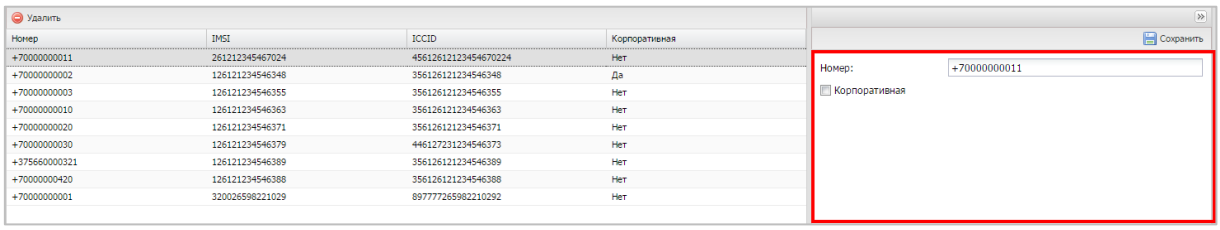


Рисунок 2.114 - Изменение записи о SIM-карте

Для удаления имеющейся SIM-карты выберите ее в таблице и нажмите кнопку **«Удалить»** (рисунок 2.115).

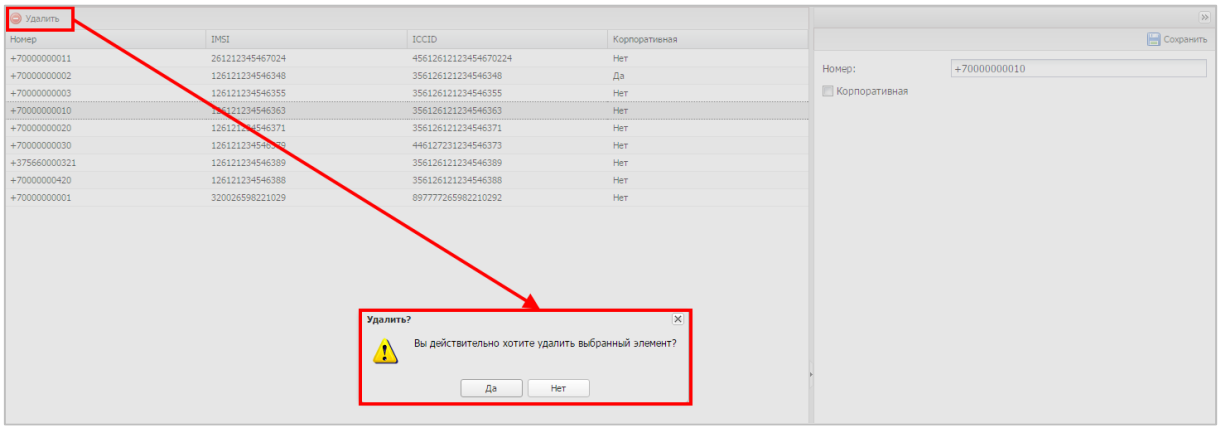


Рисунок 2.115 - Удаление записи о SIM-карте

После этого система запросит подтверждение выполняемого действия, и выбранная запись о SIM-карте удалится из базы данных при отсутствии связанных с ней объектов учёта.

Примечание.

Для Android.

Если при регистрации SIM-карты номер телефона не был определен системой автоматически, необходимо выполнить следующие действия:

1. *Применить к устройству администратора и к устройству пользователя (или ко всему дереву ОШС) профиль «Настройки монитора Android»;*
2. *Включить политику «Регистрировать SMS»;*
3. *В политике «Номер телефона для отправки SMS с параметрами SIM» указать номер администратора в формате +7XXXXXXXXXX. На телефоне администратора должен быть установлен «монитор».*

После чего на телефон администратора поступит техническое SMS с параметрами SIM-карты: ICCID и IMSI. По этим параметрам система сопоставит номер телефона отправителя смс с параметрами SIM-карт в системе, после чего номер телефона будет зарегистрирован.

2.8.9 Комплекты

Комплект является основным объектом учёта в системе. Комплект определяет абонента системы и устанавливает соответствие между SIM-картой, сотрудником и конфигурацией мобильного клиента SafeMobile. В таблице окна в соответствии с рисунком 2.116 имеются следующие столбцы:

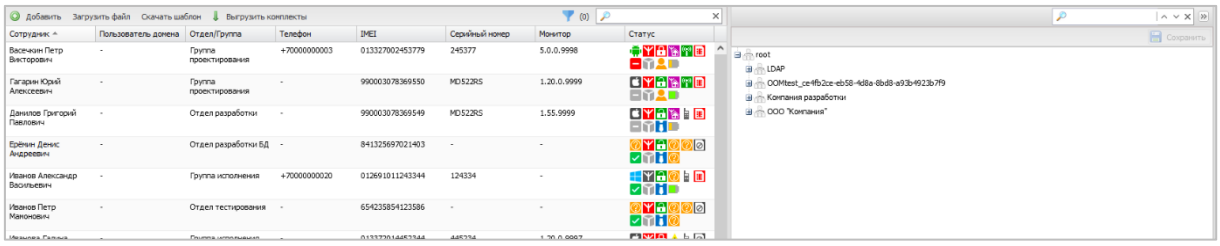


Рисунок 2.116 - Окно «Комплекты»

- Сотрудник (по умолчанию, отображается в таблице);
- Пользователь домена - Отображает ФИО сотрудника или e-mail, если ФИО не было импортировано (по умолчанию, отображается в таблице);
- Отдел/Группа (по умолчанию, отображается в таблице);
- Должность;
- SIM: Принадлежность;
- Состояние роуминга;
- IMSI;
- ICCID;
- Телефон (по умолчанию, отображается в таблице);
- id;
- Состояние блокировки;
- Управление устройством;
- Последняя активность;
- Тип соединения;
- Статус соединения;
- IP адрес;
- Тип устройства;
- Модель устройства;
- IMEI (по умолчанию, отображается в таблице);
- UDID;
- Серийный номер (по умолчанию, отображается в таблице);
- Тип контейнера;
- Заряд аккумулятора;
- Устройство: Принадлежность;
- Монитор (по умолчанию, отображается в таблице);
- Платформа;
- Версия;
- Статус (по умолчанию, отображается в таблице);
- Стратегия;
- Метки.

Перед созданием комплекта необходимо убедиться в том, что запись о сотруднике, которому планируется назначить создаваемый комплект, уже содержится в справочнике системы.

Для добавления нового комплекта используется кнопка **«Добавить»**, после нажатия которой отображается диалоговая форма в соответствии с рисунком 2.117, в которой необходимо выбрать ФИО сотрудника, которому будет назначен добавляемый комплект.

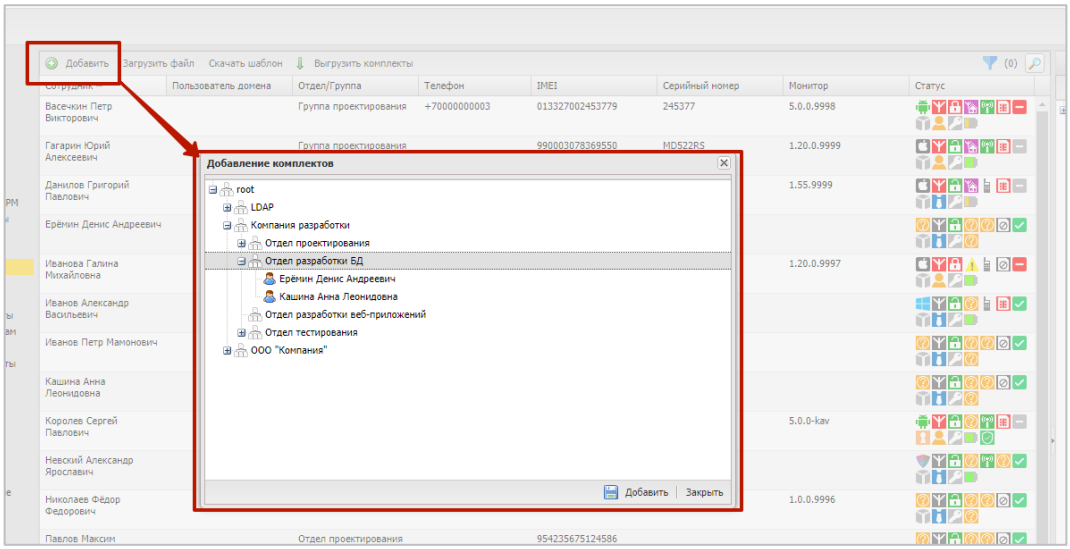


Рисунок 2.117 - Создание комплекта, вкладка «Сотрудник»

Для осуществления поиска, дополнительно к поисковой системе в главной таблице предназначена кнопка в правом верхнем углу.

В верхней панели инструментов правой части окна расположена кнопка **«Сохранить»**, при нажатии которой осуществляется сохранение конфигурации комплекта. Кнопка **«Сохранить»** становится доступной только после выбора сотрудника на вкладке **«Сотрудник»**.

Кнопка **«Загрузить файл»** предназначена для добавления комплектов сотрудников, МСК которых были зарегистрированы посредством КМЕ в соответствии с «Руководством администратора по регистрации устройств в SafeMobile с помощью КМЕ». А также для МСК, для которых известны IMEI или серийные номера и которые планируется подключать со стратегией управления «Только устройство». После нажатия кнопки открывается диалоговая форма в соответствии с (рисунок 2.118). В которой необходимо выбрать подразделение, в которое будут импортированы комплекты и файл с комплектами.

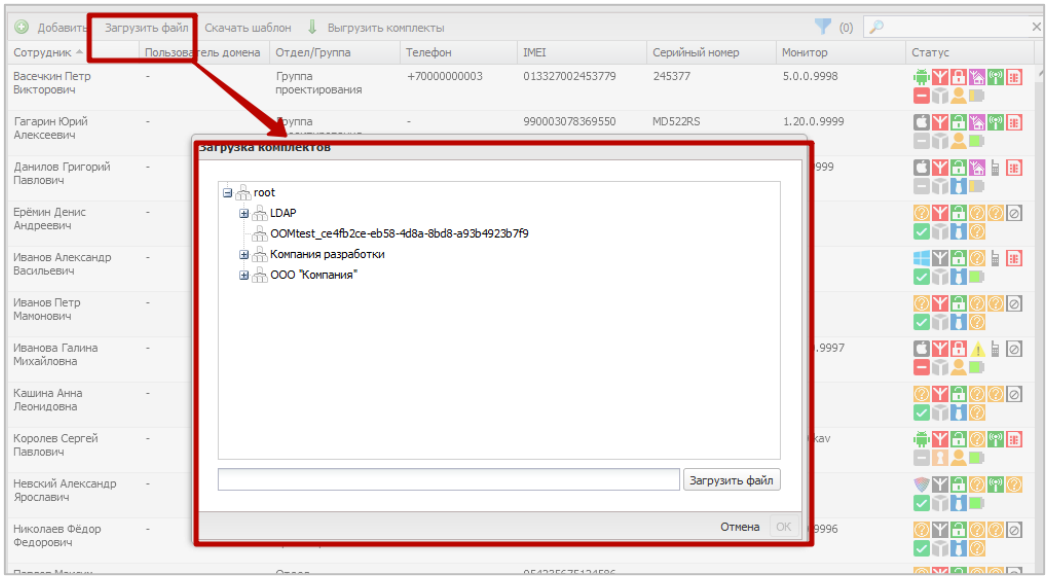


Рисунок 2.118 - Загрузка комплектов

Загружаемый файл может иметь формат CSV или XLSX. Первая строка должна содержать название колонок в следующем составе:

- IMEI;
- Serial Number;
- Фамилия;
- Имя;
- Отчество;
- Должность;
- Домен;
- Имя пользователя;
- E-mail;
- Место работы 1;
- Место работы 2;
- …
- Место работы 10.

Файлы формата CSV предназначены для загрузки данных, выгружаемых из портала Knox Mobile Enrollment корпорации Samsung. Из файла импортируются только первые две колонки IMEI/MEID и Serial Number.

Вторая и последующие строки должны содержать импортируемые данные. При импорте комплектов нужно учесть следующие ограничения:

1. В каждом комплекте должен быть заполнен «IMEI» и/или «Serial Number».
2. В каждом комплекте должны быть заполнены поля: «Фамилия», «Имя» и «Должность». Либо все поля с данными сотрудника должны быть пустыми. В этом случае данные сотрудников будут сгенерированы автоматически.
3. Поля «Место работы N» должны заполняться последовательно начиная с «Место работы 1». От родительских подразделений к дочерним. Например: «Место работы 1» - root; «Место работы 2» - Департамент разработки; «Место работы 3» - Отдел тестирования.
4. Поле «Место работы 1» должно совпадать с подразделением, которое выбрано для импорта.
5. Если поля место работы не заданы, то все комплекты будут импортированы в подразделение, выбранное при импорте.
6. Если подразделения, указанные в полях «Место работы 1-N» отсутствуют в дереве ОШС, они будут добавлены автоматически.

Для выгрузки комплектов в файле формата XLSX, следует нажать кнопку **«Выгрузить комплекты»** в соответствии с рисунком 2.119.

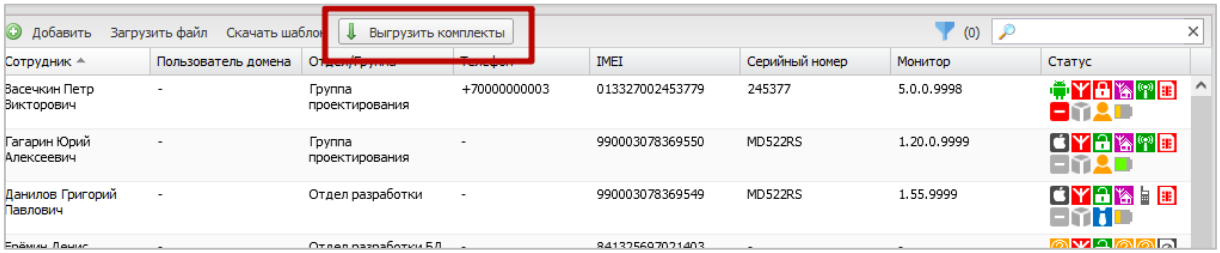


Рисунок 2.119 - Выгрузка комплектов

> ***Примечание.***
> *Выгружаемый файл можно использовать в качестве образца для загружаемого файла только если добавить второй колонкой «Serial Number».*

Для отключения комплекта от управления системой следует нажать кнопку **«Отключить»**, после чего система предоставит выбор параметра отключения в соответствии с рисунком 2.120. Затем требуется подтвердить действие, нажав на кнопку **«Применить»**.

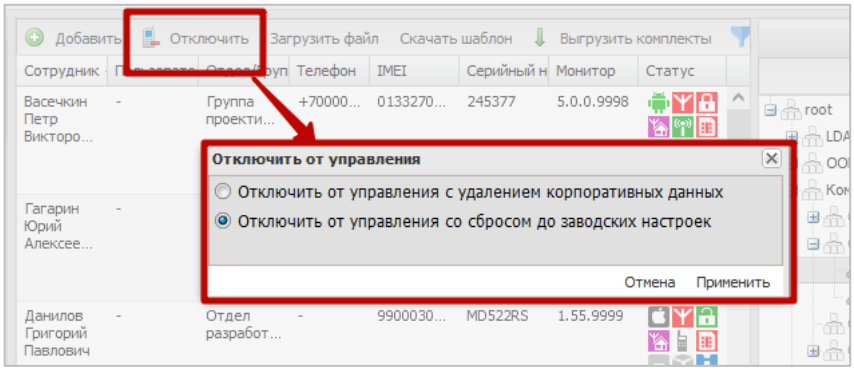


Рисунок 2.120 - Отключение комплекта от управления

После отключения от управления комплект можно будет удалить из системы. Для этого необходимо выбрать в таблице соответствующую ему запись, нажать кнопку **«Удалить»** (рисунок 2.121), после подтверждения выполняемого действия выбранная запись удалится из БД.

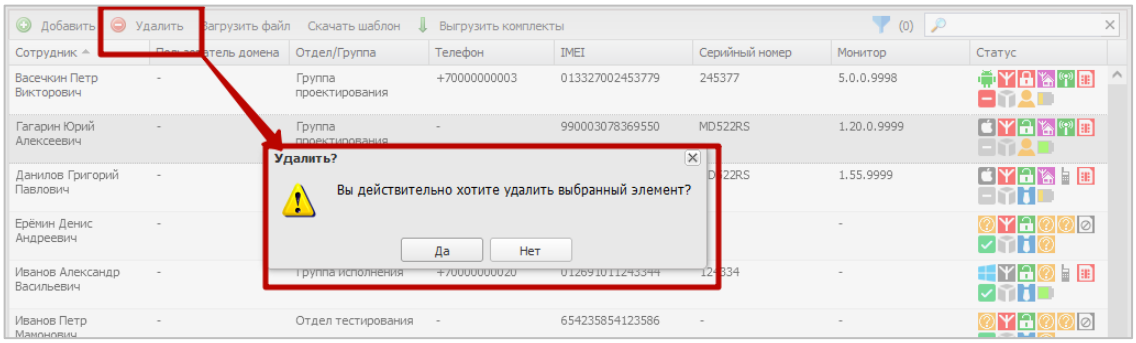


Рисунок 2.121 - Удаление комплекта

Удаление комплекта инициирует команду удаления данных с устройства. Такую операцию следует применять только в случае полного удаления пользователя из «UEM SafeMobile» (при увольнении сотрудника или утере устройства).

Примечания

1. *Для корректного повторного использования МСК в системе необходимо удалить его комплект из АРМ Администратора SafeMobile. При этом выполняется очистка МСК путем отправки на МСК команды удаления данных и возврата его к заводским настройкам.*
2. *Если очистка МСК была выполнена вручную непосредственно на устройстве (путём возврата МСК к заводским настройкам), то комплект также*

требуется удалить, используя АРМ, так как не удалённый комплект будет учитываться при лицензировании (при превышении допустимого количества таких комплектов невозможно будет подключить новые).

2.8.10 Комплекты Linux

В данном разделе задаются комплекты для устройств на платформе Linux. Страница раздела состоит из следующих блоков и элементов управления:

- Подразделение – строка отображения названия подразделения, выбранного в структуре ОШС;
- Окно выбора подразделения – представлено в виде структуры ОШС;
- Список комплектов выбранного подразделения или пользователя – отображает список комплектов для выбранного подразделении или пользователя. Информации по каждому комплекту распределена по следующим колонкам таблицы (включенным по умолчанию):
  - Отдел/группа – наименование отдела/группы в структуре ОШС к которой принадлежит пользователь;
  - Сотрудник – ФИО пользователя;
  - Пользователь домена - отображает ФИО сотрудника (или e-mail, если ФИО не было импортировано);
  - Подключение SSH – параметры подключения по SSH;
  - Статус – статус устройства.
- Кнопка «Фильтр списка» – позволяет фильтровать список комплектов в соответствии с значениями колонок.
- Параметры комплекта – отображает параметры заданного комплекта. Для каждого комплекта могут отображаться следующие параметры:
  - Строка подключения по SSH к устройству в формате URI – помимо формата ssh://user@hostname:22 допускается использовать IP адрес (например - ssh://root@10.17.7.221:22)
  - Сменить ключ – чекбокс. Если включен, то становятся доступны для редактирования поля смены ключа RSA:
    - Приватный RSA ключ SSH – поле ввода строки данных ключа;
    - Пароль RSA ключа – поле ввода пароля.
  - Кнопка «Сохранить» - сохранение изменений в настройках комплектов или сохранение данных о новом комплекте (доступна при внесении изменений или при создании нового комплекта).
- Кнопка «Добавить» - создать новый комплект,

- Кнопка «Отключить» - удаляет комплект из системы (кнопка появляется только при наведении на комплект, в блоке списка комплектов).

2.8.10.1 Добавить новый комплект Linux

Чтобы добавить новый комплект linux, необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета - Комплекты Linux»;
2. В структуре ОШС найти пользователя, для которого создается комплект;
3. Нажать кнопку «Добавить»;
4. В блоке параметров комплекта заполнить поля:
    a. Строка подключения по SSH к устройству в формате URI. Например: ssh://user@hostname:22 (обязательно для заполнения);
    b. Приватный RSA ключ SSH подключения (обязательно для заполнения);
    c. Пароль RSA ключа (опционально),
5. Нажать кнопку «Сохранить».

2.8.10.2 Удаление комплекта Linux

Чтобы удалить комплект Linux, необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета - Комплекты Linux»;
2. В структуре ОШС найти пользователя, чей комплект необходимо удалить;
3. Выделить комплект в списке комплектов;
4. Нажать кнопку «Отключить».

2.8.11 Геозоны

Пункт меню «Геозоны» предназначен для создания и управления именованными областями на географической карте, которые используются для применения на МСК заданных ограничений и настроек ОС. В разделе отображается фрагмент карты и таблица с реестром геозон в соответствии с рисунком 2.122.

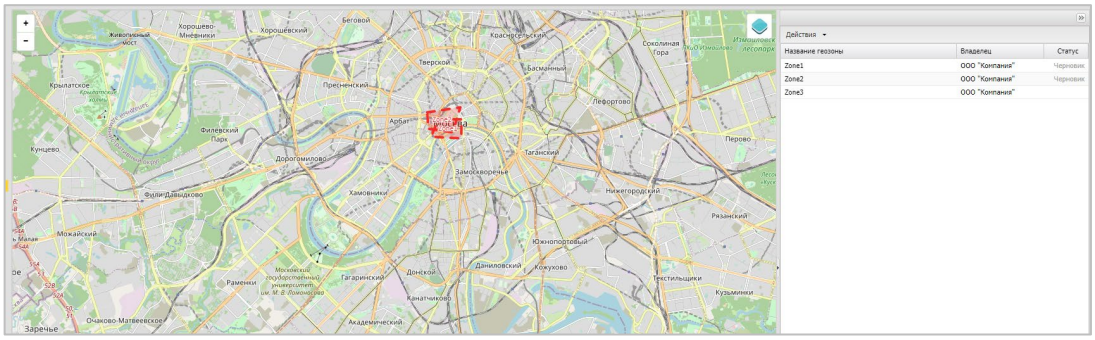


Рисунок 2.122 - Окно «Геозоны»

В правой части окна расположена таблица, в которой отображаются все созданные геозоны и их статус. В верхней части таблицы находится кнопка «Действия» при нажатии на которую выпадает меню с вариантами:

- Добавить – предназначена для создания новой геозоны;
- Удалить – предназначена для удаления уже созданной геозоны;
- Изменить – предназначена для внесения изменений в геозону только в статусе «Черновик»;
- Активировать – предназначена для активирования геозоны в системе и возможности использования ее при назначении профиля. Кнопка доступна только для геозон в статусе «Черновик».
- Сменить владельца – предназначена для смены владельца геозоны.

В левой части окна расположен фрагмент карты, на которой отображаются созданные геозоны в форме многоугольника. Контур геозоны со статусом «Черновик» воспроизводится в виде пунктирной линии, а контур активированной геозоны − в виде сплошной линии.

Для изменения масштаба карты (увеличения или уменьшения изображения) используется шкала масштабирования, расположенная в верхнем левом углу карты. Кроме того, масштаб изображения можно изменять, используя вращение колеса мыши, если курсор расположен в области карты.

При нажатии на значок в правой верхней части карты раскрывается меню настройки источника картографической информации (сервер ГИС), который используется для отображения карты: openstreetmap.org (рисунок 2.123).

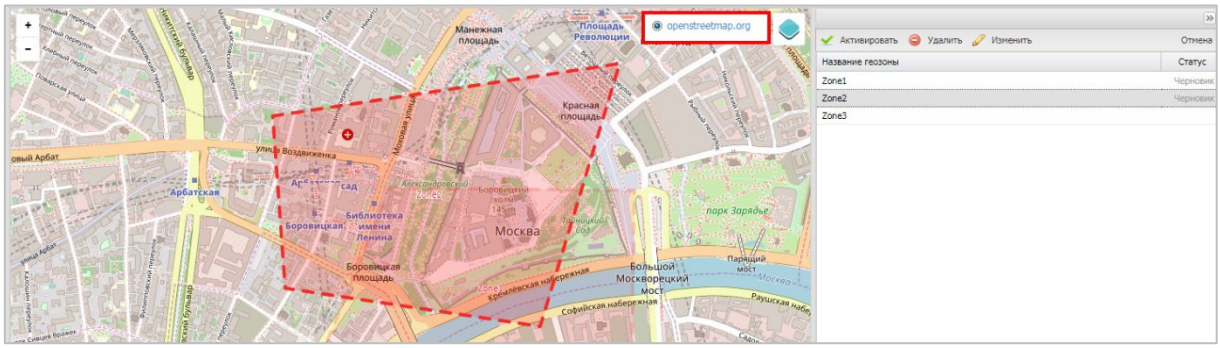


Рисунок 2.123 - Настройка режима отображения информации о геозонах на карте

Для *создания* геозоны следует нажать на кнопку «Действия», выбрать **«Добавить»** и, посредством мыши, нарисовать на выбранном участке карты необходимую область, повторный щелчок мыши завершит рисование. Для сохранения рисунка геозоны нажать на кнопку **«Сохранить черновик»**, затем в всплывающем окне в соответствии с рисунком 2.124 ввести имя новой геозоны, которое должно отличаться от уже созданных, и нажать **«ОК»**. Созданная геозона отобразится в реестре со статусом «Черновик».

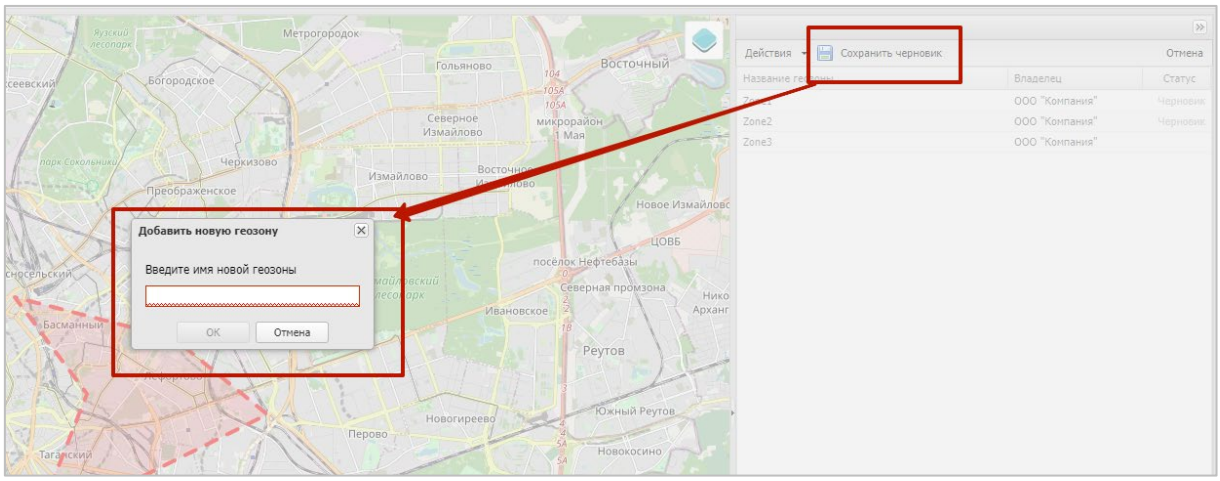


Рисунок 2.124 - Добавление геозоны

Для редактирования следует в реестре выбрать требуемую строку с названием геозоны и статусом «Черновик» и нажать кнопку «Действия», выбрать **«Изменить»**. Затем внести изменения в рисунок на карте, нажать кнопку **«Сохранить черновик»** и подтвердить название, нажав на кнопку **«ОК»**.

Для активирования геозоны необходимо в реестре выбрать требуемую строку с названием геозоны и статусом «Черновик» и нажать кнопку «Действия», выбрать **«Активировать»**. Активированная геозона в реестре отобразится без статуса и будет доступна в условиях применения профиля. После активирования геозоны ее редактирование будет **невозможно**.

Примечание.

По отношению к активным геозонам доступны только два вида действий:

- *Удаление;*
- *Смена владельца.*

Для смены владельца геозоны необходимо в реестре выбрать требуемую строку с названием геозоны, нажать кнопку «действия», выбрать «Смена владельца», после чего откроется окно структуры ОШС. Выбрать владельца геозоны в структуре ОШС, нажать кнопку «Ок».

Для удаления геозоны требуется в реестре выбрать строку с ее названием и нажать кнопку «Действия», выбрать **«Удалить»**. После подтверждения действия геозона будет удалена из реестра. Если геозона активирована и является условием применения профиля, то при выборе **«Удалить»** воспроизведется предупреждение о невозможности ее удаления. Удаление возможно только для несвязанных геозон.

Для отмены действий следует нажать кнопку **«Нет»**.

2.8.12 Серверные сертификаты

Пункт меню **«Серверные сертификаты»** предназначен для учёта и распространения серверных сертификатов на МСК. Мобильные клиенты системы используют серверные сертификаты для аутентификации серверов системы. В разделе отображается таблица с перечнем сертификатов в соответствии с рисунком 2.125.

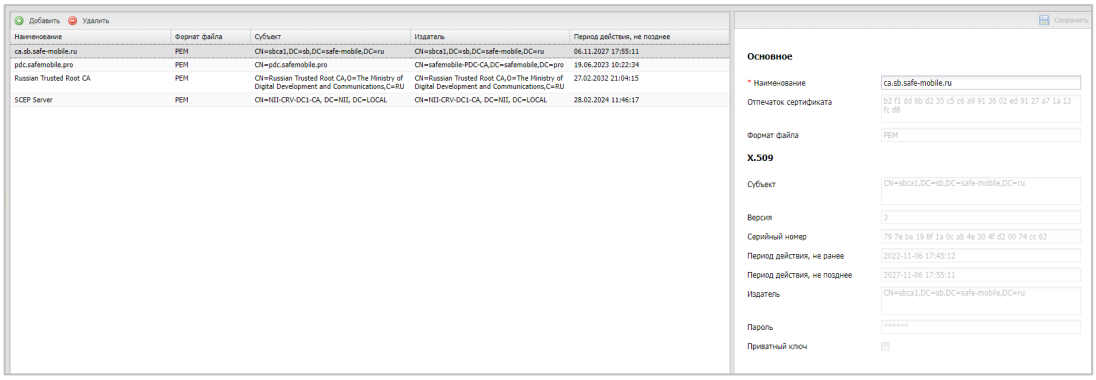


Рисунок 2.125 - Окно «Серверные сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование – наименование сертификата (по умолчанию, отображается в таблице);
- Отпечаток сертификата – хэш сертификата, вычисляемый по всем данным сертификата и его подпись;
- Формат файла – формат файла сертификата (по умолчанию, отображается в таблице);
- Субъект – информация о владельце сертификата (по умолчанию, отображается в таблице);
- Версия – версия сертификата;
- Серийный номер – серийный номер сертификата;
- Издатель – информация об издателе сертификата (по умолчанию, отображается в таблице);
- Период действия, не ранее – дата начала действия сертификата;
- Период действия, не позднее – дата окончания действия сертификата (по умолчанию, отображается в таблице);
- Приватный ключ – (Да/Нет).
- Владелец – подразделение, владеющее сертификатом.

Для *добавления* нового серверного сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна (рисунок 2.126).

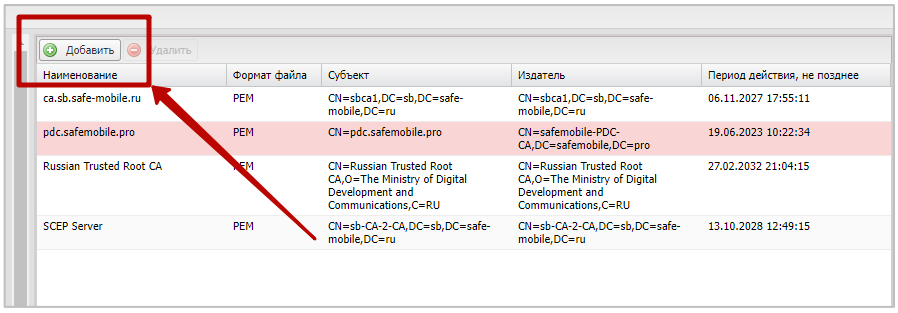


Рисунок 2.126 - Кнопка «Добавить» новый серверный сертификат

Затем в форме правой части окна ввести пароль (при необходимости) и загрузить файл, полученные от администратора системы. После загрузки файла отобразится форма с параметрами загруженного сертификата в соответствии с рисунком 2.127.

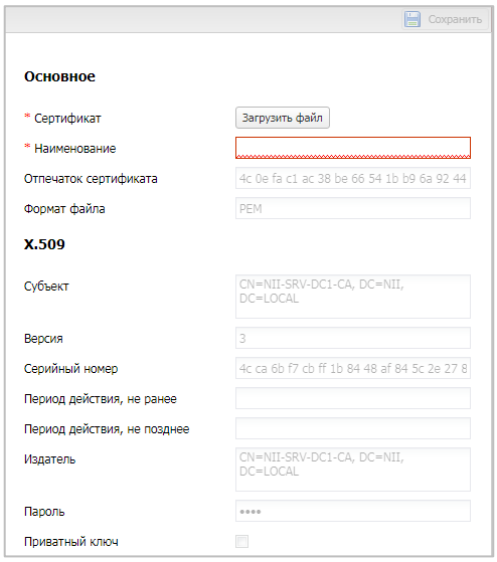


Рисунок 2.127 - Форма «Серверный сертификат»

Поле, обозначенное * – обязательное для заполнения. После заполнения формы нажать кнопку **«Сохранить»** и серверный сертификат отобразится в таблице с сертификатами.

Для *удаления* серверного сертификата необходимо выбрать в таблице (рисунок 2.128) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

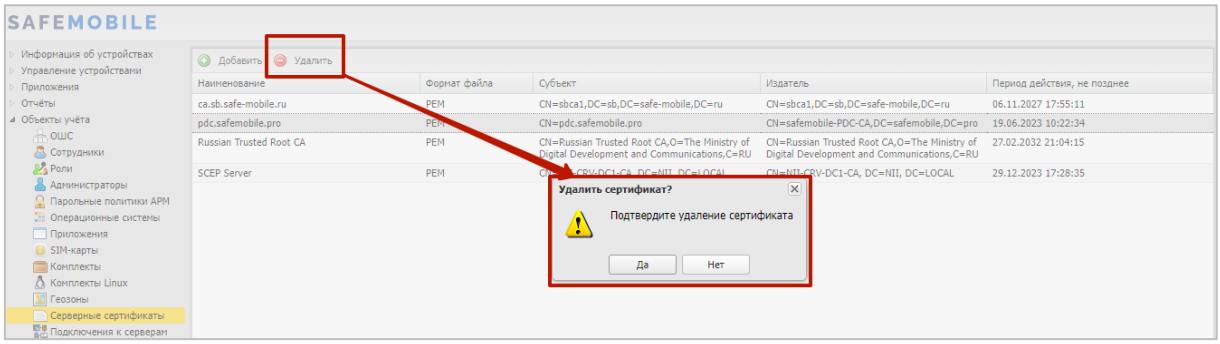


Рисунок 2.128 - Удаление серверного сертификата

2.8.13 Подключения к серверам

Пункт меню **«Подключения к серверам»** предназначен для настройки подключения МСК к серверам системы. Подключение МСК к серверам системы осуществляется по протоколу TLS. Серверный сертификат, указанный в настройках подключения будет использоваться МСК для аутентификации сервера. Если сервер использует сертификат TLS, выпущенный публичным центром сертификации, то указывать сертификат в настройках подключения не требуется.

Перед подключением первого МСК к системе должны быть выполнены следующие настройки:

Настройка подключения к **MDMServer** - обязательна. MDMServer выполняет следующие функции:

- Авторизации пользователя при регистрации МСК.
- Отправка политик, приложений и конфигураций приложений (за исключением МСК на платформе Windows).
- Отправка команд (за исключением МСК Android).

Настройка подключения к серверу команд **SocketServer**. Сервер отвечает за отправку команд на МСК Android.

- Если управление МСК на платформе Android не планируется, настраивать подключение не требуется.

Настройка подключений к **WinMDM Enrollment** и **WinMDM Management** необходима при использовании МСК Windows.

- Если управление МСК на платформе Windows не планируется, настраивать данное подключение не требуется.
- Для упрощения регистрации МСК (пользователь введет свой e-mail вместо URL сервера) необходимо: в DNS зоне предприятия зарегистрировать имя сервера WinMDM Enrollment вида enterpriseenrollment.<company.ru>. Имя enterpriseenrollment зарезервировано и используется встроенным клиентом Windows при поиске сервиса регистрации устройства.
- Если сертификаты серверов WinMDM Enrollment и WinMDM Management выпущены непубличным центром сертификации, то сертификат выпустившего их центра сертификации должен быть предварительно размещен на МСК, в хранилище: Компьютер -> Доверенные центры сертификации.
- URL, которые необходимо указать для серверов WinMDM Enrollment и WinMDM Management зависят от следующих факторов:
    - выбрана ли при инсталляции системы установка WinMDM за внешний прокси сервер;
    - MDMServer и сервера WinMDM Enrollment и WinMDM Management размещены на одной машине или нет;
    - возможно ли добавить доменное имя третьего уровня в корпоративный DNS.

Значения URL в зависимости от этих факторов приведены в таблице **2.6**.

Настройка подключения к **SCEPServer** обязательна. Подключение к серверу SCEP необходимо для получения устройствами на платформах iOS и Android сертификатов mTLS. Сертификаты mTLS используются для авторизации устройств при подключении к серверу управления и серверу команд. Помимо mTLS настройка необходима при использовании доменной авторизации по клиентским сертификатам в приложениях.

Доменные имена в русской локализации ***не поддерживаются***.

В разделе отображается таблица с перечнем серверов и подключенных к ним серверных сертификатов в соответствии с рисунком 2.129.

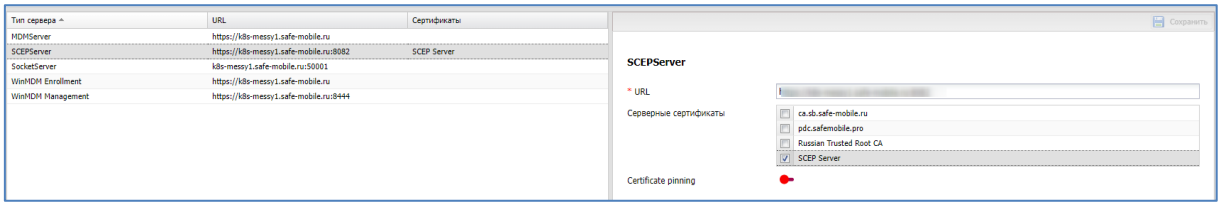


Рисунок 2.129 - Окно «Подключение к серверам»

Таблица подключения к серверам, по умолчанию, содержит столбцы:

- Тип сервера – наименование сервера системы (по умолчанию, отображается в таблице);
- URL – электронный адрес (по умолчанию, отображается в таблице);
- Сертификат – наименование серверного сертификата (по умолчанию, отображается в таблице);
- Certificate pinning – закрепление сертификата. Доступно только для:
  - MDM-сервер,
  - SCEP-сервер,
  - Socket-сервер для Android.

Примечание

Certificate pinning - подход, при котором доверенными УЦ (и их сертификатами соответственно) считаются не встроенные УЦ, а явно переданный список УЦ с цепочкой сертификатов. В таком случае доверенным сертификатом будет считаться тот и только тот сертификат, который содержится в переданном списке сертификатов.

ВАЖНО!

Подключение данной функции может привести к потере контроля над всеми устройствами.

Таблица 2.6 – Подключение к серверам

Внешний прокси	Правила на внешней прокси	Размещение	Встроенный nginx	Сервер	Регистрация в DNS	Настройка подключения
-	-	MDM и WinMDM на одной машине	example.com [x.x.x.1]	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
				WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.1	enterpriseenrollment.example.com:443
				WinMDM Management		enterpriseenrollment.example.com:8444
-	-	MDM и WinMDM на разных машинах	example.com [x.x.x.1]	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
			example.com [x.x.x.2]	WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.2	enterpriseenrollment.example.com:443
				WinMDM Management		enterpriseenrollment.example.com:8444
-	-	MDM и WinMDM на одной машине	example.com [x.x.x.1]	MDMServer	-	example.com:443
				WinMDM Enrollment		example.com:443
				WinMDM Management		example.com:8444
-	-	MDM и WinMDM на разных машинах	example.com [x.x.x.1]	MDMServer	-	example.com:443
			example1.com [x.x.x.2]	WinMDM Enrollment	-	example1.com:443
				WinMDM Management		example1.com:8444
example.com [x.x.x.1]	mdm.example.com:443 -> y.y.y.1:443	MDM и WinMDM на одной машине	y.y.y.1:443	MDMServer	mdm.example.com -> y.y.y.1	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> y.y.y.1:443		y.y.y.1:443	WinMDM Enrollment		enterpriseenrollment.example.com:443

Внешний прокси	Правила на внешней прокси	Размещение	Встроенный nginx	Сервер	Регистрация в DNS	Настройка подключения
	winmdm.example.com:p3 -> y.y.y.1:8444		y.y.y.1:8444	WinMDM Management	enterpriseenrollment.example.com ->y.y.y.1	enterpriseenrollment.example.com:8444
example.com [x.x.x.1]	mdm.example.com:443 -> y.y.y.1:443	MDM и WinMDM на разных машинах	y.y.y.1:443	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> y.y.y.1:443		y.y.y.2:443	WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.2	enterpriseenrollment.example.com:443
	enterpriseenrollment.example.com:8444 -> y.y.y.1:8444		y.y.y.2:8444	WinMDM Management		enterpriseenrollment.example.com:8444
example.com [x.x.x.1]	example.com:443 -> y.y.y.1:443	MDM и WinMDM на одной машине	y.y.y.1:443	MDMServer	-	example.com:443
	example.com:443 -> y.y.y.1:443		y.y.y.1:443	WinMDM Enrollment		example.com:443
	example.com:p3 -> y.y.y.1:8444		y.y.y.1:8444	WinMDM Management		example.com:p3
example.com [x.x.x.1]	mdm.example.com:443 -> y.y.y.1:443	MDM и WinMDM на разных машинах	y.y.y.1:443	MDMServer	-	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> y.y.y.2:443		y.y.y.2:443	WinMDM Enrollment	-	enterpriseenrollment.example.com:443
	enterpriseenrollment.example.com:8444 -> y.y.y.2:8444		y.y.y.2:8444	WinMDM Management		enterpriseenrollment.example.com:8444

Для настройки подключения МСК к серверу необходимо выполнить следующие действия:

1. В списке серверов выбрать сервер,
2. В форме правой части окна: ввести URL и установить флажок у тех серверных сертификатов, по которым МСК сможет аутентифицировать данный сервер (рисунок 2.130). В любой момент времени сервер использует только один сертификат.

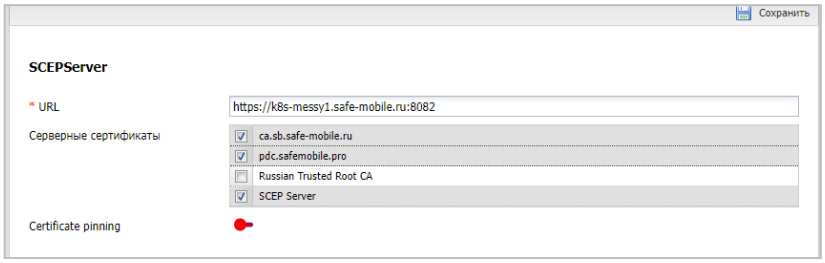


Рисунок 2.130 - Форма «Подключения к серверу»

3. Включить Certificate pinning для отмеченных серверных сертификатов (опционально).
   - При включении опции появится диалоговое окно предупреждения. Нажмите «ДА».

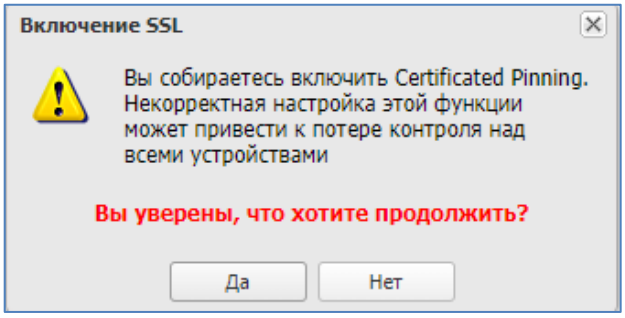


Рисунок 2.130а – предупреждение о возможных последствиях

4. После заполнения формы нажать кнопку **«Сохранить»** и подключение отобразится в реестре.

Если Certificate pinning уже включен, и требуется добавить другие сертификаты, то следует отметить необходимые сертификаты и нажать «Сохранить».

До того момента как истечет время действия текущего сертификата, необходимо выписать новый серверный сертификат и распространить его на МСК. Для этого

нужно новый сертификат добавить в список серверных сертификатов раздел 2.8.11, после чего включить его в список сертификатов, аутентифицирующих данный сервер.

2.8.14 Настройки SCEP

Раздел **«Настройки SCEP»** предназначен для учёта и распространения клиентских сертификатов с настраиваемыми параметрами посредством SCEP в соответствии с рисунком 2.131.

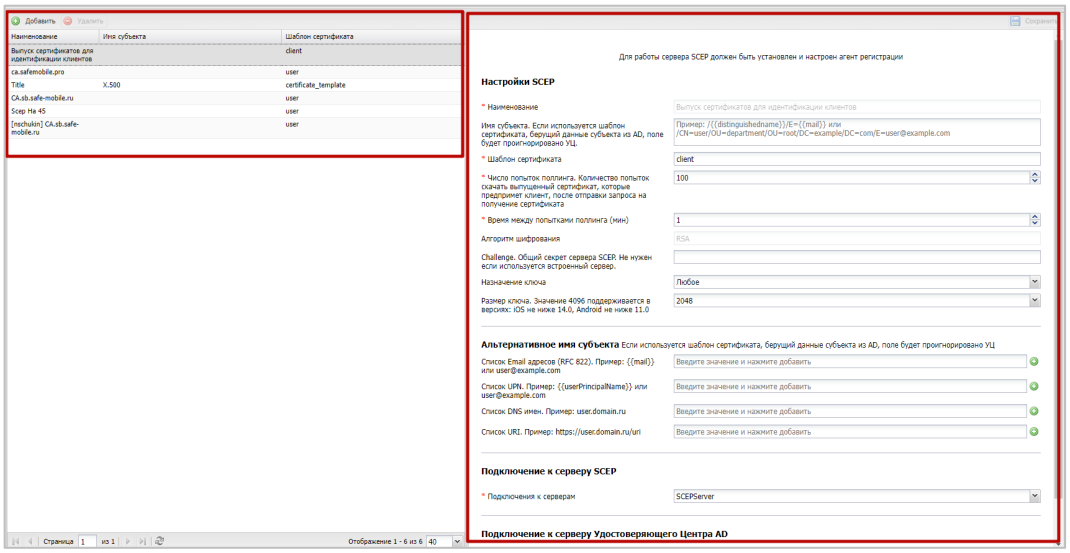


Рисунок 2.131 - Окно «Настройки SCEP»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование – наименование сертификата (по умолчанию, отображается в таблице);
- Имя субъекта – формат сертификата (по умолчанию, отображается в таблице);
- Шаблон сертификата – шаблон используемого сертификата (по умолчанию, отображается в таблице).

В правой части рабочего экрана отображаются настройки, выбранной в таблице настройки SCEP и состоят из следующих полей данных:

- **Настройки SCEP:**
  - **Наименование** – наименование настройки;
  - **Имя субъекта. Если используется шаблон сертификата, берущий данные субъекта из AD, поле будет проигнорировано УЦ** - Это отличительное имя (DN), содержащее идентифицирующую информацию об объекте, которому выдан сертификат. Имя субъекта может быть создано из стандартных компонентов каталога LDAP, таких как общие имена и организационные подразделения. Эти компоненты определены в X.500. Поле не заполняется, если данные пользователя берутся из AD (см. примечание).

    Пример:

    /CN=user/OU=department/OU=root/DC=example/DC=com/E=user@example.com.

    В имени субъекта могут быть использованы следующие подстановки:

    1. /{{distinguishedname}} - специальная подстановка (начинается с "/"), которую нужно использовать чтобы подставить полное имя пользователя.
    2. {{mail}} - подстановка адреса электронной почты.

    Пример использования подстановок:

    /{{distinguishedname}}/E={{mail}};
  - **Шаблон сертификата** – шаблон сертификата, по которому будут выпускаться сертификаты для устройств (должен быть заранее создать в AD);
  - **Число попыток поллинга. Количество попыток скачать выпущенный сертификат, которые предпримет клиент, после отправки запроса на получение сертификата.** В зависимости от настроек, УЦ может выписывать сертификат не сразу, а после подтверждения администратором УЦ;
  - **Время между попытками поллинга (мин)** - интервал времени между обращениями монитора за готовым сертификатом;
  - **Алгоритм шифрования** – RSA (всегда);
  - **Challenge. Общий секрет сервера SCEP. Не нужен если используется встроенный сервер**;
  - **Назначение ключа** – доступны значения:
    - Шифрование, Подпись, Любое;
  - **Размер ключа. Значение 4096 поддерживается в версиях: iOS не**

ниже 14.0, Android не ниже 11.0;

- **Альтернативное имя субъекта:**
  - **Список Email адресов (RFC 822). Пример: {{mail}} или user@example.com**– один и более email адресов (не заполняется, если данные пользователя берутся из AD (см. примечание);
  - **Список UPN. Пример: {{userPrincipalName}} или user@example.com**– один и более UserPrincipalName (не заполняется, если данные пользователя берутся из AD (см. примечание);
  - **Список DNS имен. Пример: user.domain.ru**– один и более DNS (не заполняется, если данные пользователя берутся из AD (см. примечание);
  - **Список URI. Пример: https://user.domain.ru/uri** – один и более Uniform Resource Identifier (не заполняется, если данные пользователя берутся из AD (см. примечание));

- **Подключение к серверу SCEP:**
  - Подключения к серверам – выбор из списка серверов SCEP;

- **Подключение к серверу Удостоверяющего Центр AD:**
  - URL корпоративного УЦ – адрес расположения корпоративного УЦ;
  - Период запросов к УЦ (мин) – задается в минутах.

Примечание.

- *В свойствах «шаблона сертификата» в УЦ должен быть указан источник данных пользователя: AD или запрос сертификата. Если в шаблоне указано, что брать данные следует из AD, то все, что введено в полях SN и SAN игнорируется и берется из AD. Если же указано брать из запроса сертификата, то нужно, чтобы в запросе было заполнено хотя бы одно из полей: SN или SAN иначе УЦ вернет ошибку создания сертификата.*
- *В поле «Имя субъекта» и полях блока «Альтернативное имя субъекта» допускается использование всех подстановок, указанных в «Руководстве администратора» 2.6.8.2 Настройка параметров профиля.*

2.8.14.1 Добавление новой настройки SCEP

Чтобы добавить новые настройки SCEP, необходимо выполнить следующие действия.

1. Перейти в раздел «Настройки SCEP».

2. Нажать кнопку **«Добавить»** в панели инструментов верхней части окна. Затем заполнить форму в правой части окна 2.132.

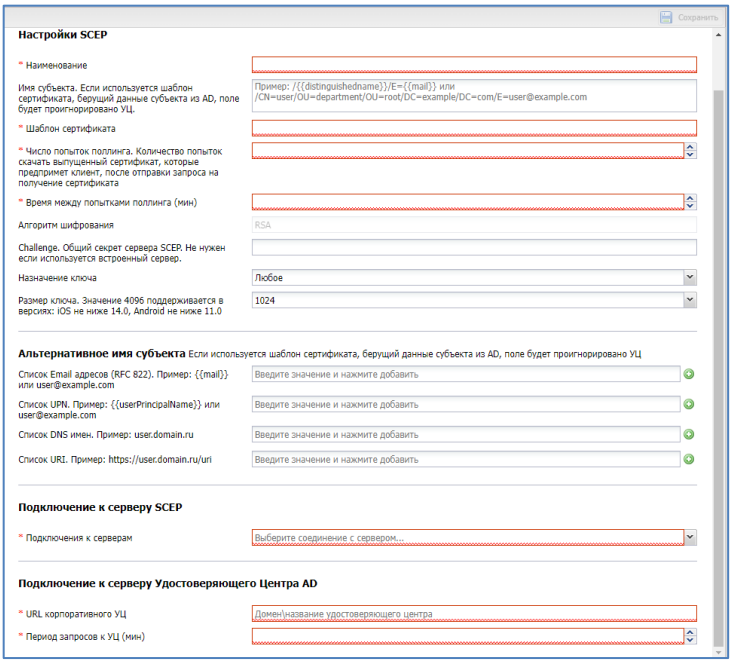


Рисунок 2.132 - Форма с настройками SCEP

После заполнения формы нажать кнопку **«Сохранить»** и новые настройки SCEP отобразится в таблице.

2.8.14.2 Удаление настроек SCEP

Для удаления настроек SCEP необходимо выбрать в таблице (рисунок 2.133) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удалится из перечня настроек SCEP (при отсутствии связанных профилей).

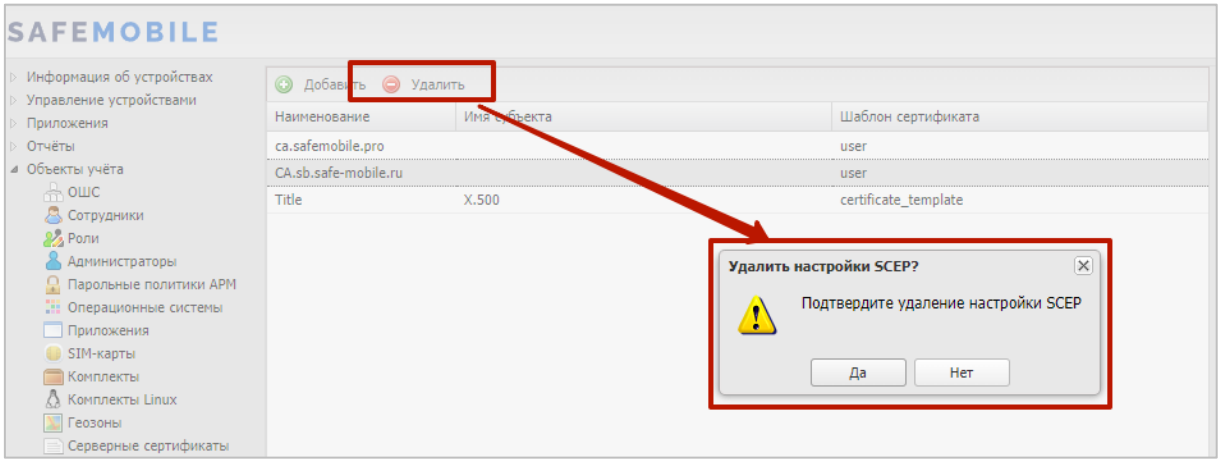


Рисунок 2.133 - Кнопка удаления настроек SCEP

2.8.15 Клиентские сертификаты

Пункт меню «Клиентские сертификаты» предназначен для учёта и распространения клиентских сертификатов, которые используются для:

- аутентификации устройства при подключении к системе с использованием протокола mTLS. Сертификаты mTLS выписываются встроенным в систему УЦ. По умолчанию имеют срок действия – 182 дня. Срок может изменен в файле конфигурации УЦ. Сертификаты обновляются автоматически, когда до истечения срока действия остается менее 10% времени. Если устройство не сможет обновить сертификат до истечения срока действия, то управление им будет потеряно, т.к. сервер не сможет аутентифицировать устройство;
- аутентификации сотрудника, при подключении к корпоративной сети WiFi;
- аутентификации сотрудника в VPN;
- аутентификации сотрудника на сервере Exchange.

В верхней части окна раздела в соответствии с рисунком 2.134 отображается таблица с перечнем сертификатов, а нижней части окна располагается главная таблица

с комплектами МСК сотрудников, для которых эти сертификаты предназначены. Описание главной таблицы с комплектами приведено в разделе 2.4.

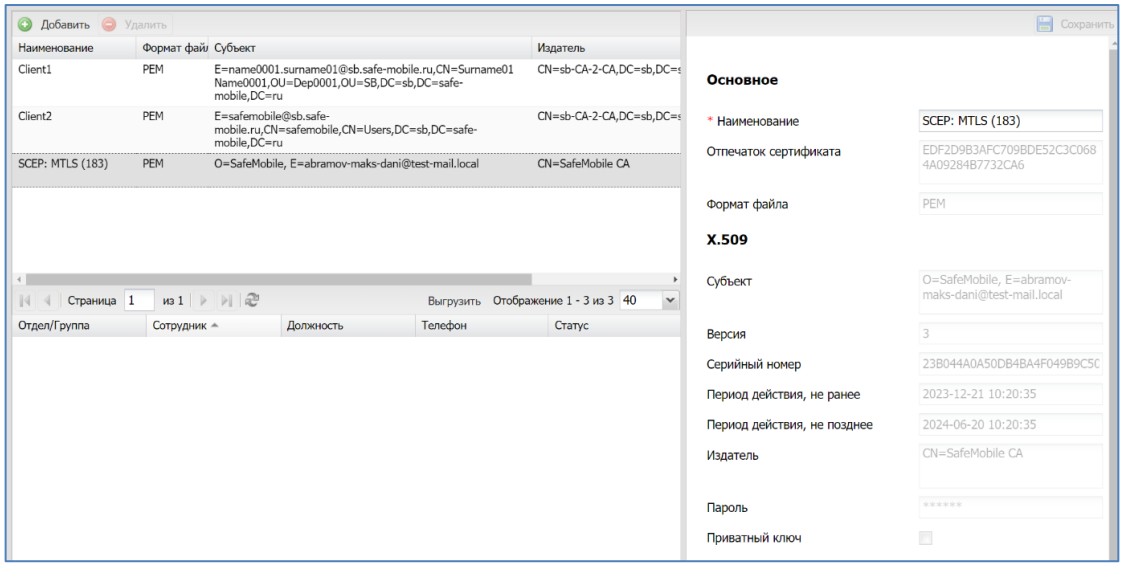


Рисунок 2.134 - Окно «Клиентские сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование – наименование сертификата (по умолчанию, отображается в таблице). У сертификатов, сгенерированных автоматически, в наименование добавляется назначение сертификата и идентификатор устройства;
- Отпечаток сертификата – информация о файле сертификата в формате base64;
- Формат файла – формат файла сертификата: X.509 для сертификата без закрытого ключа, PKCS12 для сертификата с закрытым ключом (по умолчанию, отображается в таблице);
- Субъект – информация о владельце сертификата (по умолчанию, отображается в таблице);
- Версия – версия сертификата;
- Серийный номер – серийный номер сертификата;
- Издатель – информация об издателе сертификата (по умолчанию, отображается в таблице);
- Период действия, не ранее – дата начала действия сертификата;
- Период действия, не позднее – дата окончания действия сертификата (по умолчанию, отображается в таблице);
- Приватный ключ – (Да/Нет);
- Владелец – администратор узла ОШС, назначенный владельцем сущности.

Для *добавления* нового клиентского сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна (рисунок 2.127). Затем в форме в правой части окна ввести пароль от файла сертификата и загрузить файл сертификата в формате PKCS12, полученные от администратора удостоверяющего центра AD.

> ***Примечание.***
>
> *Формат PKCS12 предназначен передачи и/или хранения закрытого ключа и цепочки доверия сертификата.*

После загрузки файла отобразится форма с параметрами загруженного сертификата в соответствии с рисунком 2.134.

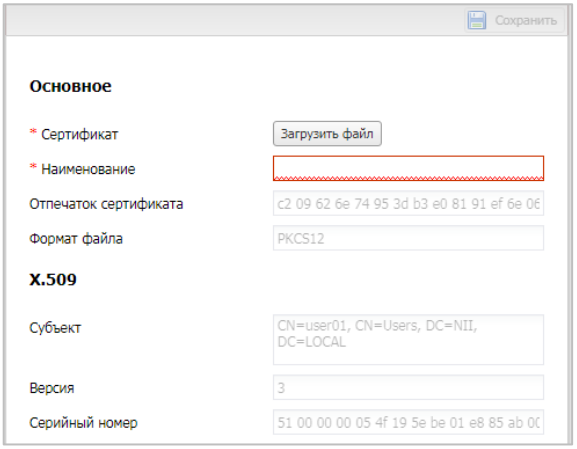


Рисунок 2.135 - Форма «Клиентский сертификат»

Поле, обозначенное * − обязательное для заполнения. После заполнения формы нажать кнопку **«Сохранить»**.

Клиентский сертификат отобразится в таблице с сертификатами, а в главной таблице отобразятся комплекты МСК, которым данный сертификат назначен.

Для *удаления* клиентского сертификата необходимо выбрать в таблице соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

Примечание.

Удаление доступно только для сертификатов, загруженных администратором вручную. Сертификаты, выписанные автоматически, через SCEP сервер – удалить нельзя.

2.8.16 Группы

В разделе отображается список групп сотрудников (рисунок 2.136). Назначение групп – использование в качестве фильтров во вкладке «условия» при применении профилей, конфигураций приложений, правил управления приложениями, правил несоответствия. Состав групп формируется автоматически, в результате синхронизации внешнего каталога и может быть изменен администратором только изменением правил синхронизации групп.

В центральной рабочей области экрана отображается список групп, где каждая строка запись об одной группе и содержит следующую информацию, упорядоченную по столбцам (отображаются по умолчанию):

- **DN/Наименование** - Для импортированной групп **distinguishedName**. Для локальной - наименование группы;
- **Тип** – тип группы (импортированная или локальная);
- **Владелец** – название подключения к внешнему каталогу, из которого была импортирована группа;
- **ObjectGUID** - Идентификатор группы в AD;
- **Синхронизация** - Дата и время последней успешной синхронизации в формате DD.MM.YY hh:mm:ss.

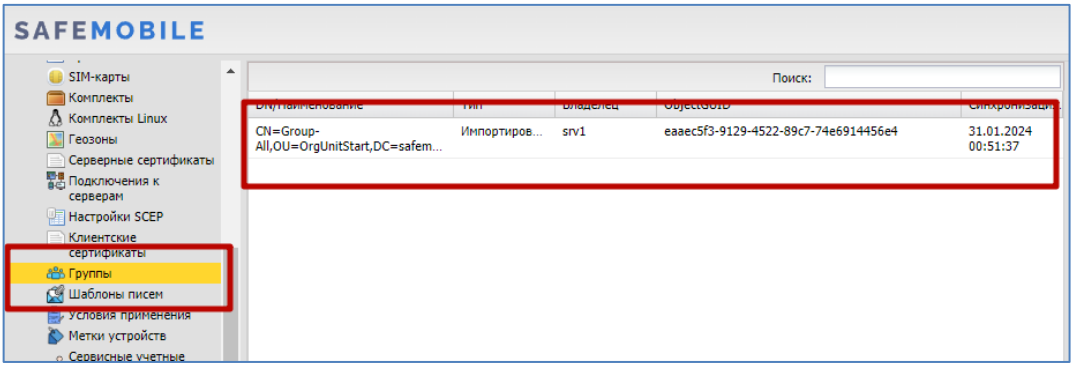


Рисунок 2.136 - Список групп

В правой части рабочей области отображается блок с настройками и информацией о выделенной в списке группе. Блок содержит следующие вкладки:

- Общие – сводные данные по группе:
  - DN/Наименование группы,
  - Тип,
  - ObjectGUID,
  - Последняя синхронизация.
- Члены группы – список сотрудников, входящих в группу. Каждая строка списка содержит информацию об одном сотруднике и упорядочена по следующим столбцам (отображаются по умолчанию):
  - ФИО – Фамили, имя и отчество,
  - Должность – должность сотрудника,
  - DN пользователя – DN пользователя в внешнем каталоге,
  - ObjectGUID – индификатор пользователя в AD.
- Владелец – отображается владелец группы в ОШС:
  - Для импортированных групп владельцем становится корневой импортированный узел.

2.8.17 Шаблоны писем

Раздел содержит список шаблонов писем для автоматической рассылки e-mail сообщений системой. Шаблоны писем применяются при создании правил несоответствия (рисунок 2.137).

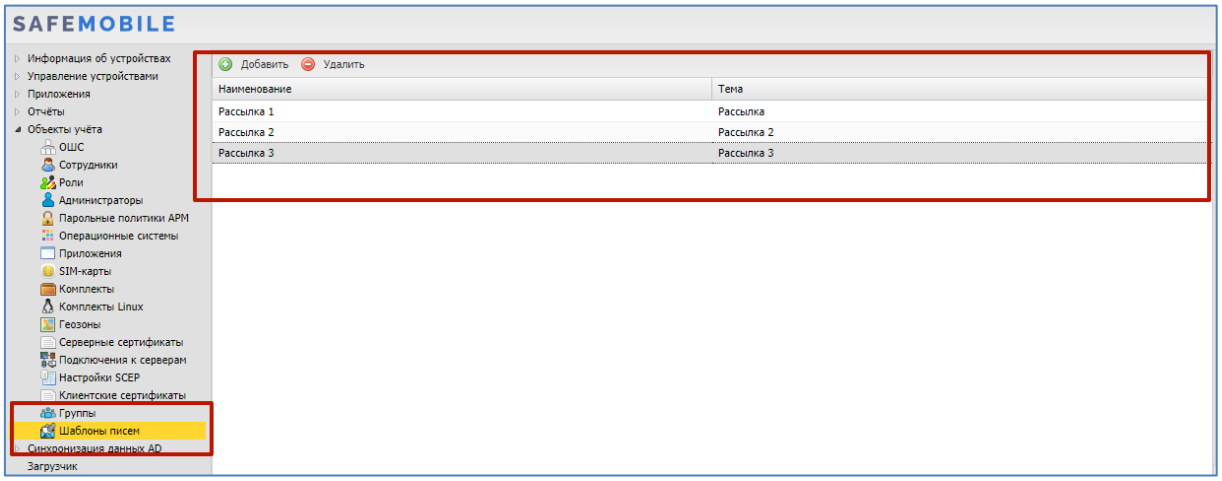


Рисунок 2.137 - Список шаблонов писем

В центральной части страницы раздела представлен список заданных шаблонов. Каждая строка списка содержит информацию об одном шаблоне и состоит из следующих полей данных:

- Наименование – наименование шаблона;
- Тема – тема сообщения, которая будет отображаться в сообщении.

В верхней части таблицы находятся кнопки:

- Добавить – добавить новый шаблон;
- Удалить – удалить выделенный в списке шаблон.

В правой части рабочего экрана отображаются настройки шаблона, выбранного в списке. Блок состоит из следующих полей данных и функциональных элементов:

- Наименование – наименование шаблона;
- Тема – тема сообщения;
- Сообщение – окно просмотра сообщения;
- Кнопка «Загрузить» - загрузка файла для создания сообщения.

2.8.17.1 Добавление нового шаблона письма

Чтобы добавить новый шаблон письма, необходимо выполнить следующие действия:

1. Перейти в раздел «Шаблоны писем»;
2. Нажать кнопку «Добавить»;
3. В блоке настроек шаблона заполнить следующие поля:
   - Наименование
   - Тема – будет отображаться как тема электронного письма
4. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора файла с шаблоном сообщения;
5. Выбрать файл;
6. Нажать кнопку «Сохранить»;
7. В модальном окне подтверждения действия нажать кнопку «Да», после чего в списке шаблоном письма появится новый шаблон.

Примечание.

- *Допускается использование подстановок в поле ввода «Тема» и в сообщении (см. список подстановок в 2.6.8.2 Настройка параметров профиля);*
- *Файл с текстом сообщения должен быть простым текстом в кодировке текста UTF8.*

2.8.17.2 Редактирование и удаление шаблона письма

Чтобы **внести изменения** в существующий шаблон, необходимо выполнить следующие действия:

1. Найти в списке шаблон, подлежащий редактированию;
2. В блоке настроек внести изменения в параметры шаблона или заменить текст сообщения, через загрузку файла;
3. Нажать кнопку «Сохранить».

Чтобы **удалить** существующий шаблон, необходимо выполнить следующие действия:

1. Найти в списке шаблон, подлежащий редактированию;
2. Нажать кнопку «Удалить»;

В модальном окне подтверждения действия нажать кнопку «Да», после чего шаблон письма будет удален.

Примечание.

- *Если шаблон уже используется в правилах несоответствия, то перед его удалением необходимо убрать использование этого шаблона в правилах несоответствия.*
- *При удалении шаблона, все не доставленные сообщения этого шаблона будут удалены.*

2.8.18 Именованные условия применения

Для применения к устройству различных сущностей (конфигурации, правила управления, профили, правила несоответствия) устройство должно соответствовать заданным условиям. Администратор может создать именованное условие применения и далее использовать его в различных назначаемых сущностях. Если администратор изменит именованное условие применения, то все сущности, использующие это условие, будут применены заново с учетом сделанных изменений.

В разделе «Условия применения» администратор может создавать, редактировать и удалять именованные условия применения (рисунок 2.138). Каждая строка списка именованных условий применения отображает следующие данные:

- Наименование – название условия. **Обязательно для заполнения**;
- Платформа – платформа, для которой может быть применено условие. **Обязательно для заполнения. После сохранения изменить параметр будет нельзя**;
- Владелец – владелец условия применения в дереве ОШС. Задается при создании условия применения.

Для поиска по списку пользователю следует воспользоваться строкой ввода поискового запроса.

В правой части раздела отображаются параметры выбранного в списке условия применения. В верхней части таблицы раздела находится панель инструментов со следующими кнопками:

- Добавить – предназначена для создания нового условия применения;
- Удалить – предназначена для удаления уже созданного условия применения.

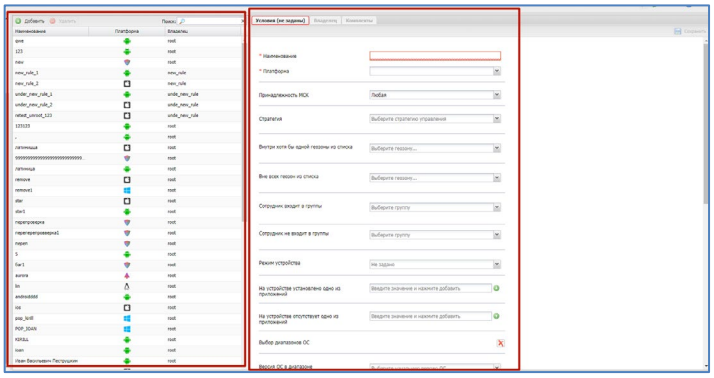


Рисунок 2.138 - Раздел «Условия применения»

2.8.18.1 Добавление нового условия применения

При добавлении нового условия применения необходимо задать его название в поле ввода «Наименование» и указать «Платформу». Описание работы с прочими параметрами условия описаны в 2.6.8.3 Задание условий применения профиля.

2.8.18.2 Удаление условия применения

Чтобы удалить условие применения необходимо выбрать его в списке условий и нажать кнопку «Удалить». Если условие не было применено ни к одной сущности, то условие будет удалено. Если условие было применено к сущностям (ПУП, конфигурация приложения, профиль, правило несоответствия), то система отобразит ошибку «Условия применения используются в назначаемых сущностях».

2.8.19 Метки устройств

Функционал маркировки устройств метками располагается в разделе «Объекты учета - Метки устройств». Пользователь имеет возможность маркировать одно или несколько устройств метками. К маркированным метками устройствам могут применяться условия применения назначаемых сущностей. На одно устройство может быть назначено произвольное количество меток.

Посмотреть список устройств и назначенные на них метки пользователь может в разделе «Информация об устройствах – Данные об устройстве», используя фильтр.

В центральной части раздела находится список меток. В правой части раздела отображаются свойства метки, выбранной в списке (рисунок 2.139).

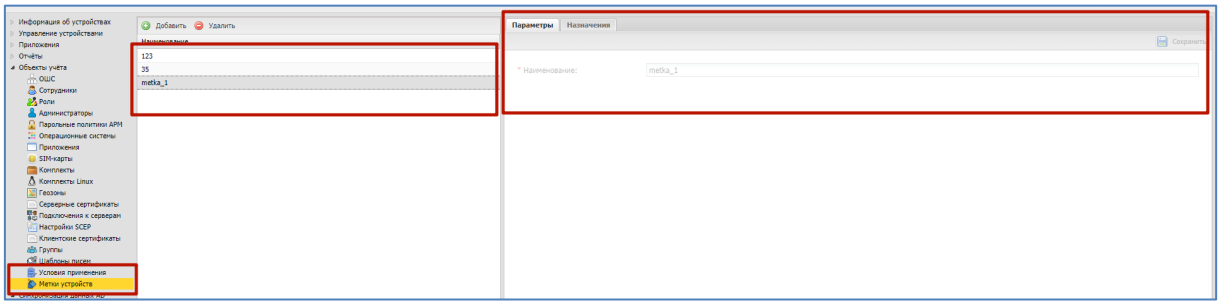


Рисунок 2.139 - Раздел «Метки устройств»

Свойства метки состоят из:

- Параметры:
  - Наименование – имя метки, задается пользователем при создании. Не может быть изменено;
- Назначения – Список устройств в ОШС, на которые можно назначить или снять назначение метки. Чтобы видеть список меток назначенных на устройства необходимо включить отображение колонки «Метки», в таблице (рисунок 2.140).

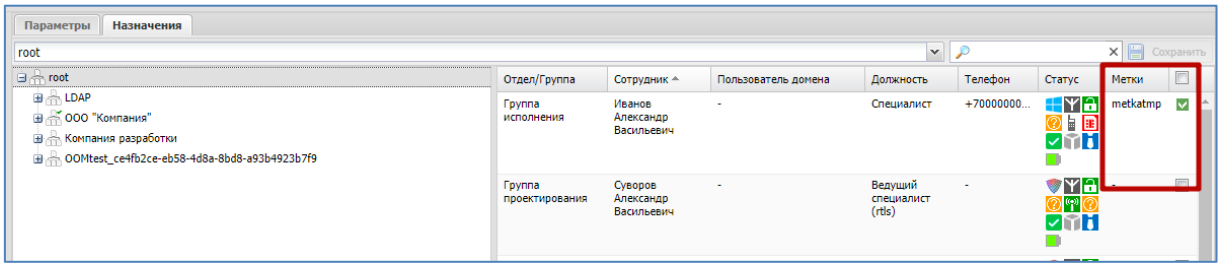


Рисунок 2.140 - Отображение колонки «Метки»

2.8.19.1 Создание и удаление метки

Чтобы создать метку необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета – Метки устройств»;
2. Нажать кнопку «Добавить»;
3. В области параметров метки задать название метки;
4. Нажать кнопку сохранить. После чего в списке меток отобразиться новая метка.

Примечание.

При вводе названия метки следует учитывать:

- *Длина ограничена 20 символами;*
- *Допустимо использовать только латинские буквы, цифры, дефис, подчерк, точку;*
- *Наименование должно быть уникальным (регистр не учитывается).*

Чтобы удалить метки необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета – Метки устройств»;
2. Выбрать метку в списке;
3. Нажать кнопку «Удалить». После чего метка будет снята со всех устройств, но останется в назначениях сущностей;
4. Перейти в раздел сущности, в которой использовалась удавленная метка (далее пример «Профили»). Профиль, в условиях которого использовалась удаленная метка, будет выделен красным (рисунок 2.141). В политике, в которой использовалась удаленная метка, будет указана дата и время удаления метки;

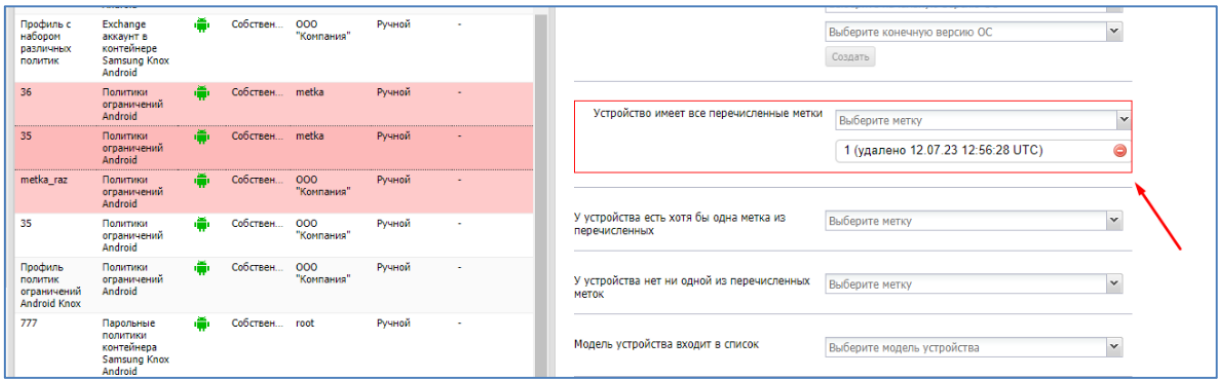


Рисунок 2.141 - Профиль с удаленной меткой в «условиях применения»

5. Выбрать профиль, перейти во вкладку «Условия»;
6. Удалить метку из условий применения профиля;
7. Нажать кнопку «Сохранить», после чего профиль не будет выделяться красным в списке.

Примечание.

Администратор может удалить метки только в своей области управления.

2.8.20 Сервисные учетные записи

Сервисные учетные записи предназначены для управления доступом к SMAPI. Для каждой сервисной учетной записи создается токен, который в дальнейшем должен быть добавлен в заголовки http-запросов к SMAPI в виде параметра "X-Domain-Api-Token". Используя токены из раздела "Сервисные учетные записи" для авторизации при подключении к SMAPI, сервис подключившийся по токену должен получать доступ:

- Только к области управления, заданной в учетной записи.
- Только URL, заданным в учетной записи.

Доступ к разделу "Объекты учета - Сервисные учетные записи" имеют администраторы назначенные на корень дерева ОШС и определяется полномочиями:

- Просмотр.
- Изменение и удаление. Только при наличии привилегии "Просмотр";
- Просмотр токена. Только при наличии привилегии "Просмотр".

Раздел содержит список учетных записей в левой части рабочей области. Каждая строка списке содержит данные о названии учетной записи и области управления. В правой части рабочей области и отображает параметры выделенной в списке учетной записи. (рисунок 2.142)

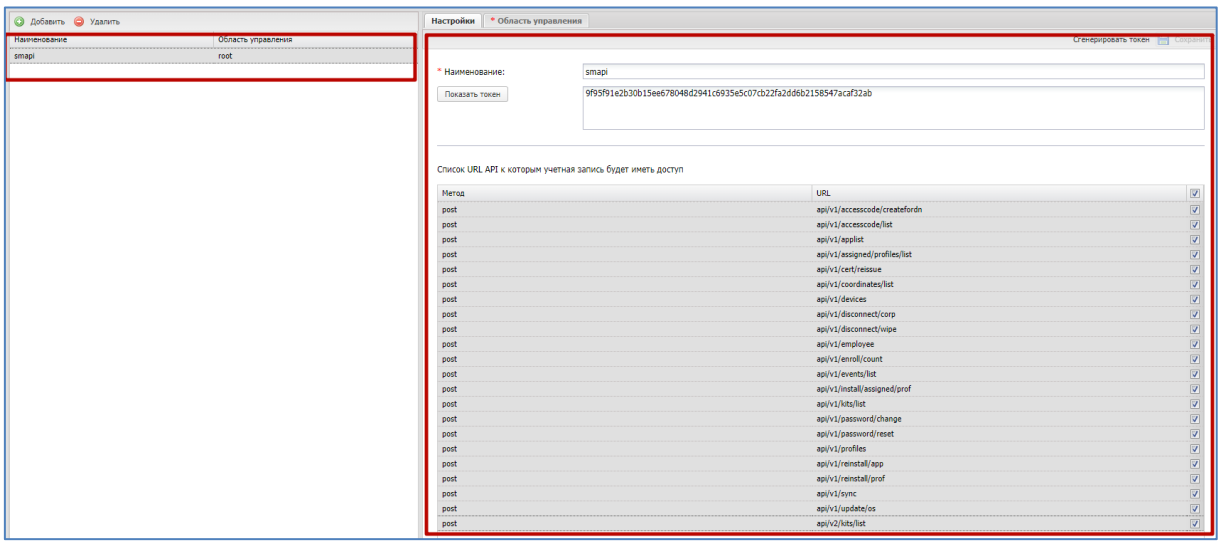


Рисунок 2.142 - Список сервисных учетных записей

Каждая сервисная учетная записи имеет следующие параметры и настройки.

- Наименование,
- Поле отображения токена - отображает токен учетной записи, после нажатия кнопки «Показать токен»;
- Кнопка «Сгенерировать токен» - При нажатии генерирует токен: 64 разряда в 16-ричном представлении. При замене токена, клиенты использовавшие прежний токен потеряют доступ к API;
  - Список URL API к которым учетная записи будет иметь доступ:
    - Метод,
    - URL,
    - чекбокс выделения с списке URL

Для создания новой сервисной учетной записи необходимо выполнить следующий действия:

1. Нажать кнопку «Добавить»;
2. В правой рабочей области заполнить поля:
   - Наименование,
   - Отметить чекбоксами URL для которых будет действовать учетная запись (опционально).
3. Во вкладке «Область применения» задать область применения;
4. Нажать кнопку сохранить;
5. Нажать кнопку «Сгенерировать токен»;
6. Задать «Область применения».

2.9 Синхронизация данных AD

2.9.1 Внешние каталоги

В центральной части страницы раздела представлен список заданных подключений, к внешним каталогам AD.

Каждая строка списка содержит информацию об одном подключении и состоит из следующих полей данных (отображаются по умолчанию):

- Наименование – наименование подключения;
- Тег агента – название компонента «агент синхронизации», предназначенного для синхронизации с AD;
- Имя пользователя – имя пользователя, для авторизации в AD;
- Синхронизация – был ли каталог синхронизирован с актуальным набором параметров и правил. Возможные значения:
    - Успешно (дата и время),
    - Ошибка (дата и время),
    - Не синхронизировался,
- Состояние синхронизации – информация о синхронизации на текущий момент. Возможные значения:
    - Запланирована (дата и время),
    - В процессе (дата и время),
    - Не запланирована,
- Последняя синхронизация – информация о последней синхронизации. Возможные значения:
    - Успешно (дата и время),
    - Ошибка (дата и время),
- Домен – название домена;
- Имя сервера - доменное имя контроллера домена.

Справа, от списка подключений располагается блок настроек выбранного в списке подключения. (рисунок 2.143.)

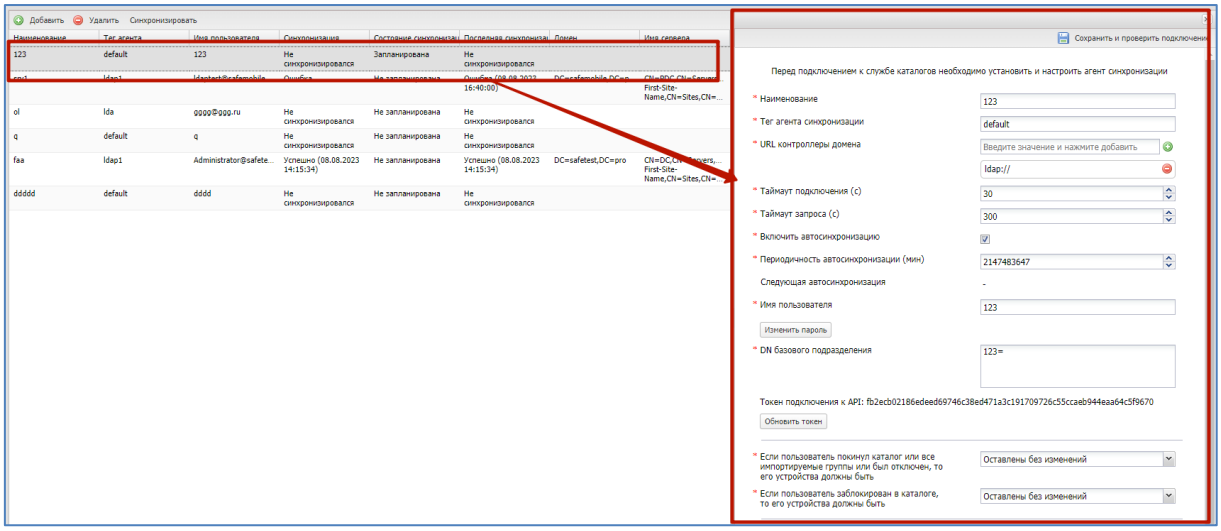


Рисунок 2.143 - Расположение блока настроек подключения

Блок настроек содержит следующие поля ввода, элементы управления и инфоблоки:

- Наименование – наименование подключения;
- Тег агента синхронизации – название компонента «агент синхронизации», предназначенного для синхронизации с AD. Тег агента должен совпадать с тегом, заданным в файле конфигурации агента синхронизации (по умолчанию имеет значение: default);
- URL контроллера домена – список из одного и более контроллеров домена. (Допускается заполнение как в виде доменного имени ldap://pdc.domain.com, так и в виде IP адреса);
- Таймаут подключения (с) – время ожидания восстановления подключения, до выдачи ошибки подключения. (заполняется в секундах);
- Таймаут запроса (с) – время ожидания ответа на запрос, до выдачи ошибки (заполняется в секундах);
- Включить автосинхронизацию – включить/выключить автоматическую синхронизацию с данным каталогом. При включенной автосинхронизации внешнего каталога изменение правил его синхронизации (Пользователи, Группы, Администраторы) невозможно;
- Периодичность автосинхронизации (мин) – период запуска автоматической синхронизации (задается в минутах);

- Следующая автосинхронизация – инфоблок с информацией о дате и времени следующей синхронизации с каталогом;
- Имя пользователя – имя пользователя, для авторизации в AD;
- Пароль – пароль пользователя;
- DN базового подразделения – заполняется в формате Distinguished Name;
- Если пользователь покинул каталог или все импортируемые группы или был отключен, то его устройства должны быть – выбор варианта действия системы:
    - Отключить от управление со сбросим к заводским настройкам;
    - Отключение от управления с удалением корпоративных данных;
    - Заблокированы;
    - Оставлены без изменений;

- Если пользователь заблокирован в каталоге, то его устройства должны быть – выбор действия системы:
    - Отключить от управление со сбросим к заводским настройкам;
    - Отключение от управления с удалением корпоративных данных;
    - Заблокированы;
    - Оставлены без изменений.

Инфоблок о состоянии подключения расположен в нижней части блока настроек подключения и содержащий следующие данные:

- Данные о проверке подключения, заполняются при нажати кнопки «Сохранить и проверить подключение»;
    - Статус подключения - возможные значения «Успех», «Ошибка», «-»;
    - Домен – название домена, записанное в формате Distinguished Name;
    - Имя сервера – имя контроллера домена, записанное в формате Distinguished Name;
- Данные об актуальной, на текущий момент синхронизации.
    - Синхронизация – был ли каталог синхронизирован с актуальным набором параметров и правил. Возможные значения:
        - Успешно (дата и время),
        - Ошибка (дата и время),
        - Не синхронизировался,
    - Состояние синхронизации – информация о синхронизации на текущий момент. Возможные значения:
        - Запланирована (дата и время),

- В процессе (дата и время),
- Не запланирована,

- Последняя синхронизация – информация о последней синхронизации. Возможные значения:
  - Успешно (дата и время),
  - Ошибка (дата и время),
  - Статус синхронизации – возможные значения «Успех», «Ошибка», «-»;
  - Время синхронизации – дата и время окончания синхронизации.

2.9.1.1 Создание нового подключения к службе каталогов

Чтобы создать подключение к внешнему каталогу AD, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги»;

2. Нажать кнопку «Добавить» (рисунок 2.144.), после чего в блоке настроек подключения будут доступны поля для ввода данных о новом подключении;

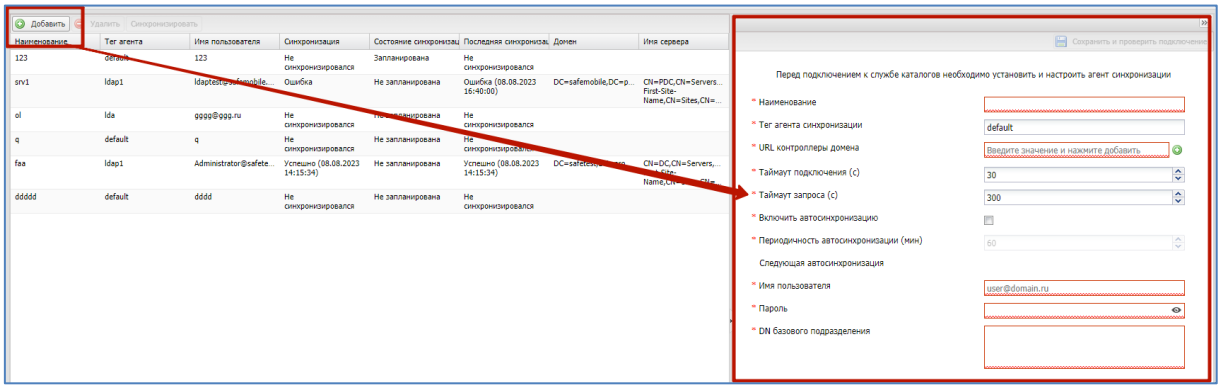


Рисунок 2.144 - Расположение кнопки «Добавить»

3. Заполнить все поля (Поле «Тег агента синхронизации» автоматически заполняется значением default);

4. Нажать кнопку «Сохранить и проверить подключение» (рисунок 2.145).

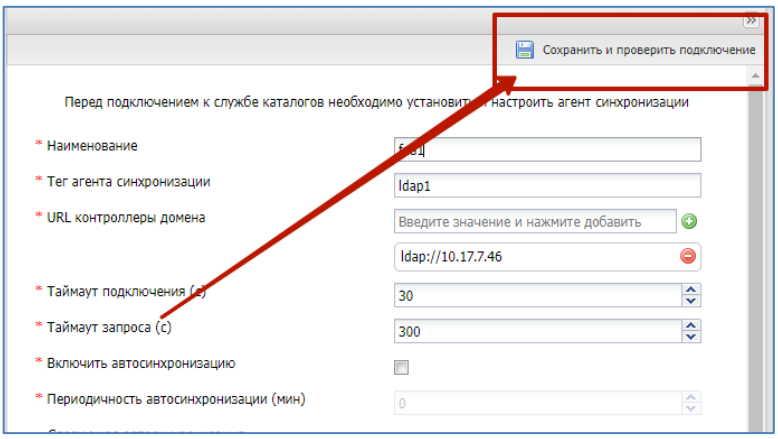


Рисунок 2.145 - Расположение кнопки «Сохранить и проверить подключение»

После нажатия кнопки «Сохранить и проверить подключение» в инфоблоке состояния подключения будет отображена информация о результатах проверки созданного подключения. (рисунок 2.146)

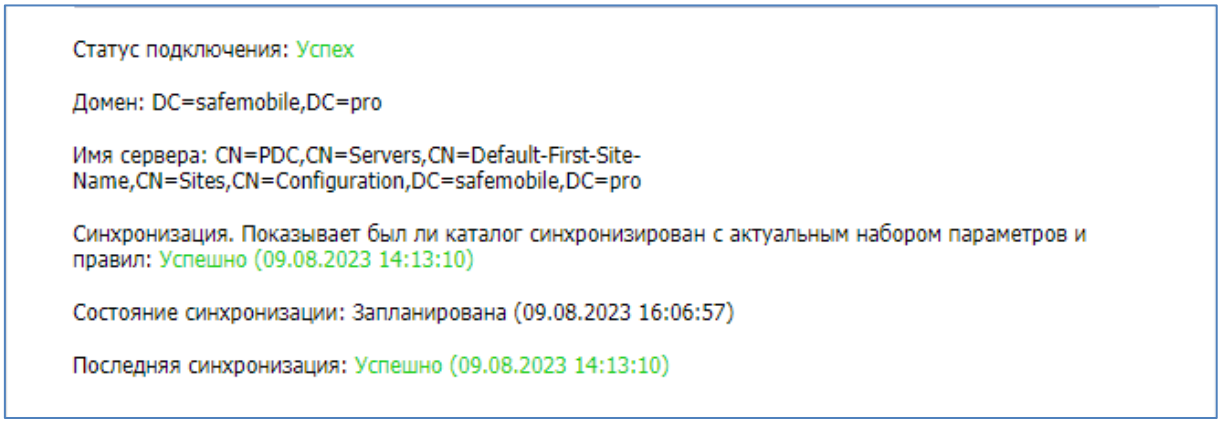


Рисунок 2.146 - Инфоблок состояния подключении

2.9.1.2 Удаление существующего подключения

Чтобы удалить существующее подключение к каталогу AD, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги»;
2. Выделить в списке подключений строку, подлежащую удалению;
3. Нажать кнопку «Удалить» (рисунок 2.147);

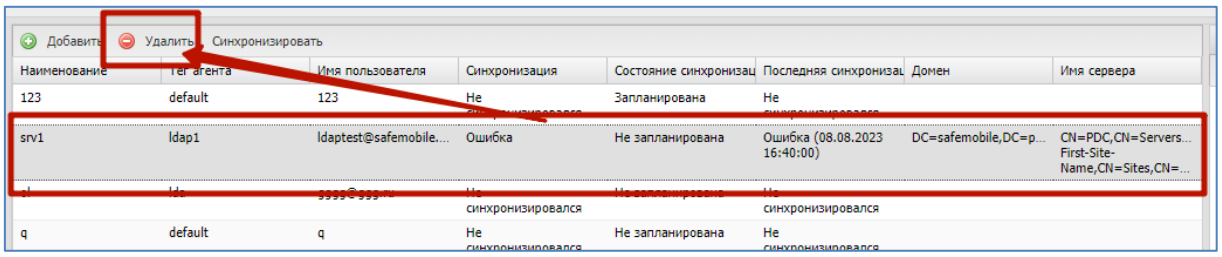


Рисунок 2.147 - Расположение кнопки «Удалить»

4. Подтвердить действие, после чего запись о подключении будет удалена.

Примечание.

- *Если удаляемое подключение ранее было успешно синхронизировано и у импортированных сотрудников имеются подключенные устройства, то система выдаст предупреждение о возможном отключении устройств пользователей от управления:*
  «Данный каталог ранее был успешно синхронизирован. Внесение изменений может привести к тому, что устройства сотрудников будут отключены от управления. Для подтверждения введите наименование внешнего каталога»;
- *Пользователи и группы, импортированные с использованием удаляемого подключения, становятся доступны для удаления;*
- *Учетные записи администраторов, импортированных с использованием удаляемого подключения, удаляются;*
- *При удалении подключения с устройствами пользователей данного подключения будут произведены операции, описанные параметре «Если пользователь покинул каталог или все импортируемые группы или был отключен, то его устройства должны быть».*

2.9.1.3 Принудительная синхронизация с каталогом AD

Чтобы запустить синхронизацию с каталогом AD принудительно, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги»;
2. Выделить в списке подключение, по которому необходимо сделать синхронизацию;
3. Нажать кнопку «Синхронизировать» (рисунок 2.148), после чего будет запущен процесс синхронизации с каталогом AD.

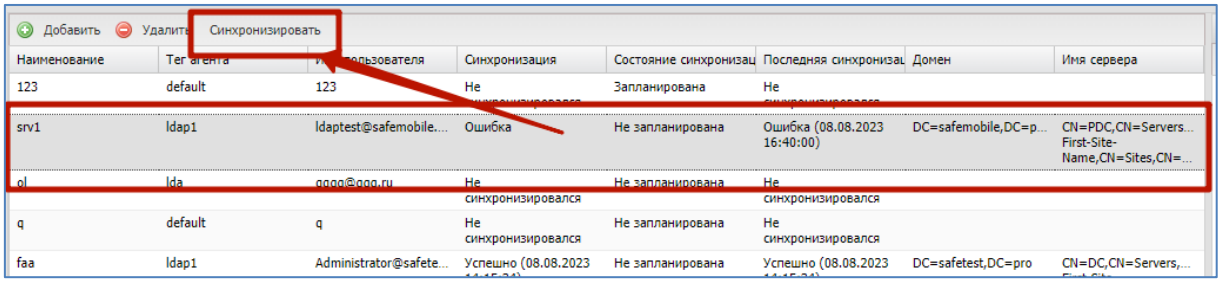


Рисунок 2.148 - Расположение кнопки «Синхронизировать»

> ***Примечание.***
>
> *Срок запуска следующей автоматической синхронизации будет отсчитываться от времени запуска принудительной синхронизации.*

2.9.2 Пользователи

В данном разделе задаются и настраиваются правила импорта пользователей из внешних каталогов AD. Результатом работы импорта пользователей является создание записи о пользователе (или списка пользователей) с атрибутами учетной записи внешнего каталога AD. Администратор может задать приоритет импорта. Если пользователь попадает под действие нескольких правил импорта, то он будет импортирован по правилу, у которого приоритет выше.

Пример: Сотрудник попадает под правила с приоритетом 1 и 2, в правилах указаны разные подразделения, к которым принадлежит сотрудник. Сотрудник будет выгружен в то подразделение, которое указано в правиле с приоритетом 1.

Учетные записи пользователей, импортированные заданными правилами, отображаются в разделе:

- Объекты учета,
  - Сотрудники.

В центральной части раздела отображается список правил импорта пользователей системы из внешнего каталога AD. (рисунок 2.149)

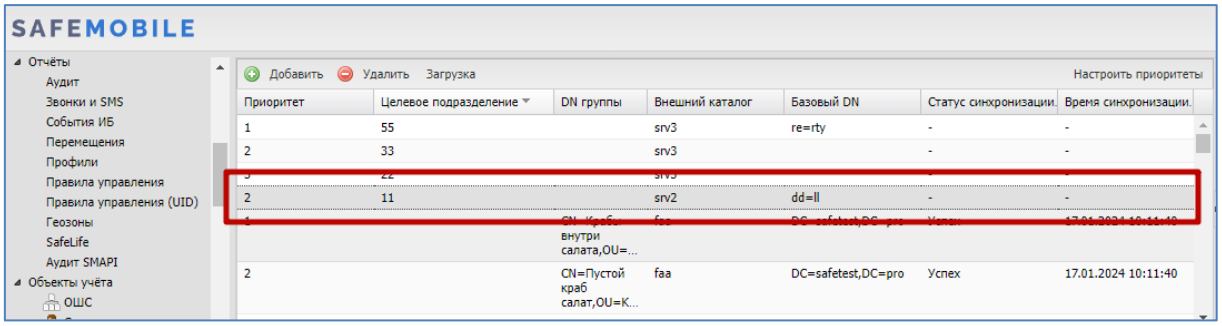


Рисунок 2.149 - Список правил синхронизации

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- Приоритет – приоритет правила импорта над другими правилами;
- Целевое подразделение – подразделение в древе ОШС, куда будет производиться импорт (опционально);
- DN группы – DN выбранной группы пользователей в каталоге AD;
- Внешний каталог – наименование подключения к внешнему каталогу AD;
- Базовый DN – DN базового подразделения;
- Статус синхронизации – статус синхронизации, актуальной на момент просмотра;
- Время синхронизации – дата и время синхронизации с внешним каталогом AD, актуальной на момент просмотра.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила. (рисунок 2.150).

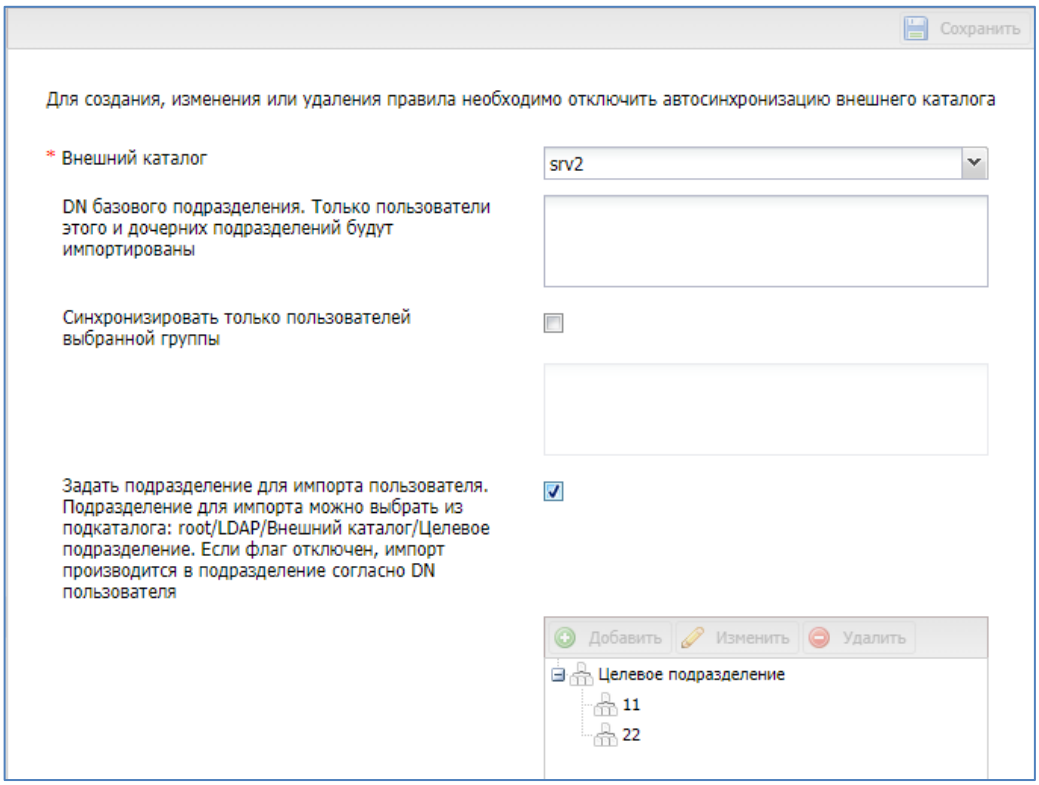


Рисунок 2.150 - Настройки правила синхронизации списка пользователей с внешним каталогом AD

Блок содержит следующие поля ввода:

- Внешний каталог - наименование подключения к внешнему каталогу AD. (Не доступен для изменения уже заданных правил).
- DN базового подразделения. Только пользователи этого и дочерних подразделений будут импортированы – задается в формате DN. (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
- Синхронизировать только пользователей выбранной группы – флаг включает/выключает возможность добавления отдельной группы пользователей AD, подлежащих импорту;
    - Поле ввода DN группы пользователей подлежащих импорту;
- Задать подразделение для импорта пользователя. Подразделение для импорта можно выбрать из подкаталога: root/LDAP/Внешний каталог/Целевое подразделение. Если флаг отключен, импорт производится в подразделение согласно DN пользователя – флаг включает/выключает возможность указания целевого подразделения.
    - Окно выбора целевого подразделения в структуре ОШС. В этом окне можно создать, изменить или удалить целевое подразделение. Так же

целевое подразделение может быть задано заранее, в разделе «Объекты учета - ОШС».

- Создание целевого подразделения – процесс аналогичен созданию подразделения в структуре ОШС;
- Удалить целевое подразделение:
  - Если есть правила импорта пользователей, которые используют данное целевое подразделение следует сначала удалить или правила или убрать целевое подразделение из этих правил. В противном случае при попытке удаления система выдаст сообщение об ошибке: «*Подразделение ОШС является целевым для импорта пользователей внешнего каталога*»;
- Изменение целевого подразделения:
  - Для внесения изменений в целевое подразделение необходимо указать новое имя и выбрать стратегию управления.

Примечание.

- *Импортированы будут только те пользователи, которые принадлежат базовому подразделению и непосредственно входят в указанную группу пользователей. Пользователи, входящие в подгруппы указанной группы, импортированы* ***не будут.***
- *При включенной автосинхронизации.*
  Если у группы пользователей, используемой в правиле импорта сотрудников, изменился distinguishedName или базовое подразделение, то будет считаться, что сотрудники, импортированные этим правилом, покинули область источника импорта. С их устройствами будут произведены действия согласно настройкам во внешнем каталоге. Сотрудники станут доступным для удаления.

В «шапке» списка правил синхронизации расположены кнопки вызова следующих функций (рисунок 2.151):

- Кнопка «Добавить» - добавить новое правило импорта;
- Кнопка «Удалить» - удалить правило импорта;

- Кнопка «Загрузить» - задать правило импорта пользователей с помощью файла, содержащего список групп пользователей;
- Кнопка «Настроить приоритеты» – открывает настройки приоритета для правил импорта.

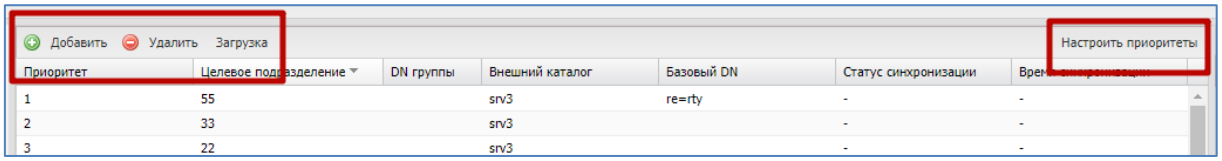


Рисунок 2.151 - расположение кнопок «Добавить», «Удалить», «Загрузить», «настроить приоритеты»

2.9.2.1 Изменение параметров существующего правила

Чтобы изменить параметры правила, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи»;
2. В списке правил синхронизации выделить правило подлежащее изменению;
3. В блоке параметров правила внести изменения;
4. Нажать кнопку «Сохранить» (рисунок 2.152).

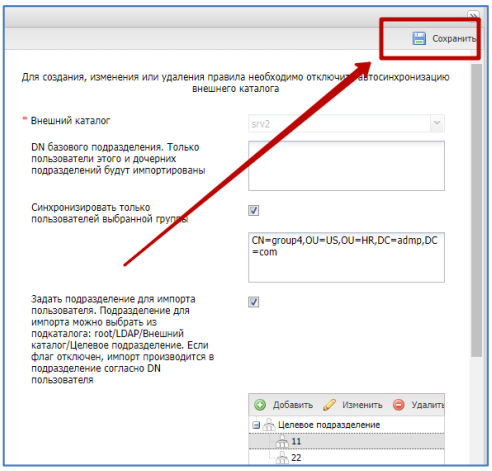


Рисунок 2.152 - Расположение кнопки «Сохранить»

2.9.2.2 Создание нового правила импорта пользователей

Чтобы создать новое правило импорта пользователей системы из списка пользователей внешнего каталога AD, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи»;
2. Нажать кнопку «Добавить»;
3. В блоке параметров создаваемого правила заполнить необходимые поля;
4. Нажать кнопку «Сохранить».

Примечание.

Импортированы будут только те пользователи, которые:

- *принадлежат и базовому подразделению и указанной группе пользователей;*
- *у которых заполнен атрибут displayName, либо атрибуты givenName и sn*

2.9.2.3 Удаление правила импорта пользователей

Чтобы удалить правило импорта пользователей, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи»;
2. В списке правил синхронизации выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной;
3. Нажать кнопку «Удалить»;
4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.153.), после чего выбранное правило будет удалено.

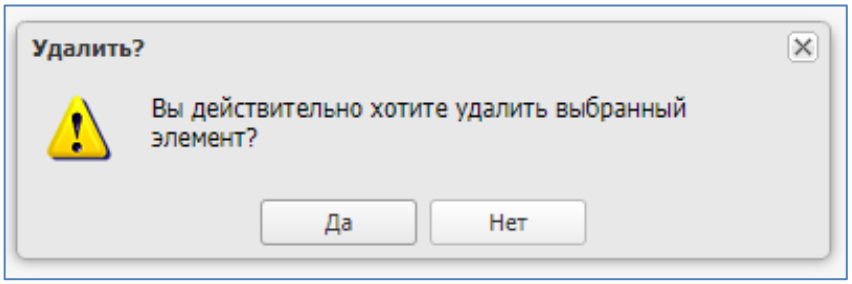


Рисунок 2.153 - Диалоговое окно подтверждения действия

2.9.2.4 Создание правила импорта пользователей с помощью файла списка групп пользователей

Данная функция используется для пакетного создания правил импорта пользователей из одного базового подразделения, но принадлежащих различным группам пользователей внешнего каталога AD. Для её использования необходимо иметь файл со списком DN имен групп пользователей внешнего каталога, подлежащих импорту. Формат файла – csv, кодировка – UTF-8.

Чтобы создать правило импорта пользователей с помощью файла, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи»;
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.154);

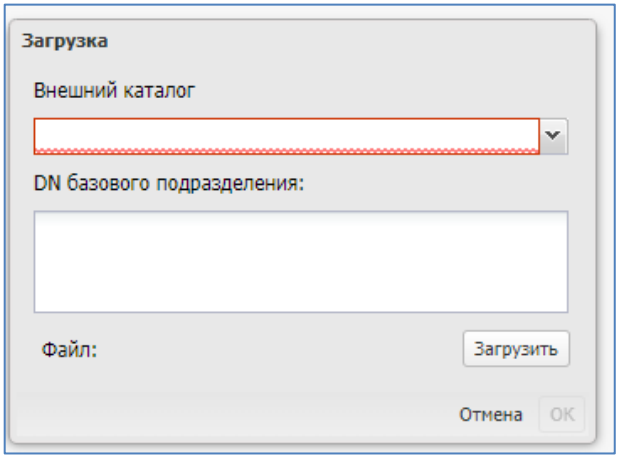


Рисунок 2.154 - Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
   - Внешний каталог – название подключения к внешнему каталогу AD (выбор из выпадающего списка существующих подключений);
   - DN базового подразделения – название подразделения которому принадлежат импортируемые пользователи внешнего каталога (задается в формате DN). Если поле не задано, то за DN базового подразделения берется DN внешнего каталога;
4. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащего список групп пользователей;
5. Выбрать файл;
6. Нажать кнопку «Ок», после чего будут созданы новые правила импорта.

2.9.2.5 Настройка приоритетов правила импорта пользователей

Чтобы настроить приоритеты правила импорта необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи»;
2. Нажать кнопку «Настроить приоритеты», после чего откроется окно настроек приоритетов правил импорта;
3. Выбрать внешний каталог, для правил которого требуется настроить приоритеты (рисунок 2.155);

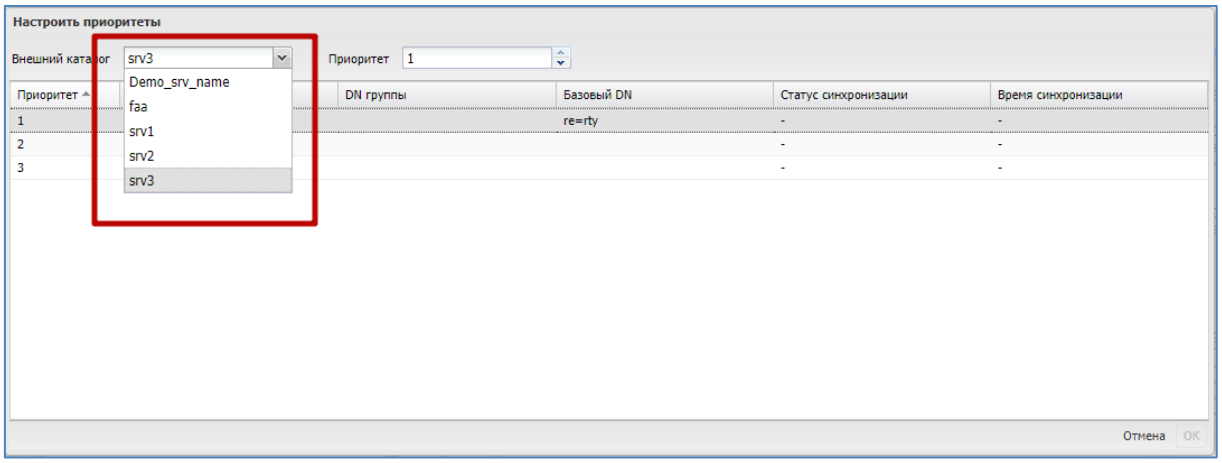


Рисунок 2.155 - Выбор внешнего каталога в настройках приоритетов импорта

4. Выбрать правило в списке и указать приоритет для данного правила (рисунок 2.156);

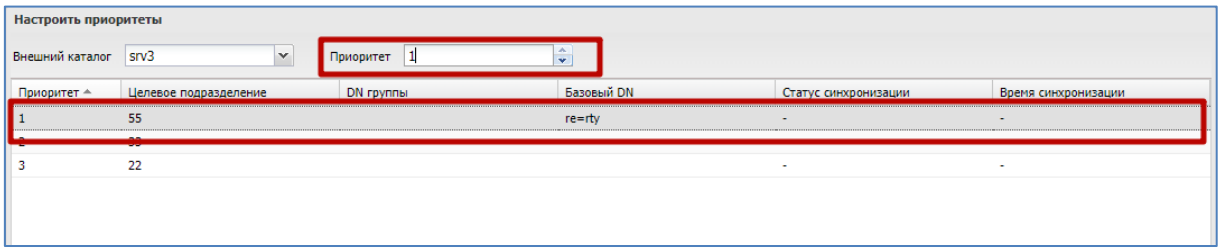


Рисунок 2.156 - Назначение приоритета на правило импорта

5. Нажать кнопку «Ок».

2.9.3 Группы

В разделе отображаются правила импорта групп пользователей из внешнего каталога AD. Результатом работы правил импорта групп пользователей является список DN групп и DN имена пользователей, принадлежащих этим группам.
Группы пользователей, импортированные по заданным правилам, отображаются в разделе:

- Объекты учета,
  - Группы.

Используются при конфигурировании приложений и устройств, в разделах:

- Приложения,
  - Правила управления,
    - Вкладка «Условия».
  - Конфигурации,
    - Вкладка «Условия».
- Управление устройствами,
  - Правила несоответствия,
    - Вкладка «Условия».
  - Профили,
    - Вкладка «Условия».

В центральной части раздела отображается список правил импорта групп пользователей внешнего каталога AD. (рисунок 2.157).

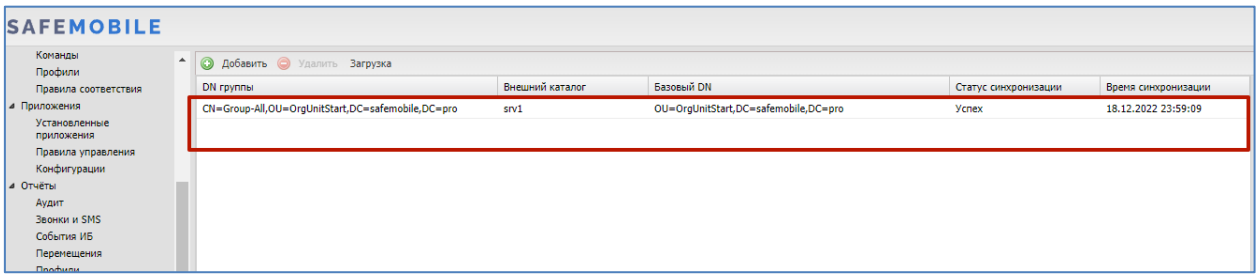


Рисунок 2.157 - Список правил импорта групп

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- DN группы – DN выбранной группы пользователей в каталоге AD,
- Внешний каталог – наименование подключения к внешнему каталогу AD,

- Базовый DN – DN базового подразделения,
- Статус синхронизации – статус синхронизации, актуальной на момент просмотра,
- Время синхронизации – дата и время синхронизации с внешним каталогом AD, актуальной на момент просмотра.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила. (рисунок 2.158)

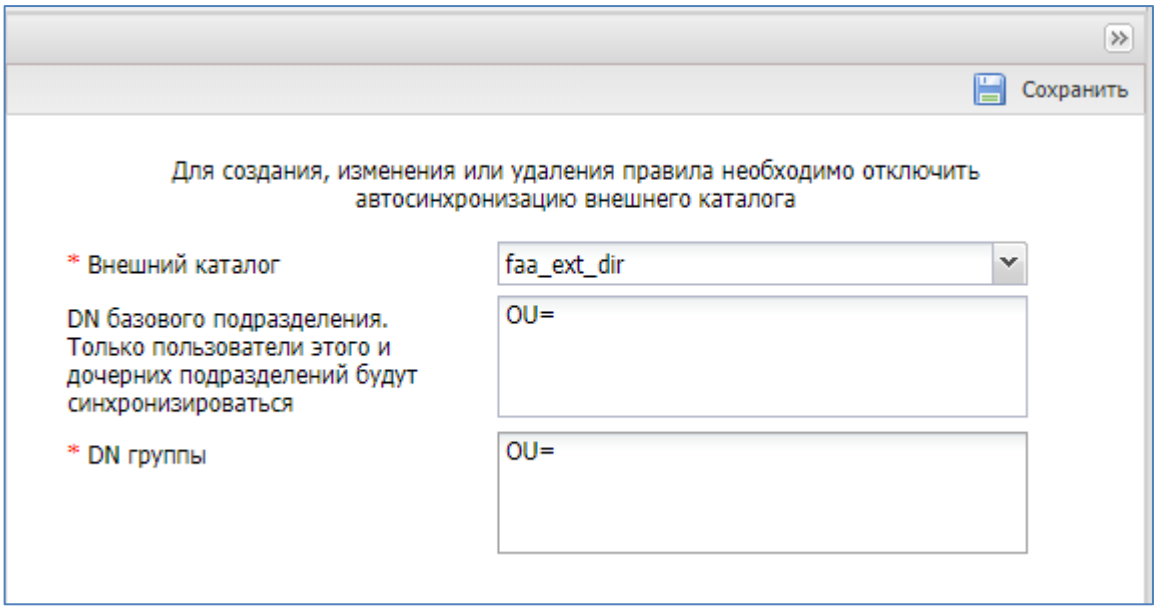


Рисунок 2.158 - Параметры правила импорта групп

Блок содержит следующие поля ввода:

- Внешний каталог - наименование подключения к внешнему каталогу AD. (Не доступен для изменения уже заданных правил);
- DN базового подразделения. Только пользователи этого и дочерних подразделений будут синхронизироваться – задается в формате DN;
  (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
- DN группы – DN имя группы, подлежащей импорту из внешнего каталога (обязательно для заполнения).

Примечание.

- *Импортируются только названия групп, а не пользователи.*

  Пользователи, импортированные из внешнего каталога, сопоставляются с импортированным группами и отображаются в разделе:

  Объекты учета
  - ***Группы***
    - ***Вкладка «члены группы»***

- *При включенной автосинхронизации.*

  Если у импортированной группы изменился distinguishedName (группа переименована или переименовано одно из родительских подразделений группы), то из импортированной группы будут удалены все сотрудники. Если импортированная группа использовалась в условиях применения профилей, правил управления, конфигурация приложений или правил несоответствия, то их назначения будут сняты с сотрудников, ранее входивших в группу.

В «шапке» списка правил синхронизации расположены кнопки вызова следующих функций (рисунок 2.159):

- «Добавить» - добавить новое правило импорта;
- «Удалить» - удалить правило импорта из списка;
- «Загрузить» - задать правило импорта с помощью файла, содержащего список групп.

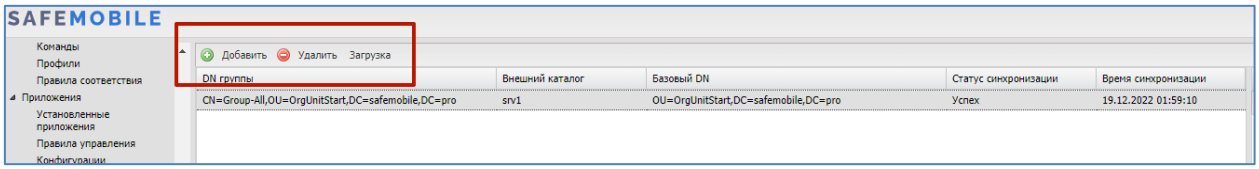


Рисунок 2.159 - Расположение кнопок «Добавить», «Удалить», «Загрузить»

2.9.3.1 Изменение параметров существующего правила импорта

Чтобы изменить параметры существующего правила импорта групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы»
2. Найти и выделить в списке правило, подлежащее изменению параметров
3. В блоке параметров правила внести изменения
4. Нажать кнопку «Сохранить». (рисунок 2.160)

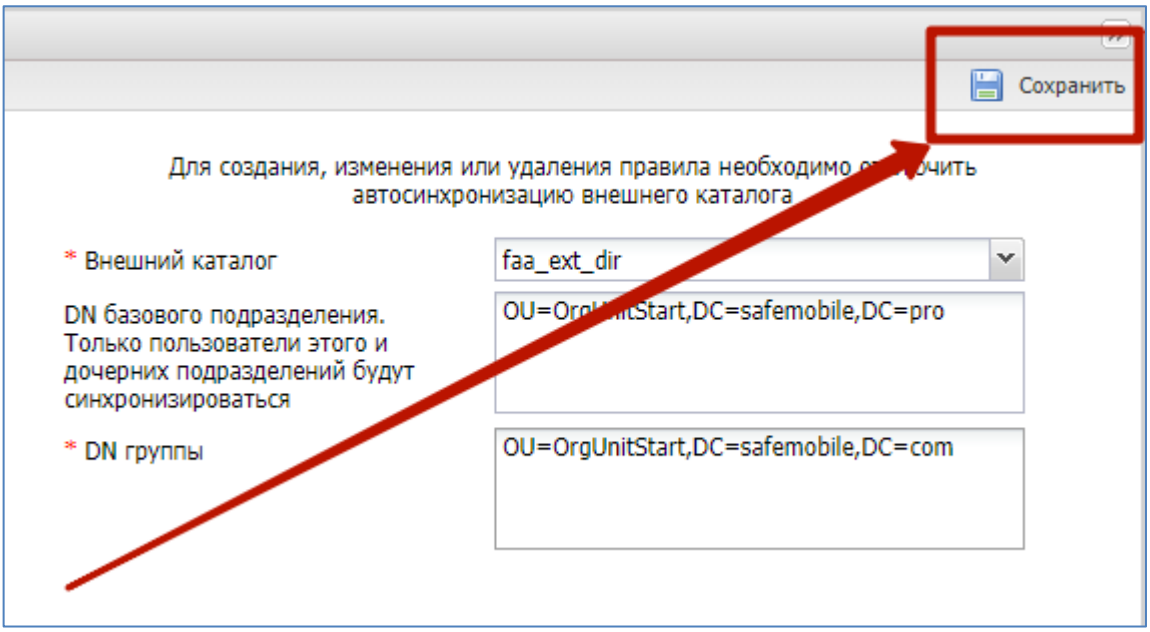


Рисунок 2.160 - Расположение кнопки «Сохранить»

2.9.3.2 Добавить новое правило импорта групп пользователей

Чтобы добавить новое правило импорта группы пользователей, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы»;
2. Нажать кнопку «Добавить»;
3. В блоке параметров правила заполнить необходимые поля ввода;
4. Нажать кнопку «Сохранить».

2.9.3.3 Удалить существующее правило импорта групп из списка

Чтобы удалить правило импорта групп из списка, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы»;
2. В списке правил импорта выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной;
3. Нажать кнопку «Удалить»;
4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.161), после чего выбранное правило будет удалено.

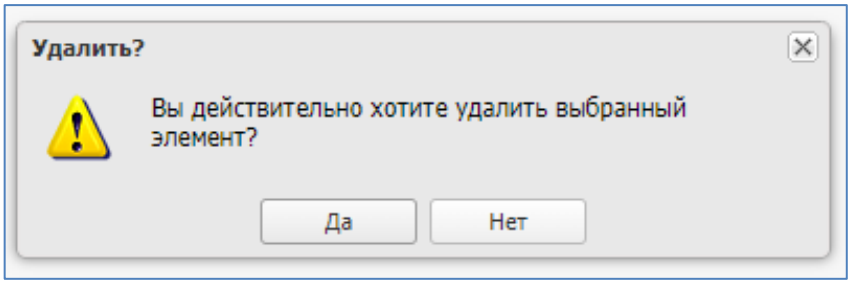


Рисунок 2.161 - Диалоговое окно подтверждения действия

2.9.3.4 Создание правила импорта групп из файла, содержащего список групп внешнего каталога

Данная функция используется для пакетного создания правил импорта групп внешнего каталога. Для её использования необходимо иметь файл со списком групп внешнего каталога, подлежащих импорту.

Чтобы создать правило импорта групп с помощью файла, содержащего список групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы»;
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.162);

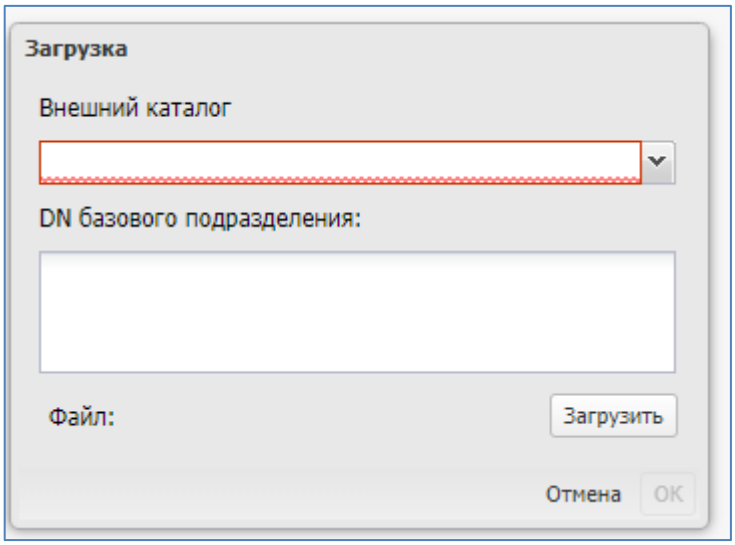


Рисунок 2.162 - Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
4. Внешний каталог – название подключения к внешнему каталогу AD (выбор из выпадающего списка существующих подключений);
5. DN базового подразделения – название подразделения, которому принадлежит загружаемый список групп (задается в формате DN). (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
6. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащим список групп;
7. Выбрать файл;
8. Нажать кнопку «Ок», после чего будет созданы новые правила импорта.

2.9.4 Администраторы

В данном разделе задаются правила импорта списка пользователей из внешнего каталога AD, подлежащих назначению администраторами в системе.

Список пользователей-администраторов, созданных с помощью правил импорта из внешнего каталога доступен в разделе:

- Объекты учета
  - Администраторы

В центральной части раздела отображается список правил импорта администраторов из внешнего каталога AD. (рисунок 2.163).

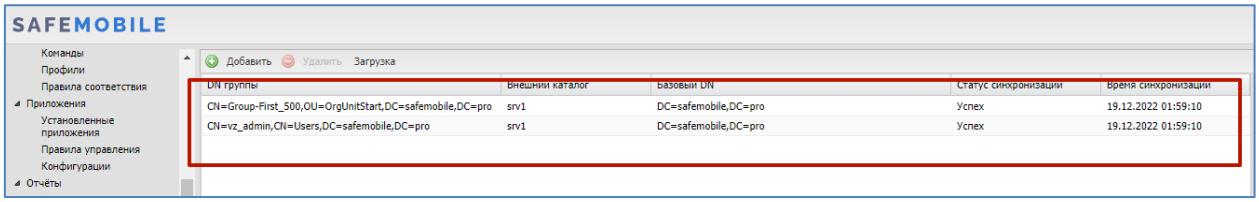


Рисунок 2.163 - Список правил синхронизации

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- DN группы – DN выбранной группы пользователей в каталоге AD,
- Внешний каталог – наименование подключения к внешнему каталогу AD,
- Базовый DN – DN базового подразделения,
- Статус синхронизации – статус синхронизации, актуальной на момент просмотра,
- Время синхронизации – дата и время синхронизации с внешним каталогом AD, актуальной на момент просмотра.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила. (рисунок 2.164)

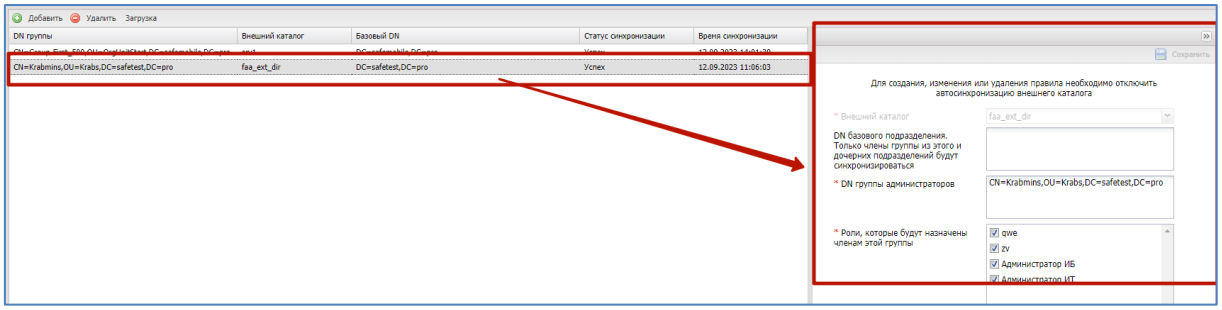


Рисунок 2.164 - Расположение блока параметров правила импорта

Блок содержит следующие поля ввода:

- Внешний каталог - наименование подключения к внешнему каталогу AD. (Не доступен для изменения уже заданных правил);
- DN базового подразделения. Только члены группы из этого подразделения и дочерних подразделений будут синхронизироваться – задается в формате DN.
  (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
- DN группы администраторов – DN имя группы администраторов (обязательно для заполнения);
- Роли, которые будут назначены членам этой группы – список ролей администраторов системы (обязательно для заполнения).

Примечание.

- *Список ролей, отображаемый в параметрах правила задается в разделе: Объекты учета - Роли.*
- *При включенной автосинхронизации. если у группы, используемой в правиле импорта администраторов, изменился distinguishedName, то будет считаться, что администраторы, импортированные этим правилом, покинули область импорта AD. Администраторы будут удалены.*

В «шапке» списка правил расположены кнопки вызова следующих функций (рисунок 2.165):

- Кнопка «Добавить» - добавить новое правило импорта;
- Кнопка «Удалить» - удалить правило импорта из списка;
- Кнопка «Загрузить» - задать правило импорта с помощью файла, содержащего список групп.

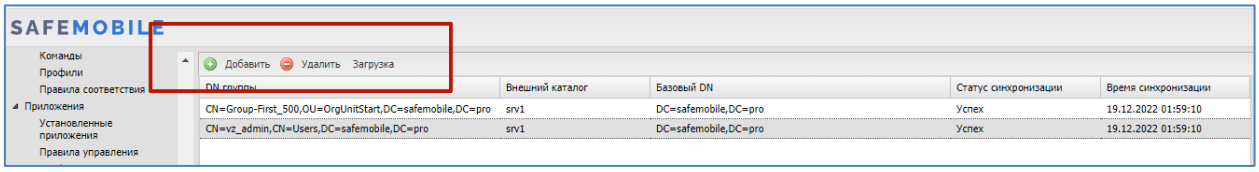


Рисунок 2.165 - Расположение кнопок «Добавить», «Удалить», «Загрузить»

2.9.4.1 Изменение параметров существующего правила

Чтобы изменить параметры правила, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы»;
2. В списке правил синхронизации выделить правило подлежащее изменению;
3. В блоке параметров правила внести изменения;
4. Нажать кнопку «Сохранить».

2.9.4.2 Добавить новое правило импорта администраторов

Чтобы добавить новое правило импорта администраторов, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы»;
2. Нажать кнопку «Добавить»;
3. В блоке параметров правила заполнить необходимые поля ввода;
4. Нажать кнопку «Сохранить».

Примечание.

Импортированы будут только те пользователи, у которых заполнен атрибут displayName, либо атрибуты givenName и sn.

2.9.4.3 Удалить существующее правило импорта администраторов

Чтобы удалить правило импорта администраторов, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы»;
2. В списке правил выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной;
3. Нажать кнопку «Удалить»;
4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.166), после чего выбранное правило будет удалено.

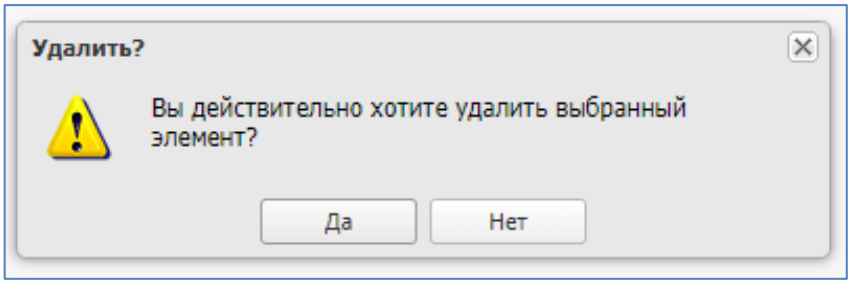


Рисунок 2.166 - Диалоговое окно подтверждения действия

2.9.4.4 Создание правила импорта администраторов из файла, содержащего список групп администраторов внешнего каталога.

Данная функция используется для пакетного создания правил импорта администраторов из нескольких групп пользователей внешнего каталога.

Для её использования необходимо иметь файл со списком групп пользователей внешнего каталога, подлежащих импорту.

Чтобы создать правило импорта групп с помощью файла, содержащего список групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы;
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.167);

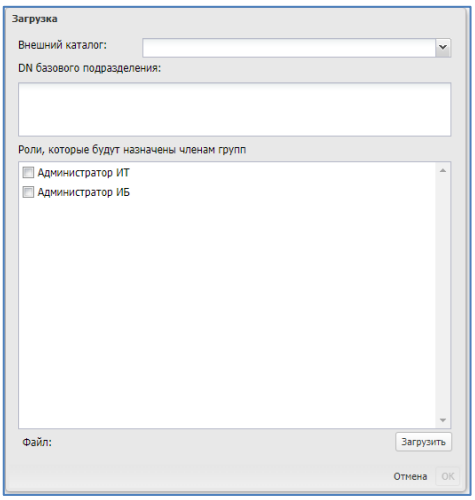


Рисунок 2.167 - Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
   - Внешний каталог – название подключения к внешнему каталогу AD (выбор из выпадающего списка существующих подключений);
   - DN базового подразделения – название подразделения, которому принадлежит загружаемый список групп (задается в формате DN).
     (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога).

4. Роли, которые будут назначены членам групп – отметить флагами роли администраторов из списка;
5. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащим список групп;
6. Выбрать файл;
7. Нажать кнопку «Ок», после чего будет создано новое правило импорта.

2.9.5 Журнал

В разделе отображается список событий, связанных с импортом данных из внешних каталогов AD.

Каждая строка списка – запись о событии синхронизации одного правила импорта и содержит в себе следующие данные (отображаются по умолчанию):

- Тип – тип импортируемых данных (Пользователи, Группы, Администраторы);
- DN группы – DN группы импортируемых данных;
- Внешний каталог – название подключения к внешнему каталогу;
- Базовый DN – DN базового подразделения;
- Время начала – время начала синхронизации с внешним каталогом;
- Время завершения – время завершения синхронизации с внешним каталогом;
- Статус – статус операции, после ее завершения;
- Детали – детальная информация о возникших ошибках.

2.10 Управление кодами приглашения (пункт меню «Загрузчик»)

«UEM SafeMobile» предоставляет возможность самостоятельной регистрации пользователей МСК при помощи кодов приглашений. Для управления кодами приглашений используется пункт меню **«Загрузчик»**. В окне отображается таблица кодов приглашений в соответствии с рисунком 2.168, которая состоит из следующих столбцов:

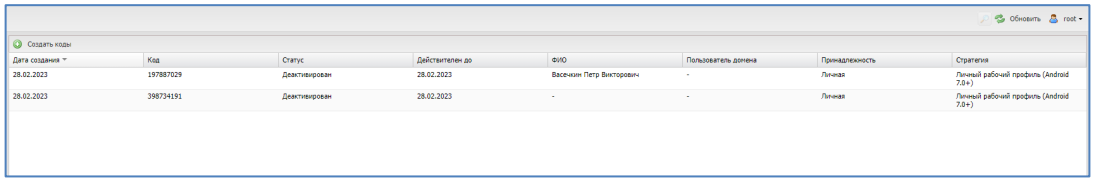


Рисунок 2.168 - Окно «Загрузчик»

- Дата создания – отображает дату создания кода приглашения.
- Код – отображает значение кода;
- Статус – отображает состояние кода приглашения;
- Действителен до – отображает дату истечения срока действия кода приглашения;
- ФИО – отображает фамилию, имя и отчество сотрудника, которому присвоен код приглашения;
- Принадлежность – признак собственности МСК (корпоративное / личное);
- Стратегия – способ управления устройством Android. Возможны варианты:
    - Автоматический выбор управления – монитор автоматически выбирает стратегию в зависимости от полученных привилегий;
    - Только устройство (Android) – требует наличия у монитора привилегий владельца устройства (Device Owner) или привилегий KNOX, и администратора устройства. Применима для всех поддерживаемых версий Android;
    - Устройство и контейнер KNOX (Samsung 5.0 - 9) – требует наличия у монитора привилегий KNOX и администратора устройства (Device Admin). Применима для МСК Samsung с версией Android начиная с 5.0 по 9.0;
    - Корпоративный рабочий профиль (Android 11.0+) – требует наличия у монитора привилегий владельца профиля (Profile Owner). Применима для МСК с версией Android 11.0 и выше. На МСК Samsung при отсутствии у монитора привилегий KNOX Premium и МСК прочих производителей, применение правил управления приложениями, требует действий от пользователя.

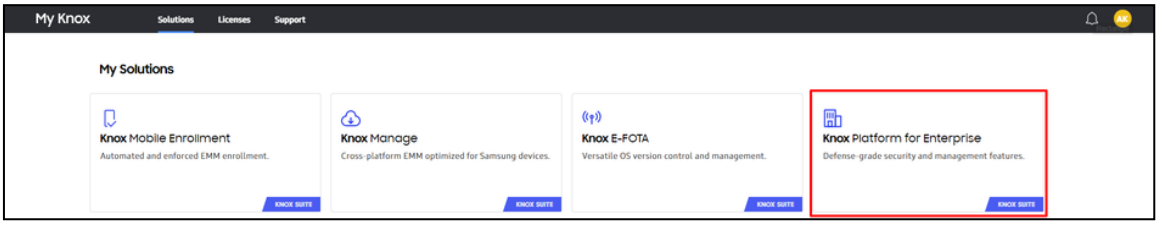
- Личный рабочий профиль (Android 7.0+) – требует наличия у монитора привилегий владельца профиля (Profile Owner). Применима для МСК с версией Android 7.0 и выше. На МСК Samsung при отсутствии у монитора привилегий KNOX Premium и МСК прочих производителей, применение правил управления приложениями, требует действий от пользователя.

Примечание.

Чтобы получить привилегии KNOX Premium, необходимо выполнить следующие действия:

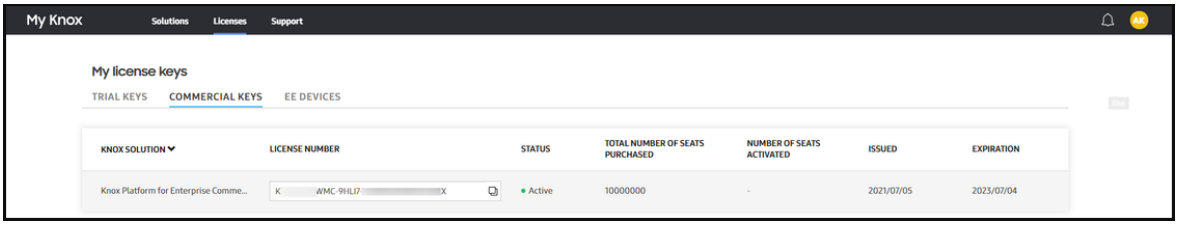
1. Перейти по ссылке: samsungknox.com со своей учетной записью, или создать новую (нужен рабочий email, публичные не принимаются);

2. Нажать на блок «Knox Platform for Enterprise»;



3. Через некоторое время появится сообщение, что коммерческий ключ успешно сгенерирован;

4. Новый ключ отобразится на странице Licenses в разделе Commercial Keys.



В таблице имеется возможность отображения кодов приглашений в зависимости от статуса. Для этого следует нажать кнопку «Отображать со статусом», после чего раскроется меню со следующими пунктами (рисунок 2.169):

- Новый код – созданный Администратором код, который пока не был использован сотрудником-абонентом МСК;

- Подготовка к установке – выполняется подготовка к установке мобильного клиента SafeMobile на МСК;
- Деактивирован – код деактивирован в результате истечения срока действия или принудительной деактивации Администратором;
- Клиент успешно установлен – мобильный клиент SafeMobile успешно установлен на МСК.

Для выбора статуса кода следует установить флажок в выбранной строке. По умолчанию в таблице показываются все коды приглашений без фильтрации (флажки в раскрывающемся меню **«Отображать со статусом»** сняты).

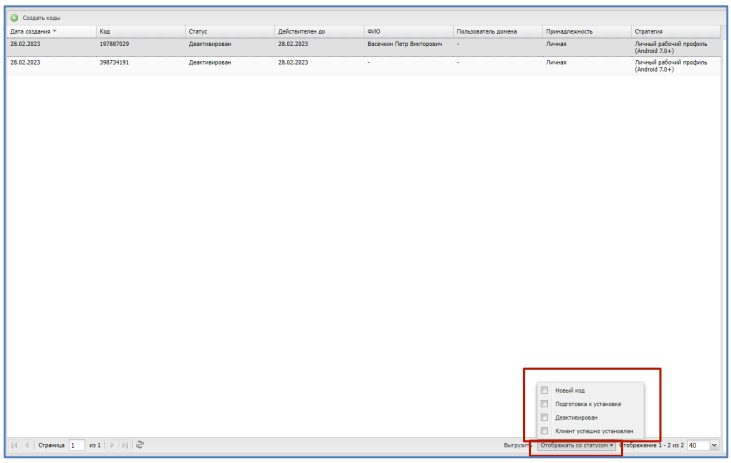


Рисунок 2.169 - Фильтрация по статусам кода приглашения

В верхней части окна расположена кнопка **«Создать коды»**, при нажатии которой открывается окно для создания кодов приглашений (рисунок 2.170).

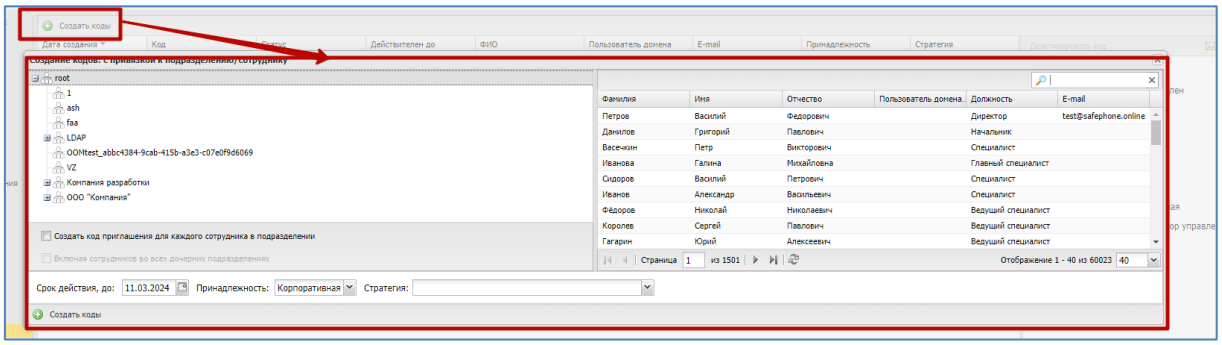


Рисунок 2.170 - Окно «Создание кодов»

Для создания кода приглашения для зарегистрированного сотрудника необходимо выбрать подразделение и сотрудника, для которого создается приглашение. С помощью «поиска» можно найти сотрудника по таким параметрам как:

- Фамилия;
- Имя;
- Отчество;
- Пользователь домена;
- Должность.

Указать в календаре дату, после которой действие кода будет прекращено (в поле **«Срок действия, до»**), выбрать принадлежность и стратегию. Стратегия будет применятся только для МСК Android. Затем следует нажать кнопку **«Создать коды»**, расположенную в нижней части окна **«Создание кодов»** в соответствии с рисунком 2.171. После подтверждения действия будет создан новый код приглашения, и запись о нем добавится в таблицу кодов со статусом **«Новый код»**.

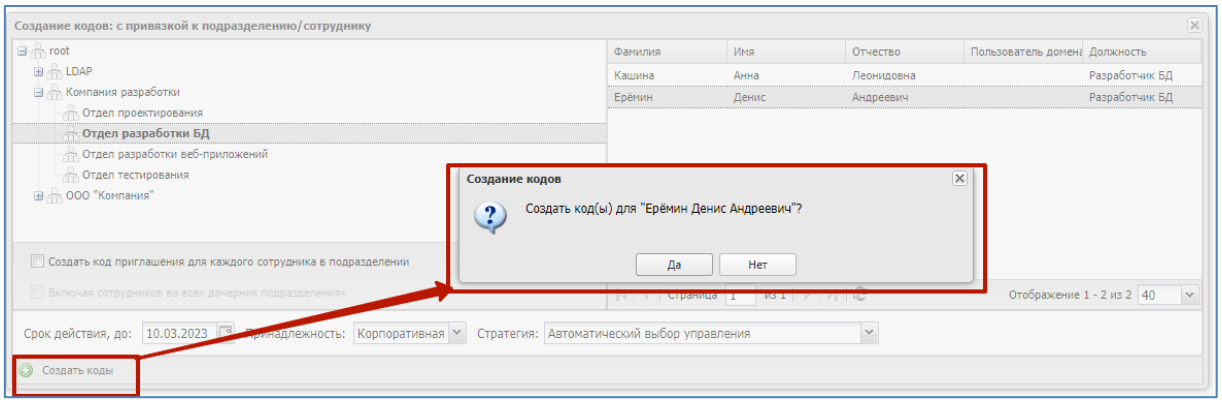


Рисунок 2.171 - Создание кодов с привязкой к сотруднику

«UEM SafeMobile» позволяет создавать коды приглашения для всех сотрудников, относящихся к одному подразделению или организации в целом. Для этого необходимо выбрать требуемое подразделение в списке слева и установить флажок **«Включая сотрудников во всех дочерних подразделениях»**, если требуется для всех подчиненных сотрудников (рисунок 2.172).

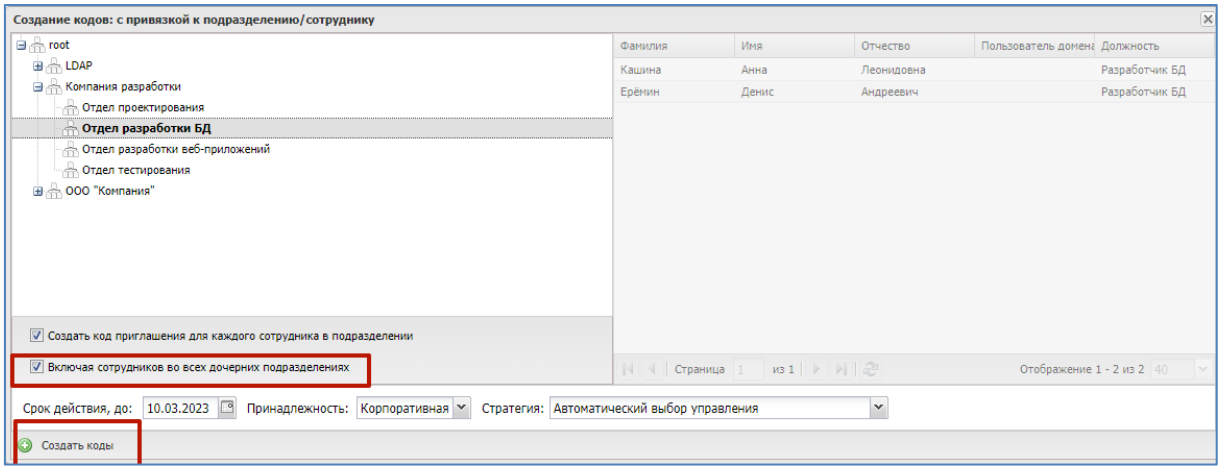


Рисунок 2.172 - Создание кодов с привязкой к подразделению

После нажатия кнопки **«Создать коды»** будут созданы новые коды приглашения и записи о них добавятся в таблицу кодов со статусом «**Новый код»**.

После этого Администратор выбирает запись с новым кодом в соответствии с рисунком 2.173, копирует QR-код и сохраняет в файл (на рисунке QR-код приведен условно). Далее Администратор рассылает файлы с QR-кодами требуемым сотрудникам и разрешает им выполнять самостоятельную регистрацию своих устройств в системе.

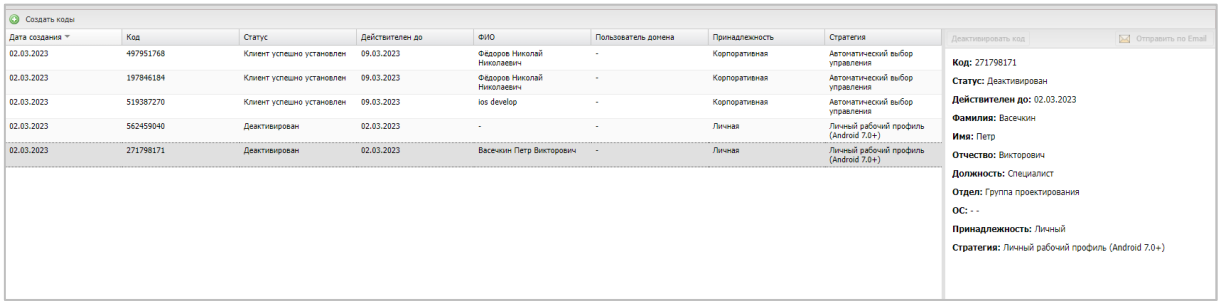


Рисунок 2.173 - Выбор записи с новым кодом

Во время регистрации Администратор следит за статусом этой операции в столбце **«Статус»**.

В зависимости от статуса кода Администратор может осуществлять следующие действия, выбрав в таблице код приглашения (рисунок 2.174):

- Деактивировать код – действие доступно только кодов со статусом «Новый».

При нажатии кнопки код перестает действовать и получает статус «Деактивирован»;

- Отправить по Email. Только для кодов в статусе «Новый код» и при наличии у сотрудника заполненного Email.

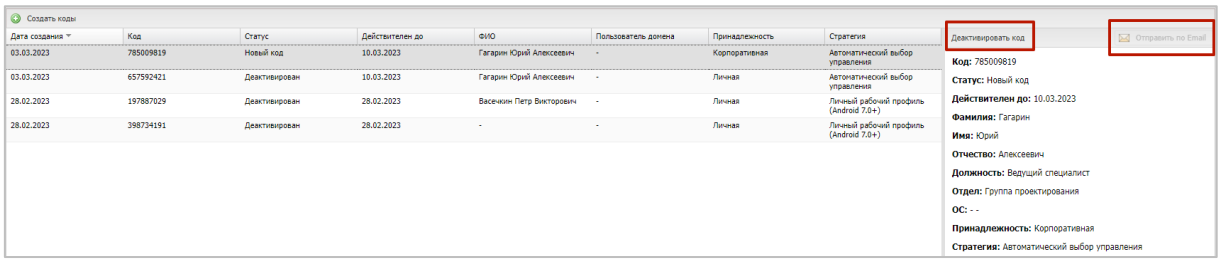


Рисунок 2.174 - Меню «Выбрать действие»

2.11 Корпоративный календарь рабочего времени (пункт меню «Календарь»)

Раздел главного меню **«Календарь»** позволяет создавать и назначать календарь рабочего времени как отдельному сотруднику, так и подразделению, а также настроить правила календаря.

Примечание.
Создание календаря рабочего времени необходимо для определения местоположения сотрудников, которое может производиться только в рабочее время.

При выборе в главном меню раздела **«Календарь»** в левой части открывшегося окна отображается список подразделений организации и их сотрудников, а в правой части окна − календарь рабочего времени выбранного подразделения или сотрудника в соответствии с рисунком 2.175.

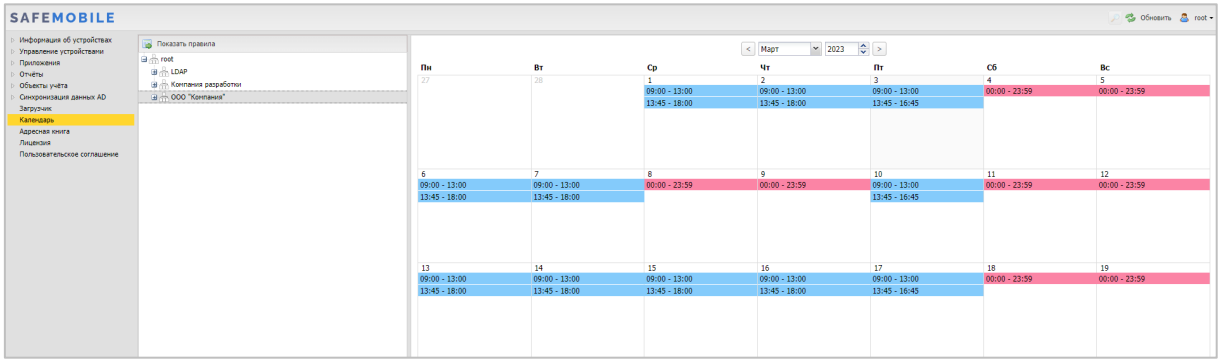


Рисунок 2.175 - Календарь рабочего времени

Для просмотра рабочего времени подразделения или сотрудника в текущем месяце выберите запись о сотруднике или подразделении в таблице слева, после чего в правой части окна отобразится календарь его рабочего времени. Для каждой даты в текущем месяце отображается диапазон рабочего времени (синим цветом) или нерабочее время (красным цветом).

Раскрывающийся список

в верхней части календаря позволяет выбирать требуемый месяц и год.

В системе предусмотрена возможность создания правил для формирования календаря рабочего времени сотрудника, подразделения или организации в целом. Чтобы

открыть окно создания правил и управления ими, нажмите кнопку **«Показать правила»** в верхней части списка сотрудников и кнопку, после чего отобразится окно в соответствии с рисунком 2.176.

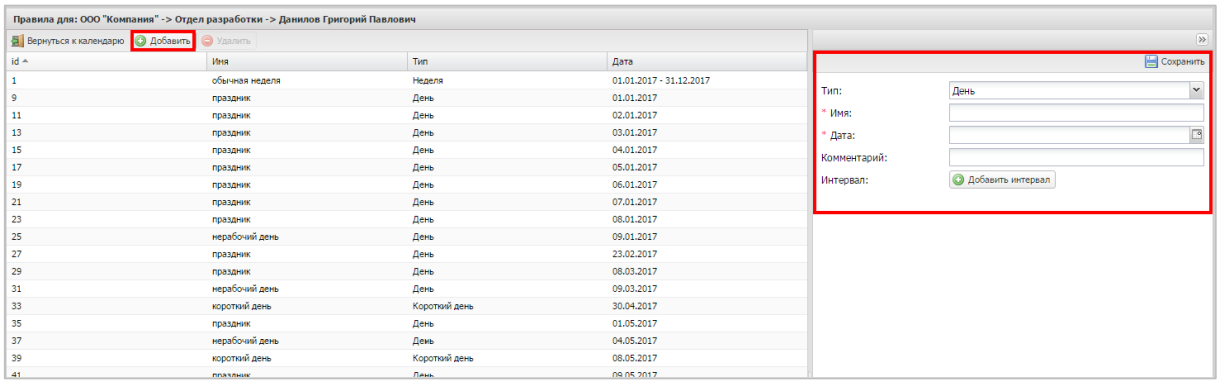


Рисунок 2.176 - Окно создания правил календаря рабочего времени

В левой части открывшегося окна расположена таблица, отображающая список правил, имеющихся в системе для выбранного сотрудника или подразделения. Для просмотра параметров правила выберите строку с правилом в таблице, после чего в правой части окна отобразятся параметры этого правила (рисунок 2.177).

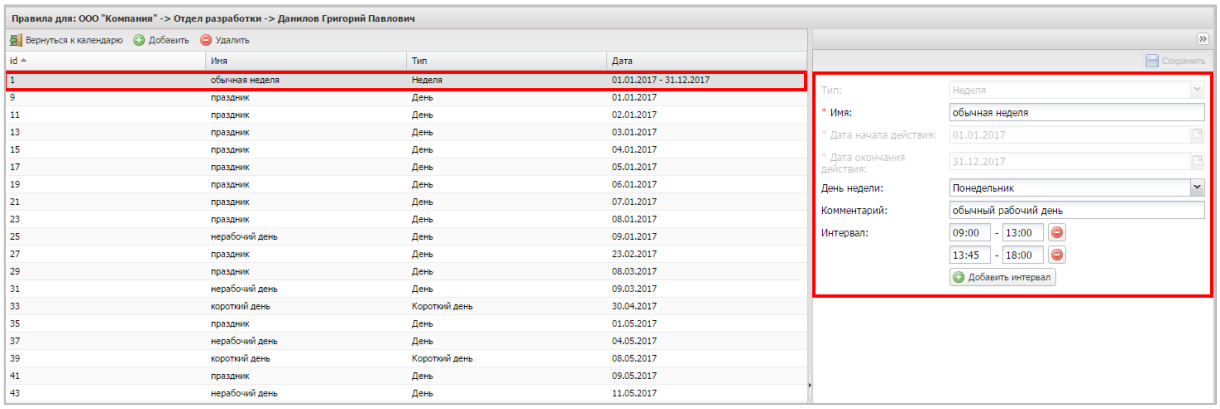


Рисунок 2.177 - Просмотр правила календаря рабочего времени

В системе предусмотрены три типа правил для формирования календаря рабочего времени:

Неделя (регулярное правило) – правила рабочей недели, которые нужно обязательно указать для всех семи дней недели (последовательно выбирая день и указывая для него интервалы рабочего времени). Такой тип правил применяется для быстрого указания рабочего времени для большого промежутка времени, например, года.

День (нерегулярное правило) – правила для конкретной даты или диапазона дат. Такой тип правил применяется для указания интервала рабочего времени, отличного от

заданного при помощи регулярного правила. Например, когда необходимо обозначить в календаре время командировки, отпуска и т.д.

Короткий день (нерегулярное правило) – при применении этого правила для конкретной даты последний интервал рабочего времени сокращается на один час. Создание правил сокращенного дня для диапазона дат недоступно. Такой тип правил применяется для обозначения в календаре предпраздничных дней на конкретные даты.

Для каждого дня правила можно задать до четырёх интервалов рабочего времени.

Каждое правило имеет срок действия:

- для нерегулярных правил срок действия составляет один год, в рамках которого они заданы (от 01 января по 31 декабря);
- регулярные правила требуют явного указания даты начала и даты окончания действия.

Правила календаря рабочего времени применяются в следующей последовательности:

1. Правила рабочего времени применяются в соответствии с организационно-штатной структурой (ОШС) предприятия. Первыми применяются правила компаний (корневых узлов дерева ОШС). Затем последовательно накладываются правила подразделений. Последними применяются правила конкретных сотрудников.
2. При наличии нескольких правил для компании/подразделения/сотрудника, они применяются в соответствии со временем их добавления. Последние добавленные правила применяются последними.
3. Сначала применяются регулярные правила, затем – нерегулярные. То есть правила сотрудника применяются следующим образом:

регулярные правила всех вышестоящих узлов ОШС, начиная с подразделения, в котором работает сотрудник (от старших к младшим);

регулярные правила сотрудника;

нерегулярные правила ОШС;

нерегулярные правила сотрудника.

4. В процессе применения правил происходит их замещение. При этом одно правило замещает другое для каждой конкретной даты, а не для всего диапазона действия.

2.11.1 Создание правил

При создании правил необходимо указать к какому узлу ОШС (компания, подразделение) или сотруднику они относятся. Для этого нужно выбрать необходимый элемент в окне календаря.

Чтобы начать создание правила, нажмите кнопку **«Добавить»** в верхней панели инструментов, после чего в правой части окна отобразятся поля, предназначенные для заполнения в соответствии с рисунком 2.178. Целесообразно начинать создание правил для организации с создания недельного правила для корневого подразделения ОШС (головного подразделения организации), а затем можно создавать нерегулярные правила, приоритет которых выше.

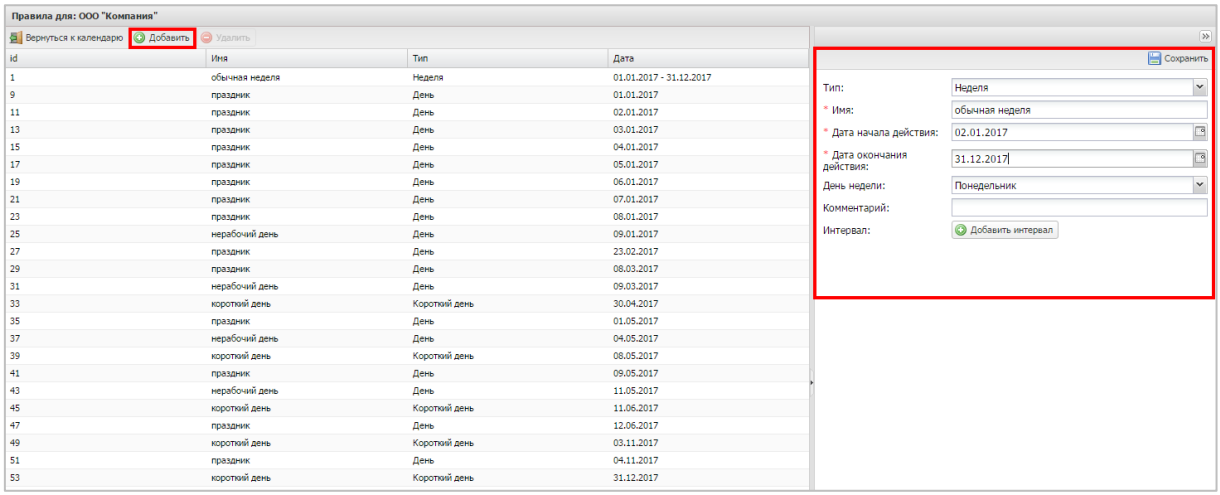


Рисунок 2.178 - Создание правила календаря рабочего времени типа «Неделя»

Для создания правила типа **«Неделя»** необходимо указать следующие обязательные параметры:

- Имя – наименование правила;
- Дата начала действия – выбрать в раскрывающемся календаре дату начала действия правила, например, день начала календарного года в организации;
- Дата окончания действия – выбрать в раскрывающемся календаре дату окончания действия правила, например, последний день календарного года в организации.

После указания и сохранения обязательных параметров правил календаря типа **«Неделя»** все дни указанного диапазона дат будут считаться выходными. Чтобы добавить рабочие дни в календарь, необходимо в раскрывающемся списке **«День недели»** выбрать дни недели, которые будут рабочими (обычно это **Понедельник**, **Вторник**,

Среда, **Четверг** и **Пятница**), и указать для каждого рабочего дня промежуток рабочего времени, например, с 10:00 до 19:00. Для добавления интервала времени используется кнопка **«Добавить интервал»**, после нажатия которой необходимо заполнить поля начала рабочего дня и его окончания. Для корректного заполнения этих полей время необходимо вводить в формате **«ЧЧ: ММ»**, при этом часы должны быть в диапазоне от 00 до 23, минуты – от 00 до 59. Разделитель часов и минут – символ двоеточия. Для удаления неиспользуемого диапазона времени используется кнопка .

При создании правила календаря можно добавить комментарий к нему. После завершения создания правила календаря его необходимо сохранить, нажав кнопку **«Сохранить»** в верхней панели инструментов.

При создании правила типа **«День»** (рисунок 2.179) необходимо указать следующие обязательные параметры:

- Имя – наименование правила;
- Дата – дата, к которой будет привязано правило.

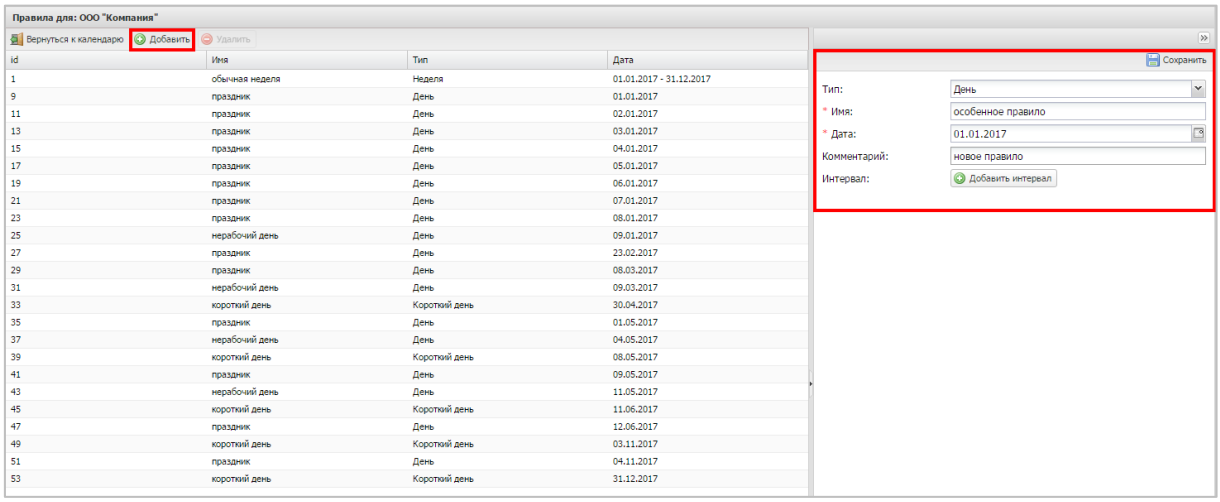


Рисунок 2.179 - Создание правила календаря рабочего времени типа «День»

Кроме того, можно записать комментарий в соответствующем поле и выбрать интервал времени (или несколько интервалов) в течение дня, когда будет действовать создаваемое правило.

Затем можно выбрать интервал времени (заполнив поле **«Интервал»**), если требуется указать в качестве нерабочего времени только часть дня.

Такой тип правил применяется для указания интервала рабочего времени, отличного от заданного при помощи регулярного правила (типа **«Неделя»**). Например, когда необходимо обозначить в календаре время командировки, отпуска и т.д.

Для создания правила типа **«Короткий день»** (рисунок 2.180) необходимо указать следующие обязательные параметры:

- Имя – название создаваемого правила;
- Дата – дата, к которой будет привязано правило.

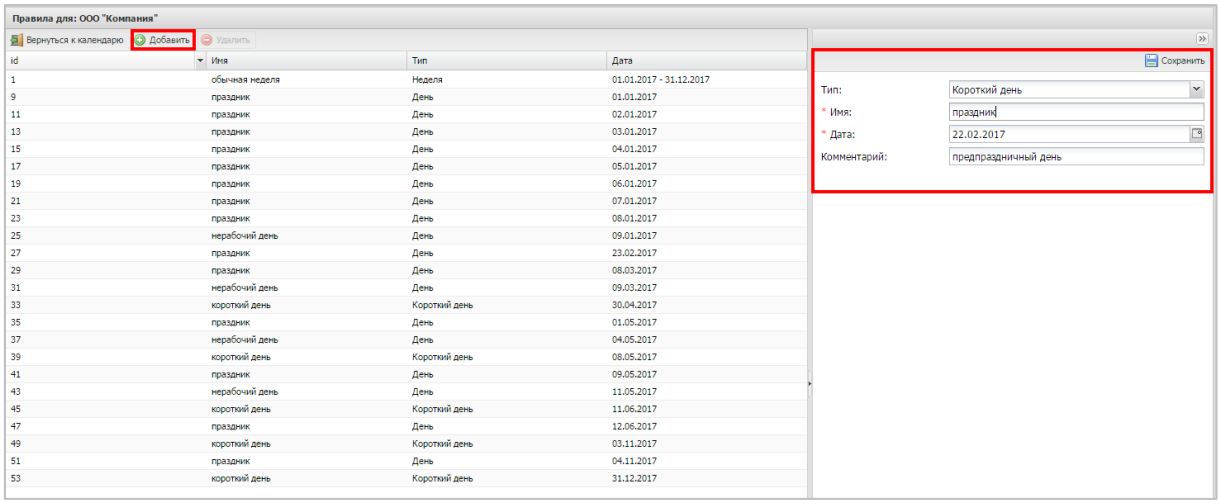


Рисунок 2.180 - Создание правила календаря рабочего времени типа «Короткий день»

Такой тип правил календаря позволяет указать в календаре дни, у которых последний интервал рабочего времени сокращён на один час.

Для сохранения созданного правила, нажмите кнопку **«Сохранить»**.

2.11.2 Изменение правил

После создания правил с ними можно совершать следующие действия:

- изменить временной интервал;
- добавить новый интервал;
- удалить интервал;
- изменить наименование;
- добавить или изменить комментарий.

Примечание.
Изменение правила приводит к его изменению в течение всего срока действия, независимо от даты внесения изменений. История изменений правил не поддерживается. Если изменить правило на третий день его действия, то для дней, в течение которых действовало неизменённое правило, будет отображаться правило с внесёнными изменениями. Тип правила и срок действия правила изменять после создания нельзя.

2.11.3 Удаление правила

Удаление правила приводит к удалению связи между правилом и элементом, к которому оно относится (компания/подразделение/сотрудник). Само правило при этом не удаляется.

Чтобы удалить выбранное правило календаря, нажмите кнопку **«Удалить»** в верхней панели инструментов в соответствии с рисунком 2.181.

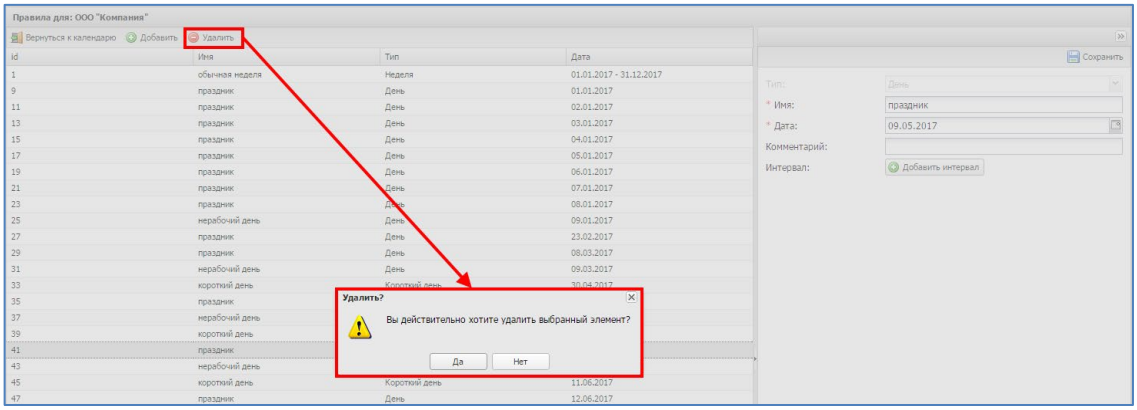


Рисунок 2.181 - Удаление правила календаря рабочего времени

После этого подтвердите действие, нажав **«Да»** в появившемся окне.

2.12 Контроль за лицензией на «UEM SafeMobile» (пункт меню «Лицензия»)

Пункт главного меню **«Лицензия»** предназначен для активации лицензии на использование системы и формирования отчета по числу подключенных устройств (см. 2.13.1).

Для активации лицензии необходимо информацию из полученного лицензионного файла поместить в поле окна **«Лицензия»** (рисунок 2.182), которое является обязательным для заполнения. Затем нажать кнопку **«Сохранить»**.

Рисунок 2.182 - Окно «Лицензия»

После проверки системой, при успешной загрузке лицензии, внизу интерфейса отобразится информация, например, «Лицензия для ООО «Кантор» на 100 устройств(а), использовано 10, действует с 30.10.2017 по 30.12.2018».

В случае нарушений условий лицензии или ее отсутствии интерфейс всех администраторов АРМ будет ограничен разделом «Лицензия», а внизу интерфейса отобразится предупреждающее сообщение красного цвета. Текст сообщения, в зависимости от предупреждения, может быть следующим (название юридического лица приведено условно):

−Отсутствует лицензия на использование системы. Для получения лицензии следует обратиться к поставщику;

−Лицензия для ООО «Кантор» действует с 30.10.2020 (в случае, если срок действия лицензии еще не наступил);

−Лицензия для ООО «Кантор» истекла 30.10.2019. Для продления лицензии обратитесь к поставщику.

Когда число подключенных комплектов достигнет числа комплектов в лицензии, подключение новых МСК будет блокироваться.

Когда до истечения срока действия лицензии остается 1 месяц, внизу интерфейса отобразится предупреждающее сообщение красного цвета: «Заканчивается срок действия лицензии, через 29 дней доступ в АРМ будет заблокирован».

Для обновления истекшей лицензии на лицензию с меньшим количеством устройств необходимо, чтобы на момент активации лицензии количество подключенных устройств не нарушало новое лицензионное соглашение. Если подключенных устройств будет больше, чем в лицензии, новая лицензия активирована не будет. Для активации лицензии необходимо отключить от управления избыточные комплекты.

2.12.1 Отчет по подключенным устройствам

Чтобы сформировать отчет о подключенных устройствах необходимо выполнить следующие действия:

1. В разделе «Лицензии» нажать кнопку «Отчет», после чего откроется диалоговое окно указания периода, за который следует сформировать отчет (рисунок 2.183);

Рисунок 2.183 - Расположение кнопки «Отчет»

2. Указать даты начала и конца периода и нажать кнопку «Выгрузить» (рисунок 2.184);

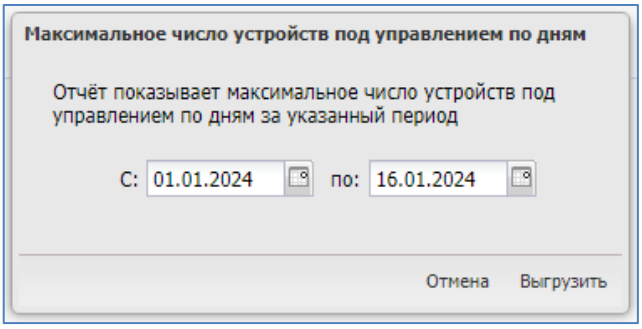


Рисунок 2.184 - Диалоговое окно указания периода формирования отчета

3. Дождаться сообщения о готовности файла и нажать кнопку «Скачать».

Отчет представлен в виде excel таблицы с вкладками:

- Параметры – сводные данные об отчете;
- Данные – данные о максимальном количестве подключений в день, за указанный период.

Примечание

Отчет не покажет данные в таких случаях как:

- *За период работы версии ниже 8.3.*
  При выгрузке отчета за период работы версии 8.2 для каждой даты подключения в отчете будет указано "нет данных".
- *Устройства бывшие под управлением менее 1 часа не попадут в отчет, если их добавление пришлось с НН:01 по НН:59 (то есть не был совершен запрос со стороны БД).*

2.13 Управление пользовательским соглашением

Пункт главного меню **«Пользовательское соглашение»** предназначен для заключения с пользователем устройства соглашения об условиях управления системой МСК на платформах Android и iOS. Для этого необходимо текст пользовательского соглашения, длиной не более 100000 символов, поместить в поле окна **«Пользовательское соглашение»** (рисунок 2.185), затем установить флажок в строке «Показывать ПС на портале регистрации пользователя» и нажать кнопку **«Сохранить»**. В этом случае предложение о принятии условий пользовательского соглашения отобразится на устройстве пользователя при регистрации МСК в «UEM SafeMobile».

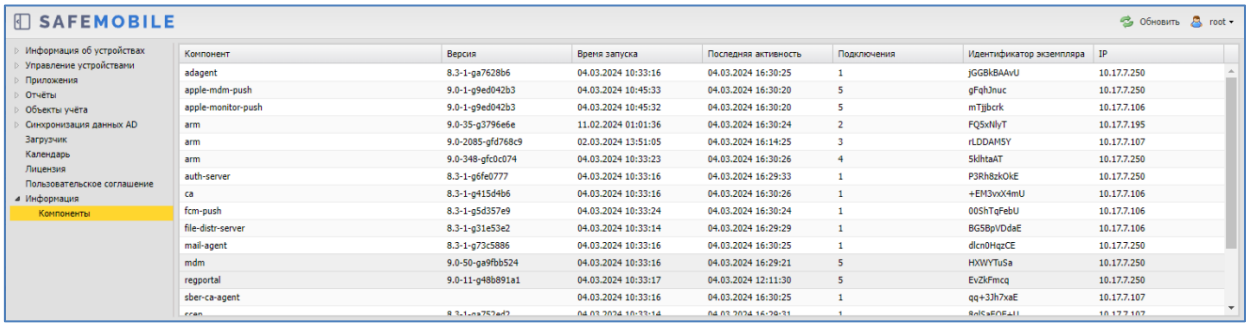
Если МСК уже зарегистрировано в системе или при изменениях в соглашении, после сохранения текста для отправки соглашения на МСК, следует нажать кнопку «**Отправить на устройства**».

Рисунок 2.185 - Окно «Пользовательское соглашение»

2.14 Информация

2.14.1 Компоненты

В данном разделе отображается список подключенных к базе данных компонентов системы. Каждая строка списка отображает данные об одном экземпляре компонента и содержит следующие данные (рисунок 2.186):



Компонент	Версия	Время запуска	Последняя активность	Подключения	Идентификатор экземпляра	IP
adagent	8.3-1-ga7628b6	04.03.2024 10:33:16	04.03.2024 16:30:25	1	jGGBkBAAvU	10.17.7.250
apple-mdm-push	9.0-1-g9ed042b3	04.03.2024 10:45:33	04.03.2024 16:30:20	5	gFqhJnuc	10.17.7.250
apple-monitor-push	9.0-1-g9ed042b3	04.03.2024 10:45:32	04.03.2024 16:30:20	5	mTjjbcrk	10.17.7.106
arm	9.0-35-g3796e6e	11.02.2024 01:01:36	04.03.2024 16:30:24	2	FQSxNlyT	10.17.7.195
arm	9.0-2085-gfd768c9	02.03.2024 13:51:05	04.03.2024 16:14:25	3	rLDDAM5Y	10.17.7.107
arm	9.0-348-gfc0c074	04.03.2024 10:33:23	04.03.2024 16:30:26	4	5kIhtaAT	10.17.7.250
auth-server	8.3-1-g6fe0777	04.03.2024 10:33:16	04.03.2024 16:29:33	1	P3Rh8zkOkE	10.17.7.250
ca	8.3-1-g415d4b6	04.03.2024 10:33:16	04.03.2024 16:30:26	1	+EM3vxX4mU	10.17.7.106
fcm-push	8.3-1-g5d357e9	04.03.2024 10:33:24	04.03.2024 16:30:24	1	00ShTqFebU	10.17.7.106
file-distr-server	8.3-1-g31e53e2	04.03.2024 10:33:14	04.03.2024 16:29:29	1	BG5BpVDdaE	10.17.7.106
mail-agent	8.3-1-g73c5886	04.03.2024 10:33:16	04.03.2024 16:30:25	1	dlcn0HqzCE	10.17.7.250
mdm	9.0-50-ga9fbb524	04.03.2024 10:33:16	04.03.2024 16:29:21	5	HXWYTuSa	10.17.7.250
regportal	9.0-11-g48b891a1	04.03.2024 10:33:17	04.03.2024 12:11:30	5	EvZkFmcq	10.17.7.250
sber-ca-agent		04.03.2024 10:33:16	04.03.2024 16:30:25	1	qq+3Jh7xaE	10.17.7.107

Рисунок 2.186 - Подключенные компоненты

- Компонент – название компонента:
    - adagent - Агент синхронизхации с контроллером домена AD;
    - apple-mdm-push - Сервис отправки пуш уведомлений клиенту MDM iOS;
    - arm - Консоль управления администратора;
    - auth-server - Сервер аутентификации (нужен для mTLS в SS);
    - ca - Сервис УЦ SafeMobile;
    - fcm-push - Сервис отправки пуш уведомлений FCM (Android);
    - file-distr-server - Сервер раздачи корпоративных приложения и файлов;
    - mdm - Сервер управления (Android, iOS, Windows и АврораОС);
    - apple-monitor-push - Сервис отправки пуш уведомлений монитору;
    - lmsrv - Сервер управления (Linux);
    - mail-agent - Сервис отправки почты;
    - nginx
    - regportal - Портал саморегистрации устройств;
    - sber-ca-agent - Сервис подключения к корпоративному УЦ (SberCA);
    - scep - Сервер SCEP (устанавливается вместе с MDM и спользует те же порты;
    - scep-standalone - Сервер SCEP (устанавливается отдельно оставлен для совместимости с прежними установками SCEP);
    - scheduler - Планировщик (периодическая очисткка);
    - sesl - Сервис отправки системных логов;

  - smapi - Сервер публичного API;
  - socket-server - Сервер команд (Android);
  - winmdm - Сервер управления (Windows);
  - scim - Сервер SCIM.

- Время запуска – дата и время запуска экземпляра компонента;
- Последняя активность – дата и время последних действий экземпляра компонента;
- Подключения – количество подключений одного экземпляра компонента;
- Идентификатор экземпляра – уникальный ID экземпляра. Идентификатор генерируется при каждом старте экземпляра компонента;
- IP – IP адрес экземпляра.

Примечание.

1. Если время работы компонента меньше 1 минуты, то допустимо кратковременное отсутствие компонента в списке. Если, при этом, время старта не меняется, то контейнер не перезагружался и проблем в соединении с БД у контейнера нет.

2. Компоненты обслуживания windows и linux не отображаются.

2.15 Очистка данных в «UEM SafeMobile»

Система предоставляет возможность выполнять автоматическую очистку базы данных, что позволяет не хранить в базе данных записи об устаревших событиях, произошедших в системе.

Сценарий очистки запускается ежедневно и удаляет из БД журнальные записи, после создания которых прошло более 183 суток. Очистке подлежат следующие данные:

- Журнал событий МСК;
- Журнал отправленных на МСК команд;
- Журнал координат МСК.

2.16 Завершение работы в «UEM SafeMobile»

Для завершения сеанса работы пользователя с АРМ Администратора SafeMobile следует нажать кнопку **«Выход»** в верхней правой части основного окна. При этом происходит переход к окну аутентификации в соответствии с п. 2.1.

3 Частые вопросы

Вопрос 1:

Что делать, если при загрузке АРМ в браузере Firefox появляется окно: *«Внимание: сценарий не отвечает»,* содержащее следующее сообщение *«Похоже, исполняемый на этой странице сценарий занят или не отвечает. Вы можете остановить его сейчас или продолжить и посмотреть, сможет ли он завершить свою работу».*

Ответ:

Для продолжения работы необходимо в настройках браузера Firefox увеличить значение параметра **dom.max_script_run_time**. Для этого следует выполнить действия:

1. В адресной строке наберать **about:config** и нажать на клавиатуре клавишу «Enter».
2. Может появиться страница предупреждения:

   about:config «**Будьте осторожны, а то лишитесь гарантии!**».

   Нажать кнопку «**Я обещаю, что буду осторожен!**», чтобы перейти на страницу **about:config.**

3. На странице **about:config** найти настройку **dom.max_script_run_time** и дважды нажать на нее.
4. Увеличьте исходное значение.
5. Нажать OK.

Вопрос 2:

Что делать, если при смене пароля после успешной аутентификации появляется окно **Подтверждение смены пароля** с выбором пользователя (рисунок 3.1).

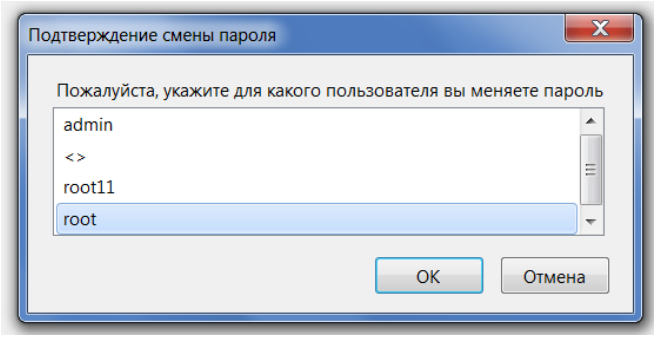


Рисунок 3.1 - Окно подтверждения смены пароля

Ответ:

Отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox (рисунок 3.2).

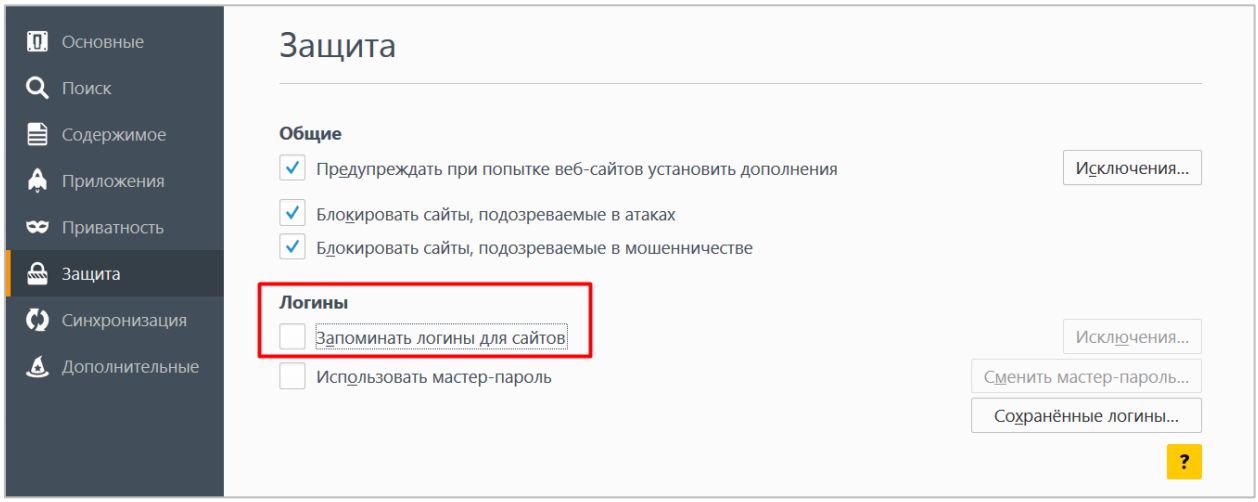


Рисунок 3.2 - Настройка отмены автозаполнения логина и пароля в браузере Firefox

Вопрос 3:

Что делать, если при открытии раздела главного меню «Администраторы» поле логин и пароль заполнено логином и паролем, сохраненным в окне аутентификации (рисунок 3.3)?

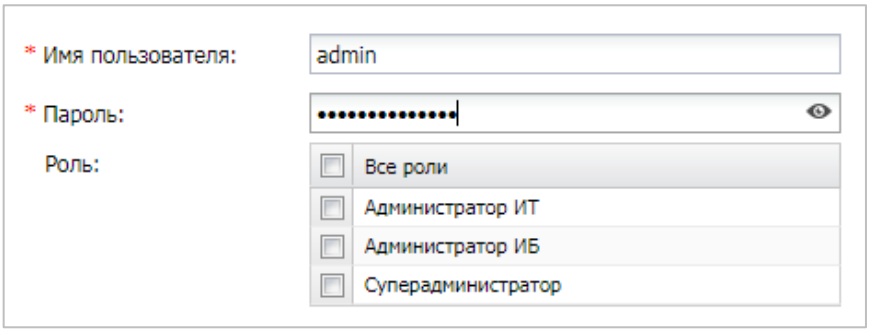


Рисунок 3.3 - Автозаполнение пароля и логина в окне управления «Администраторы»

Ответ:

Отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox (рисунок 3.4).

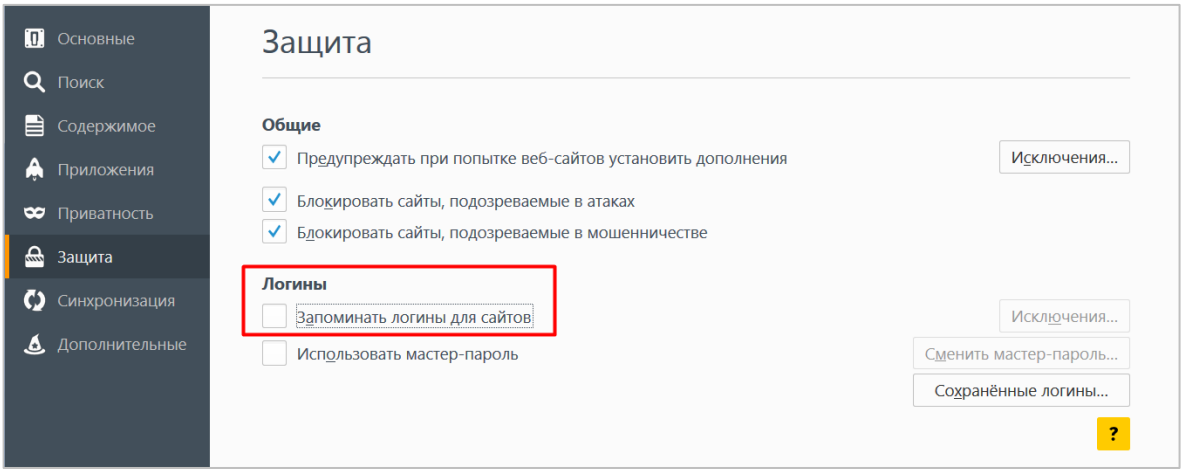


Рисунок 3.4 - Настройка отмены автозаполнения логина и пароля в браузере Firefox

Приложение А
Установка МСК на платформе iOS в режим Supervised

Перевод МСК на платформе iOS в режим Supervised с установкой требуемых параметров и ограничений для осуществления контроля над устройством, следует выполнять в соответствии со следующим регламентом:

1. Скачать и запустить ПО Apple Configurator 2.

2. Подключить iPhone (iPad) к ПК Mac.

3. Выбрать подключенное МСК и нажать кнопку **«Prepare»** (подготовить) в соответствии с рисунком А.1.

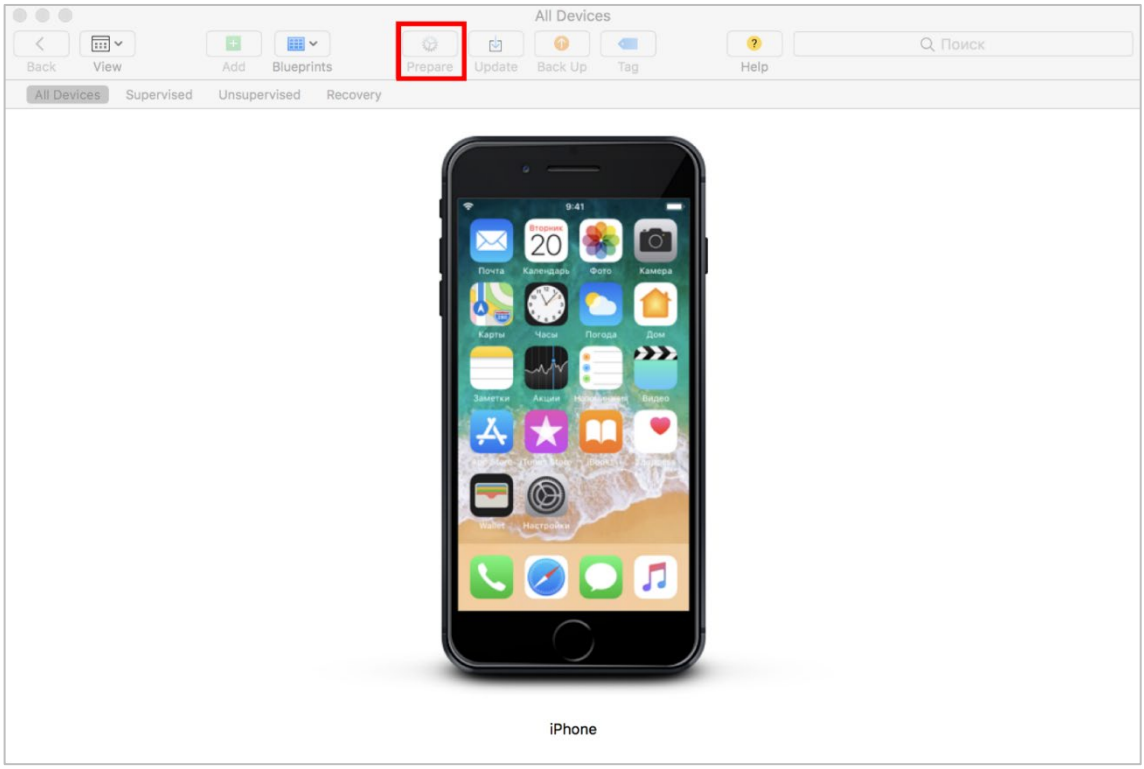


Рисунок А.1 - Окно подключенных устройств

4. В поле **«Prepare with»** в соответствии с рисунком А.2 выбрать значение по умолчанию **«Manual Configuration»** (установка конфигурации вручную). Для получения доступа к правам супервайзера поставить галочку напротив пунктов **«Supervise devices»** (контролировать устройства) и **«Allow devices to pair with other computers»** (разрешить устройствам соединяться с другими компьютерами), затем нажать кнопку **«Next»**. При необходимости возврата в предыдущее меню следует нажать на кнопку **«Previous»**.

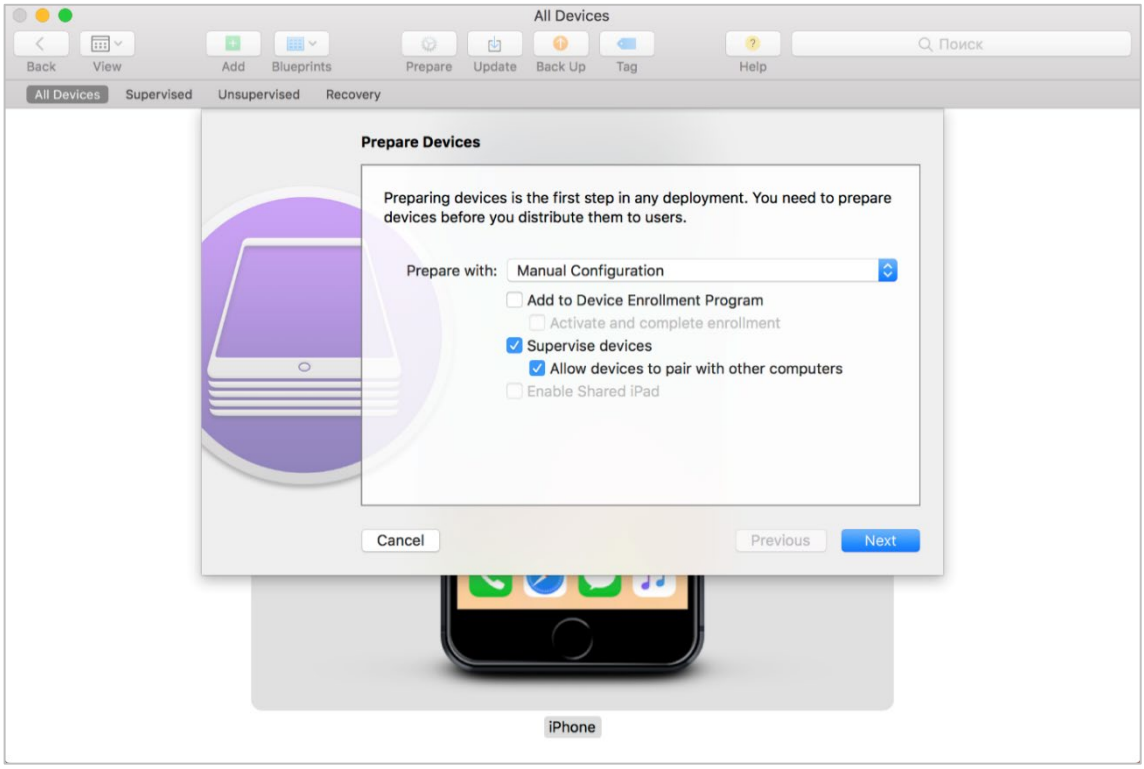


Рисунок А.2 - Выбор режима подготовки устройства

5. В поле **«Server»** (рисунок А.3) выбрать значение **«Do not enroll in MDM»** (не регистрироваться в MDM) и нажать кнопку **«Next»**.

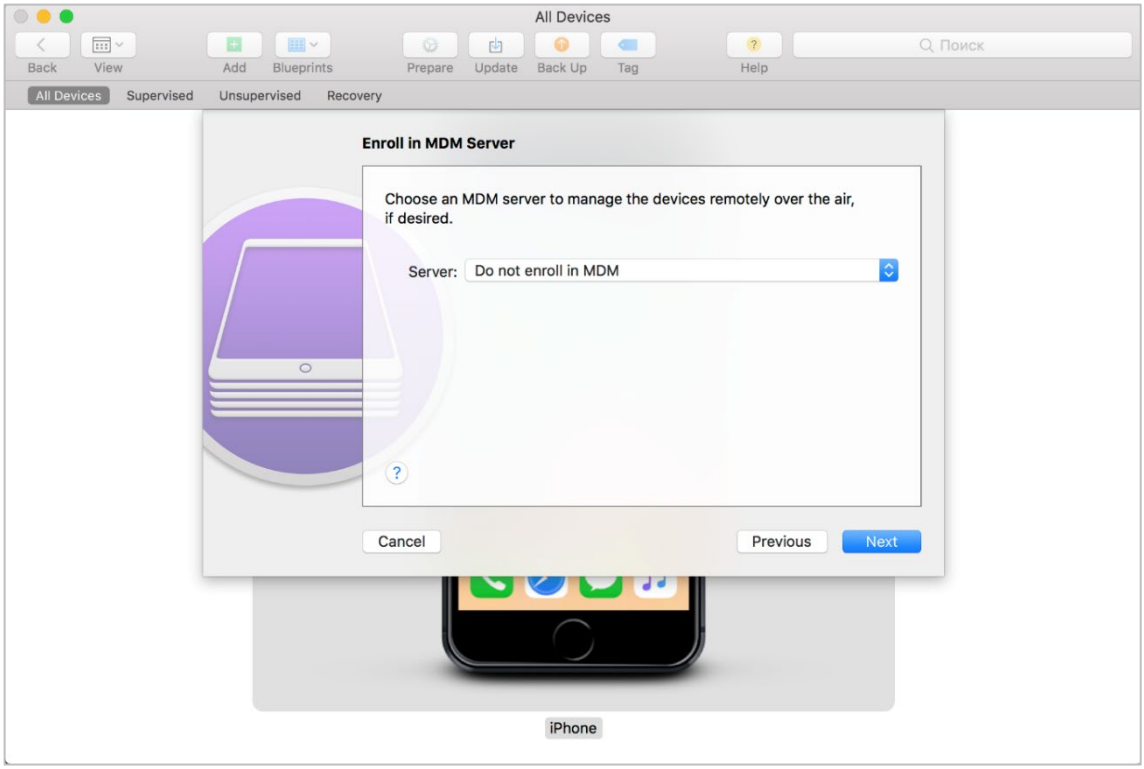


Рисунок А.3 - Выбор MDM сервера

6. Нажать кнопку **«Skip»** (рисунок А 4);

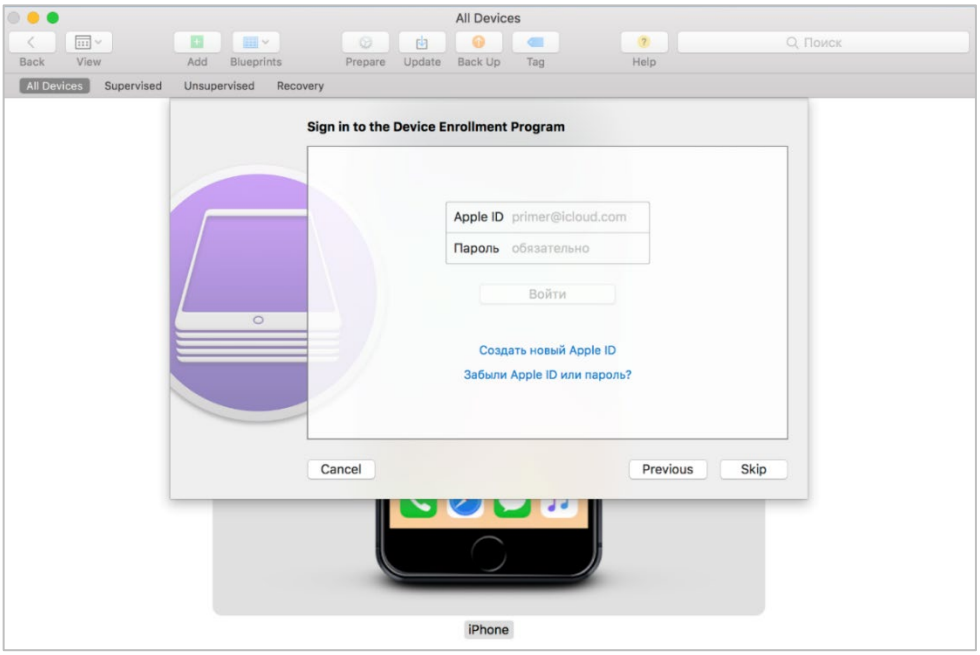


Рисунок А.4 - Аутентификация в ADEP

7. В поле **«Name»** (рисунок А.5) следует указать название организации, остальные поля можно оставить пустыми и нажать **«Next»**.

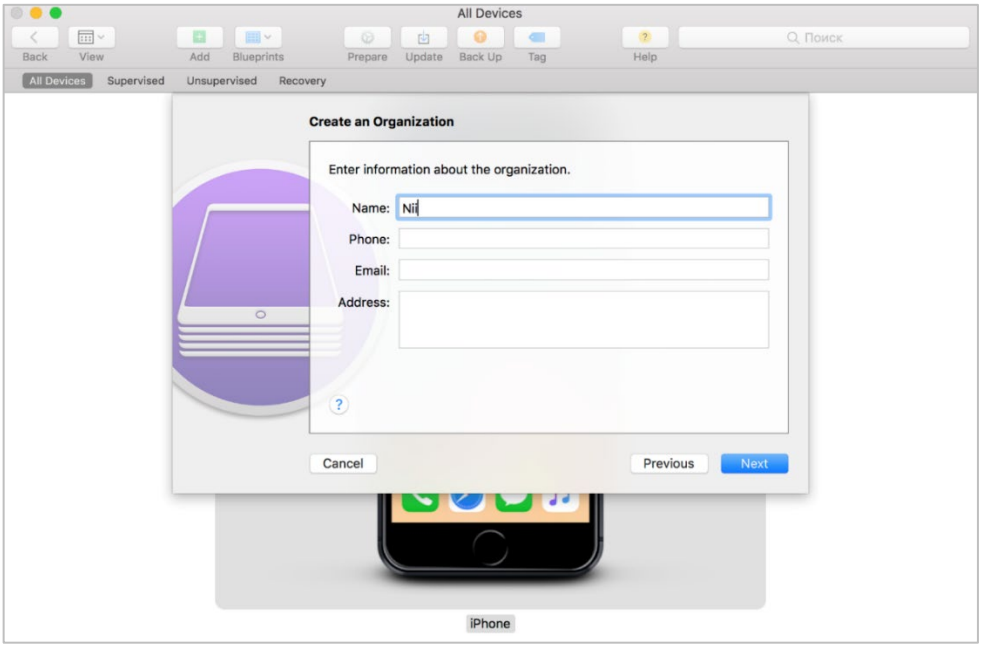


Рисунок А.5 - Создание записи о контролирующей организации

8. Если перевод в режим supervision осуществляется в первый раз, следует выбрать пункт **«Generate a new supervision identity»** (создать новый supervision-идентификатор) в соответствии с рисунком А.6, в противном случае выбрать пункт **«Choose an existing supervision identity»** (выберите существующий supervision-

идентификатор). Далее нажать **«Next»**.

Рисунок А.6 - Выбор supervision-идентификатора

9. В поле **«Setup Assistant»** (рисунок А.7) выбрать значение **«Show all steps»** (показать все шаги). В этом случае все указанные параметры первоначальной конфигурации МСК будут доступны для настройки пользователю после перепрошивки устройства. Далее нажать **«Prepare»**.

> ***Примечание***
>
> *Подробную информацию по настройке параметров конфигурации устройства посредством ПО Apple Configurator 2 можно получить на сайте производителя устройства на платформе iOS (apple.com).*

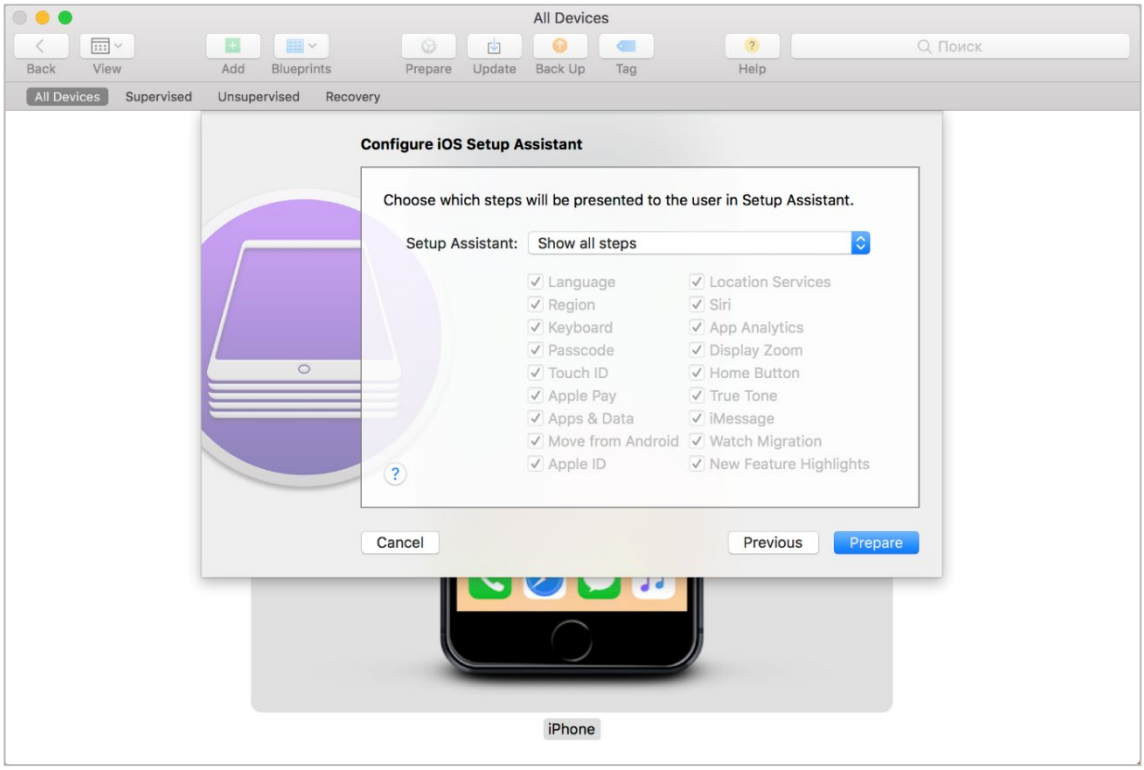


Рисунок А.7 - Выбор параметров первоначальной конфигурации МСК

Затем запустится процесс перепрошивки МСК и подготовки в соответствии с заданными параметрами конфигурации (рисунок А.8). МСК в ПО Apple Configurator 2 отобразится в разделе **«Supervised»**.

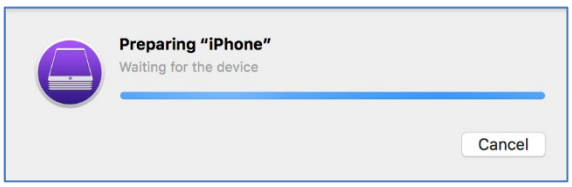


Рисунок А.8 - Индикация процесса подготовки устройства

ВНИМАНИЕ!

Подготовка устройства может занять несколько минут. Попытка остановить или отменить процесс установки iOS после ее запуска или закрытие ПО Apple Configurator 2 может повредить устройство.

10. На МСК после перепрошивки и завершения настройки конфигурации в

приложении **«Настройки»** отобразится сообщение об осуществлении контроля над устройством в соответствии с рисунком А.9.

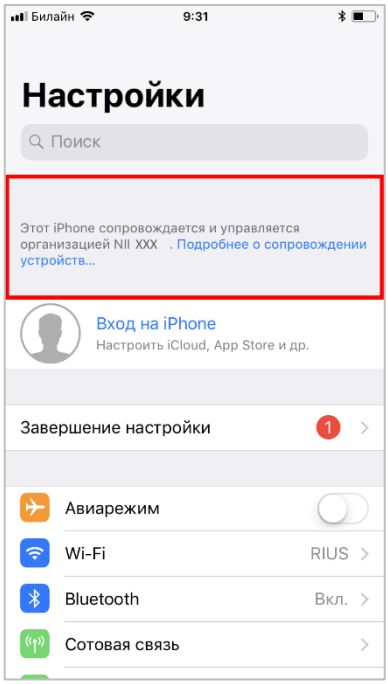


Рисунок А.9 - Сообщение о контроле над устройством в приложении «Настройки»

11. Для отмены контроля над устройством следует выполнить действия в соответствии с регламентом, но при выборе режима в п. А.4 снять галочку напротив пункта **«Supervise devices»** и продолжить подготовку устройства.

Приложение Б
Перечень возможных ошибок при выполнении команд Администраторов

Результат	Описание ошибки	Действие Администратора
Ошибка в ходе обработки ответа на команду	Ошибка обработки пакета клиента сервером	Повторно отправить команду
Команда была выдана на устройство, после чего устройство отключилось	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Нарушение защиты ОС	Устройство получило команду, выполнение которой опасно для ОС	Действие не требуется
Данные, полученные от сервера SafeMobile, искажены (дистрибутив приложения)	Ошибка в ходе передачи пакета от сервера клиенту	Повторно отправить команду
Приложение уже установлено (или запущено)	Попытка установки уже установленного приложения	Действие не требуется
Недопустимое значение параметра команды	Параметр команды не поддерживается. При использовании GPRS точки доступа на МСК iOS	Изменить параметр команды и отправить команду повторно. Параметры команд приведены в п.2.6.6
Неизвестная ошибка	Ошибка в ходе выполнения команды	Повторно отправить команду

Результат	Описание ошибки	Действие Администратора
Сокет закрыт другой стороной	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Истекло время ожидания ответа	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Истекло количество попыток повторного доведения	Потеря соединения	Повторно отправить команду
Получен недействительный набор записей	Неверный параметр команды	Изменить параметр команды и отправить команду повторно
Пустой список точек доступа	В системе нет точек доступа, привязанных к комплекту	1) Создать одну или несколько точек доступа (раздел «Объекты учета/Точка доступа»); 2) Привязать точки доступа к комплекту на экранной форме комплекта (раздел «Объекты учета/Комплект»); 3) Повторно отправить команду

Приложение В
Приложения для мобильных устройств iOS

Данная информация была взята из сетевой документации производителя устройств iOS.

App	iOS Bundle ID
Activity	com.apple.Fitness
App Store	com.apple.AppStore
Books	com.apple.iBooks
Calculator	com.apple.calculator
Calendar	com.apple.mobilecal
Camera	com.apple.camera
Clock	com.apple.mobiletimer
Compass	com.apple.compass
Contacts	com.apple.MobileAddressBook

FaceTime	com.apple.facetime
Files	com.apple.DocumentsApp
Find Friends	com.apple.mobileme.fmf1
Find iPhone	com.apple.mobileme.fmip1
Health	com.apple.Health
Home	com.apple.Home
iCloud Drive	com.apple.iCloudDriveApp
iTunes Store	com.apple.MobileStore
Mail	com.apple.mobilemail
Maps	com.apple.Maps
Measure	com.apple.measure
Messages	com.apple.MobileSMS

Music	com.apple.Music
News	com.apple.news
Notes	com.apple.mobilenotes
Phone	com.apple.mobilephone
Photo Booth	com.apple.Photo-Booth
Photos	com.apple.mobileslideshow
Podcasts	com.apple.podcasts
Reminders	com.apple.reminders
Safari	com.apple.mobilesafari
Settings	com.apple.Preferences
Stocks	com.apple.stocks

Tips	com.apple.tips
TV	com.apple.tv
Videos	com.apple.videos
Voice Memos	com.apple.VoiceMemos
Wallet	com.apple.Passbook
Watch	com.apple.Bridge
Weather	com.apple.weather

Приложение Г
Состав полномочий предустановленных ролей

Роль	Назначенные полномочия
Администратор ИБ	1. «Информация об устройствах»: «Действия» (просмотр и отмена команд). 2. «Информация об устройствах»: «Данные об устройстве» 3. «Приложения / Установленные приложения: «Просмотр установленных на устройстве приложений», «Запрос списка установленных на устройстве приложений», «Просмотр установленных в контейнере приложений» 5. Отчёты: «События ИБ», «Аудит»
Администратор ИТ	Все полномочия, кроме: отчётов «События ИБ» и «Аудит», разделов «Лицензия», «Пользовательское соглашение», "Информация", "Синхронизация данных AD"
Суперадминистратор	Все полномочия

Приложение Д
Подготовка устройства Windows для установки МСК

Назначение и условие применения

Для регистрации МСК в системе необходимо, чтобы на МСК была установлена и активирована ОС Windows 10 версии не ниже 1703 в редакции Pro или Enterprise.

Для гарантированного уничтожения данных (в случае утраты устройства) необходимо, чтобы на всех несъемных накопителях МСК было включено шифрование данных посредством встроенного компонента BitLocker.

МСК не должно быть присоединено к домену Active Directory.

Для обеспечения возможности сброса к заводским настройкам должна быть включена среда восстановления (Windows Recovery Environment). Чтобы проверить состояние среды восстановления нужно запустить из-под учетной записи администратора консоль и выполнить команду: reagentc /info.

```
PS C:\WINDOWS\system32> reagentc /info
Информация о конфигурации среды восстановления Windows и
сброса системы:

    Состояние среды восстановления Windows:         Enabled
    Расположение среды восстановления Windows:       \\?\GLOBALROOT\device\harddisk2\partition1\Recovery\WindowsRE
    Идентификатор данных конфигурации загрузки: 40cc6258-1bdd-11ec-9dca-a0510bbcd256
    Расположение образа для восстановления:
    Индекс образа для восстановления:      0
    Расположение пользовательского образа:
    Индекс пользовательского образа:          0

REAGENTC.EXE: операция выполнена успешно.

PS C:\WINDOWS\system32>
```

Если среда восстановления выключена, то необходимо выполнить команду: reagentc /enable.

Эксплуатация устройства должна выполнятся из-под учетной записи с ограниченными правами.

Подготовка к работе

Перед началом работы пользователю необходимо проверить корректность значений даты, времени и часового пояса на МСК. Если эти параметры установлены неверно, следует выключить на МСК автоматическое определение даты и времени, предоставляемое сетью, и осуществить настройку вручную.

Проверить наличие обновлений. Последние обновления ОС должны быть установлены и выполнена перезагрузка устройства.

Для того, чтобы на МСК, после подключения к Системе, имелась возможность установки публичных приложений, сотруднику необходимо аутентифицироваться в магазине публичных приложений Microsoft Store.

Приложение E
Основные сценарии работы с системой

Первоначальная настройка SafeMobile, после инсталляции.

1. Загрузить лицензию;
    a. Заполнить раздел «Подключения к серверам», предварительно, при необходимости, добавив сертификаты в раздел «Серверные сертификаты»;
    b. Создать Роль(и), распределяя функции, доступные админам;
    c. ОШС, сотрудники, администраторы;
        - Если необходим LDAP, настроить «Внешние каталоги» и импортировать: Сотрудников, Администраторов, Группы;
        - Если LDAP не нужен, создать узлы ОШС, Сотрудников, Администраторов, назначая им нужные подразделения;
        - Если необходим KME загрузить список Устройство+Сотрудник в разделе «Комплекты»;
        - Если есть только список сотрудников, загрузить через раздел «Сотрудники»;
2. Загрузить для всех используемых платформ мониторы в раздел Приложения и создать для них правила управления. Назначать рекомендуется на самый верхний узел ОШС, если нет особых условий;
3. Создать «Профили мониторов». Назначать рекомендуется на самый верхний узел ОШС, если нет особых условий;
4. Подключить устройства согласно РП по мобильным клиентам:
    - Если LDAP - доменными учетными данными;
    - Если KME - мастером первоначальной настройки после сброса к заводским настройкам;
    - Если только сотрудники - выписать коды приглашения.

Настройка после обновления сервера SafeMobile.

1. Загрузить для Андроид (Аврора) новые версии мониторов в раздел Приложения;
2. Создать для новой версии монитора тестовое правило управления. Назначить тестовое правило на несколько проверочных устройств;

3. Убедиться, что все проверочные устройства успешно обновили монитор;
4. В основном ПУП монитора изменить версию монитора на новую;
5. Удалить тестовое правило;
6. Проверить «Профили мониторов» на предмет появления новых политик, скорректировать их значения, при необходимости.

Определение местоположений.

1. Проверить наличие профилей для мониторов, необходимых мобильных платформ и настройку в них периода опроса GPS;
2. Для iOS проверить наличие ПУП монитора на целевых устройствах;
3. Настроить график рабочего времени в разделе «Календарь». Правила могут быть созданы, как для подразделений, так и для отдельных сотрудников. Допустимо индивидуально добавлять отпуска и больничные;
4. Если есть уже подключенные устройства, необходимо выполнить для них команду "Установка графика рабочего времени". Вновь подключаемые устройства будут получать «Календарь» автоматически;
5. Раздел «Местоположения» - для отдельных сотрудников. «Перемещения» - для нескольких;
6. При необходимости задать Геозоны и отслеживать вход/выход, либо настраивать их как условия применения в различных сущностях.

Исключающие назначения.

Сущности могут быть назначены на:

- Отдельное устройство,
- Сотрудника,
- Подразделение,
- Узел ОШС целиком.

Для большей гибкости, есть возможность исключить из общего списка назначенных: и отдельное устройство, и сотрудника и подразделение и узел ОШС.

Настройка профилей "Точка доступа WiFi iOS" и "Точка доступа WiFi Android" с корпоративными точками доступа WiFi.

Корпоративные точки доступа могут быть настроены с доступом через:

- Общий пароль.
  "Тип безопасности" = Personal;
- Доменные логин/пароль пользователя.
  "Тип безопасности" = Enterprise, "Тип EAP" = PEAP;
- Сертификат пользователя (группы);
  - Вариант 1
    Выгруженный из УЦ (с приватным ключом). "Тип безопасности" = Enterprise, "Тип EAP" = TLS, "Учётные данные" = сертификат формата PKCS12 из раздела Клиентские сертификаты;
  - Вариант 2
    Полученный по протоколу SCEP (приватный ключ генерируется на устройстве и не покидает его). "Тип безопасности" = Enterprise, "Тип EAP" = TLS, " Учётные данные" = Настройки SCEP.

Для работы по «Вариант 2» должен быть запущен регистрационный агент, заполнен раздел "Настройки SCEP" и настроен пункт "SCEPServer" в разделе "Подключения к серверам". Получаемые по SCEP сертификаты (формата PEM, без приватных ключей), кроме устройств, появляются еще и в разделе "Клиентские сертификаты".

Настройка запрета приложения.

1. Запросить список установленных приложений с устройства;
2. Кнопкой "зарегистрировать" добавить приложение в объекты учёта;
3. Выбрать приложение в «объектах учёта», нажать "создать правило", в правиле указать:
   - "приложение должно быть на устройстве" - "нет" если его необходимо удалить;
   - "приложение должно быть включено" - "нет" если его необходимо спрятать, не удаляя данные;
4. Назначить правило на устройство, сотрудника или узлы ОШС.

Приложение Ж
Поддерживаемые платформы мобильных устройств

В текущей версии система поддерживает работу на устройствах следующих платформ:

- iOS – версии от 11.0 и выше;
- Android – версии от 5.0 и выше;
- Windows – Windows 10 не ниже 1703 в редакции Pro или Enterprise;
- Аврора – версии 4 и выше.

Для работы на устройствах платформ Android и Аврора требуется установка на МСК приложения «Монитор». В зависимости от типа устройства, версии платформы и метода установки приложения будут доступны различные стратегии управления устройством.

Выбор стратегии управления для Android

Стратегия управления устройством зависит от версии операционной системы и способа установки на него приложения «Монитор».

Монитор установлен на устройство как обычное приложение

Стратегия управления	**Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС**				
	Samsung (Android 5-6)	**Samsung (Android 7-11)**	**Samsung (Android 12+)**	**Android 5-6**	**Android 7+**
Личный рабочий профиль	Стратегия не применима	Profile Owner, KNOX	Profile Owner, KNOX	Стратегия не применима	Profile Owner,
Корпоративный рабочий профиль	Стратегия не применима	Стратегия не применима	Стратегия не применима	Стратегия не применима	Стратегия не применима
Только устройство (Android)	Device Admin, KNOX	Device Admin, KNOX	Device Admin, KNOX (*)	Device Admin	Device Admin
Устройство и контейнер KNOX	Device Admin, KNOX	Device Admin, KNOX (**)	Device Admin, KNOX (*,**)	Стратегия не применима	Стратегия не применима

** - пользователю доступно управление частью разрешений монитора.*

*** - начиная с Android 10, knox container доступен на ограниченном наборе устройств.*

Монитор установлен на устройство через NFC

Стратегия управления	Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС	
	Samsung (Android 5.0+)	**Android 5.0+**
Личный рабочий профиль	Стратегия не применима	Стратегия не применима
Корпоративный рабочий профиль	Стратегия не применима	Стратегия не применима
Только устройство (Android)	Device Owner, KNOX (опционально)	Device Owner, System
Устройство и контейнер KNOX	Device Admin, KNOX	Стратегия не применима

Монитор подключается по QR после сброса устройства к заводским настройкам (метод доступен, начиная с Android 7.0)

Стратегия управления	**Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС**	
	Samsung (Android 7-10)	**Android 11+**
Личный рабочий профиль	Стратегия не применима	Стратегия не применима
Корпоративный рабочий профиль	Стратегия не применима	Corporate Profile Owner + KNOX (опционально)
Только устройство (Android)	Device Owner, KNOX (опционально)	Device Owner, KNOX (опционально)
Устройство и контейнер KNOX	Стратегия не применима	Стратегия не применима