

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬ-
НЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ
РУКОВОДСТВО АДМИНИСТРАТОРА

SAFEMOBILE

Москва

2022

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений	5
1 Введение.....	8
2 Описание действий при работе с APM Администратора SafeMobile	9
2.1 Аутентификация в APM Администратора SafeMobile.....	9
2.2 Обзор интерфейса APM Администратора SafeMobile.....	10
2.3 Панель ОШС.....	16
2.4 Главная таблица	17
2.5 Информационная таблица.....	21
2.6 Главное меню.....	22
2.6.1 Отчёт «Информация об устройстве»	24
2.6.2 Раздел «Сообщения».....	27
2.6.3 Раздел «Звонки»	29
2.6.4 Раздел «Местоположения»	32
2.6.5 Раздел «Действия»	35
2.6.6 Раздел «События»	37
2.6.7 Раздел «Команды».....	52
2.6.8 Раздел «Профили»	59
2.6.9 Раздел «Установленные приложения».....	70
2.6.10 Раздел «Правила управления»	72
2.6.11 Раздел «Конфигурации».....	82
2.7 Построение отчётов (пункт меню «Отчёты»).....	89
2.7.1 Отчёт «Аудит»	89
2.7.2 Отчёт «Звонки и SMS»	93

2.7.3	Отчёт «События ИБ».....	93
2.7.4	Отчёт «Перемещения»	94
2.7.5	Отчёт «Профили».....	95
2.7.6	Отчёт «Правила управления»	97
2.7.7	Отчет «Геозоны»	98
2.7.8	Отчет «SafeLife»	99
2.8	Управление объектами учёта (пункт меню «Объекты учёта»)	102
2.8.1	Организационно-штатная структура	103
2.8.2	Сотрудники	105
2.8.3	Роли	108
2.8.4	Администраторы.....	111
2.8.5	Парольные политики APM	113
2.8.6	Операционные системы.....	114
2.8.7	Приложения	116
2.8.8	SIM-карты.....	121
2.8.9	Комплекты.....	122
2.8.10	Геозоны.....	128
2.8.11	Серверные сертификаты	130
2.8.12	Подключения к серверам.....	132
2.8.13	Настройки SCEP.....	137
2.8.14	Клиентские сертификаты	139
2.9	Управление кодами приглашения (пункт меню «Загрузчик»)	141
2.10	Корпоративный календарь рабочего времени (пункт меню «Календарь»).....	146

2.10.1	Создание правил.....	149
2.10.2	Изменение правил.....	152
2.10.3	Удаление правила.....	152
2.11	Управление адресной книгой (пункт меню «Адресная книга»).....	153
2.11.1	Вкладка «Контакты».....	154
2.11.2	Вкладка «Привязки».....	156
2.12	Контроль за лицензией на «UEM SafeMobile» (пункт меню «Лицензия»).....	160
2.13	Управление пользовательским соглашением.....	161
2.14	Очистка данных в «UEM SafeMobile».....	162
2.15	Завершение работы в «UEM SafeMobile».....	162
3	Частые вопросы.....	163
	Приложение А Установка MCK на платформе iOS в режим Supervised.....	165
	Приложение Б Перечень возможных ошибок при выполнении команд Администраторов.....	171
	Приложение В Приложения для мобильных устройств iOS.....	173
	Приложение Г Состав полномочий предустановленных ролей.....	177
	Приложение Д Подготовка устройства Windows для установки MCK.....	178

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)
CHAP	Протокол аутентификации с косвенным согласованием (Challenge Handshake Authentication Protocol)
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)
Кнох	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)
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)

Сокращение	Полное наименование
SIM	Модуль идентификации абонента (Subscriber Identification Module)
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	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)
APM	Автоматизированное рабочее место
ЗУ	Зарядное устройство
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
Метаинформация	Дополнительная информация, раскрывающая сведения о признаках и свойствах, характеризующих какие-либо сущности, позволяющие автоматически искать и управлять ими в больших информационных потоках
МСК	Мобильное средство коммуникации (мобильный телефон, смартфон, планшетный компьютер, смарт-браслет)
ОС	Операционная система
ОШС	Организационно-штатная структура предприятия

Сокращение	Полное наименование
ПК	Персональный компьютер
ПО	Программное обеспечение
Профиль	Совокупность значений и настроек ОС
ПУН	Приложение с управляемыми настройками
ПУП	Правило управления приложением
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
УПАТС	Учрежденческо-производственная автоматическая телефонная станция
Сущность	Именованный набор данных, который можно атомарно (целиком) назначить или снять с узла ОШС, сотрудника или МСК. К сущностям относятся профиль, ПУП и КП
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 APM Администратора, а также действий по управлению комплексной цифровой мультиплатформы 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
- мониторинг состояния здоровья сотрудников посредством смарт-браслетов.

2 Описание действий при работе с APM Администратора SafeMobile

2.1 Аутентификация в APM Администратора SafeMobile

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

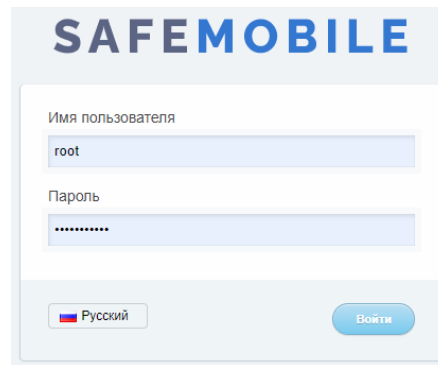




Рисунок 2.1 – Окно аутентификации

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 APМа, заданными в 2.8.1.

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 APM, зависит от полномочий Администратора, от имени которого выполнен вход в систему.

2.2 Обзор интерфейса APM Администратора SafeMobile

Главное окно APM Администратора SafeMobile (рисунок 2.2), открывающееся после аутентификации, состоит из следующих компонентов:

- 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;
- **главное меню**, которое находится в левой части окна и включает элементы, позволяющие осуществлять управление и получать информацию о состоянии МСК.

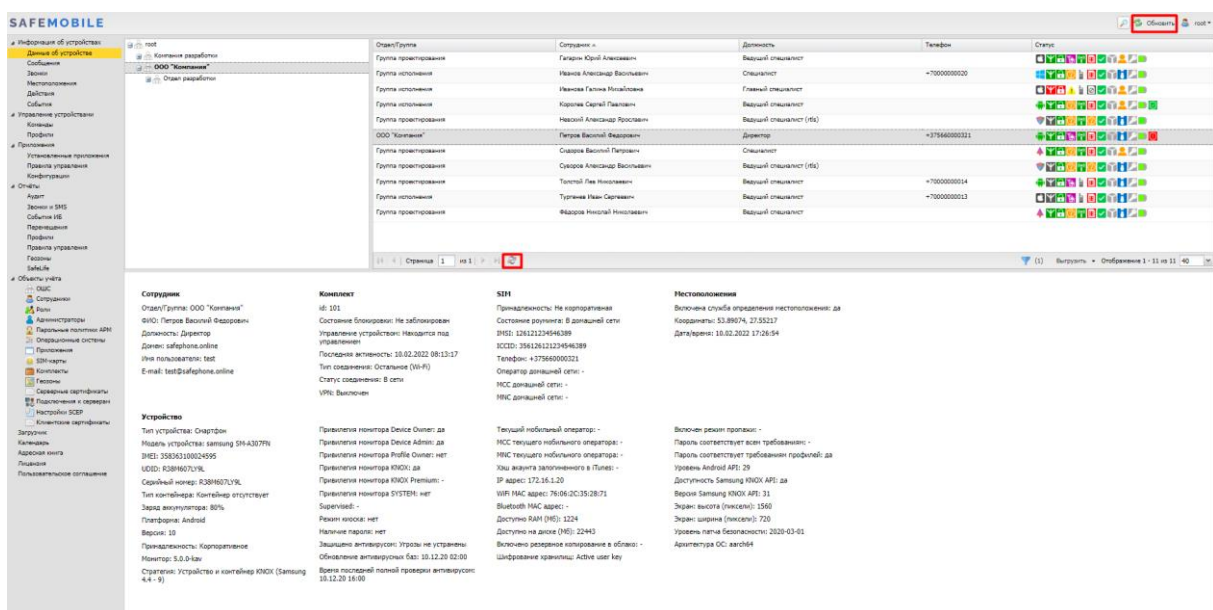


Рисунок 2.2 – Главное окно APM Администратора SafeMobile

Кнопка **«Обновить»**, 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.

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 APM Администратора SafeMobile; переключить интерфейс на английский язык, нажав на кнопку **Русский** (рисунок 2.3), после перехода на английский язык кнопка изменится на **English**.

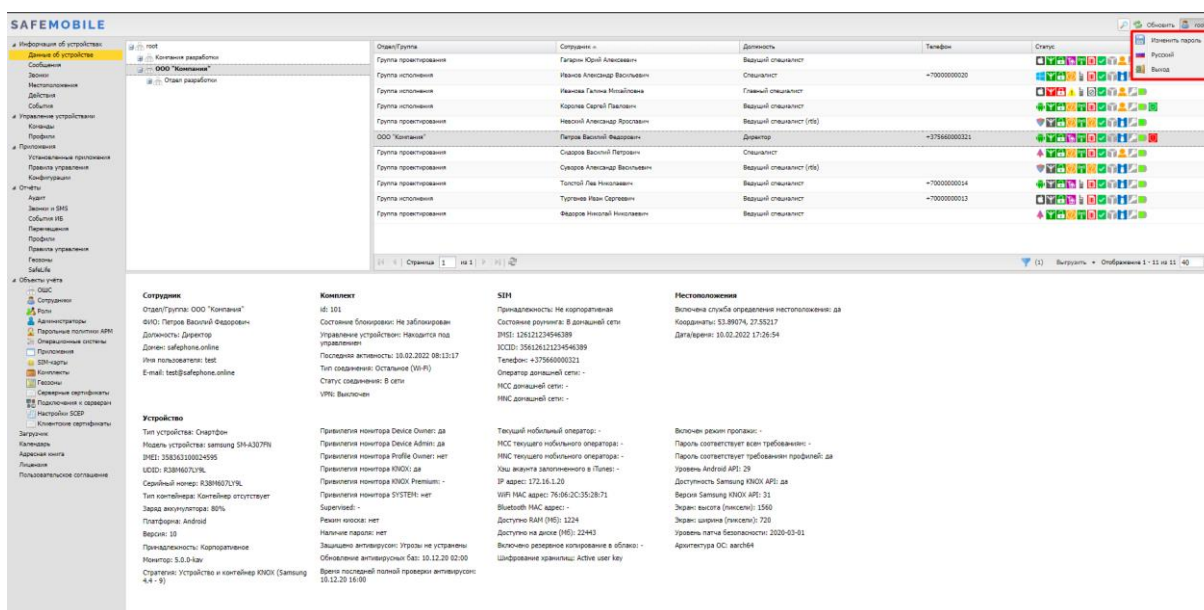


Рисунок 2.3 – Меню, отображающее имя пользователя (логин)

Для осуществления поиска в таблицах предназначена кнопка в правом верхнем углу окна, раскрывающая меню поиска в соответствии с рисунком 2.4, в котором следует ввести параметры искомой записи.

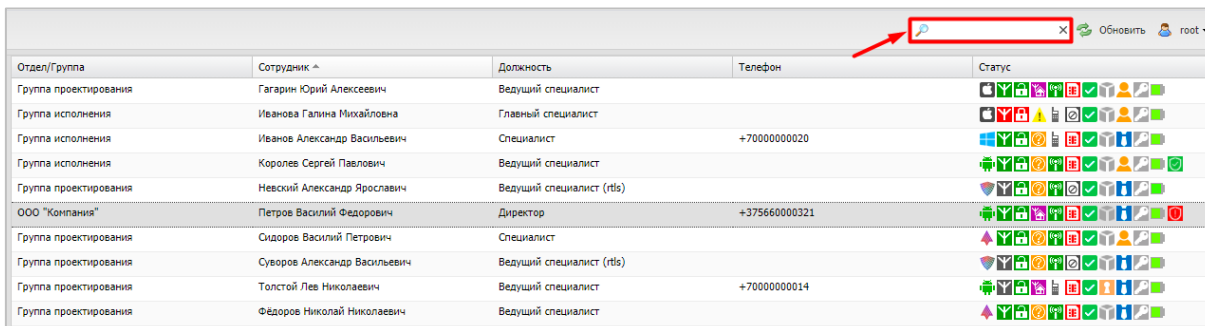


Рисунок 2.4 – Меню поиска в главной таблице

В APM 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  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.

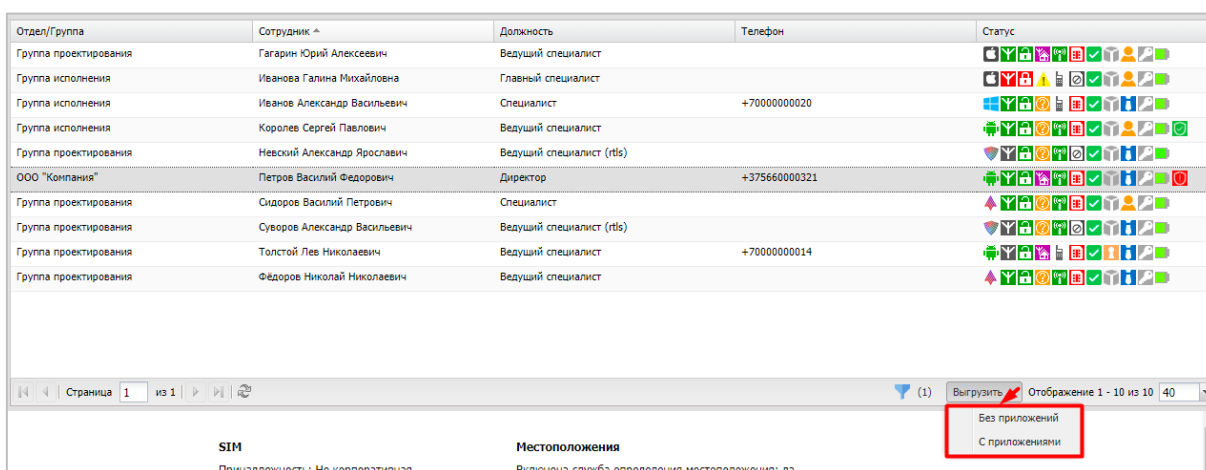


Рисунок 2.5 – Меню «Выгрузить» в главной таблице

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 APM 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.

Отдел/Группа	Сотрудник	Должность	Телефон	Статус
Группа проектирования	Гагарин Юрий Алексеевич	Ведущий специалист		[Иконки]
Группа исполнения	Иванова Галина Михайловна	Главный специалист		[Иконки]
Группа исполнения	Иванов Александр Васильевич	Специалист	+70000000020	[Иконки]
Группа исполнения	Королев Сергей Павлович	Ведущий специалист		[Иконки]
Группа проектирования	Невский Александр Ярославич	Ведущий специалист (rtls)		[Иконки]
ООО "Компания"	Петров Василий Федорович	Директор	+375660000321	[Иконки]
Группа проектирования	Сидоров Василий Петрович	Специалист		[Иконки]
Группа проектирования	Суворов Александр Васильевич	Ведущий специалист (rtls)		[Иконки]
Группа проектирования	Толстой Лев Николаевич	Ведущий специалист	+70000000014	[Иконки]
Группа проектирования	Федоров Николай Николаевич	Ведущий специалист		[Иконки]

Страница 1 из 1

Выгрузить | Отображение 1 - 10 из 10 | 40

20
40
60
100
Другое

SIM
Принадлежность: Не корпоративная
Состояние роуминга: В домашней сети
IMSI: 126121234546389

Местоположения
Включена служба определения местоположения: да
Координаты: 53.89074, 27.55217
Дата/время: 26.02.2021 23:48:42

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».

Отдел/Группа	Сотрудник	Должность	Телефон	Статус
Группа проектирования	Гагарин Юрий Алексеевич	Ведущий специалист		[Иконки]
Группа исполнения	Иванова Галина Михайловна	Главный специалист		[Иконки]
Группа исполнения	Иванов Александр Васильевич	Специалист	+70000000020	[Иконки]
Группа исполнения	Королев Сергей Павлович	Ведущий специалист		[Иконки]
Группа проектирования	Невский Александр Ярославич	Ведущий специалист (rtls)		[Иконки]
ООО "Компания"	Петров Василий Федорович	Директор	+375660000321	[Иконки]
Группа проектирования	Сидоров Василий Петрович	Специалист		[Иконки]
Группа проектирования	Суворов Александр Васильевич	Ведущий специалист (rtls)		[Иконки]
Группа проектирования	Толстой Лев Николаевич	Ведущий специалист	+70000000014	[Иконки]
Группа проектирования	Федоров Николай Николаевич	Ведущий специалист		[Иконки]

Страница 1 из 1

Выгрузить | Отображение 1 - 10 из 10 | 40

Рисунок 2.7 – Сортировка записей в столбце главной таблице

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

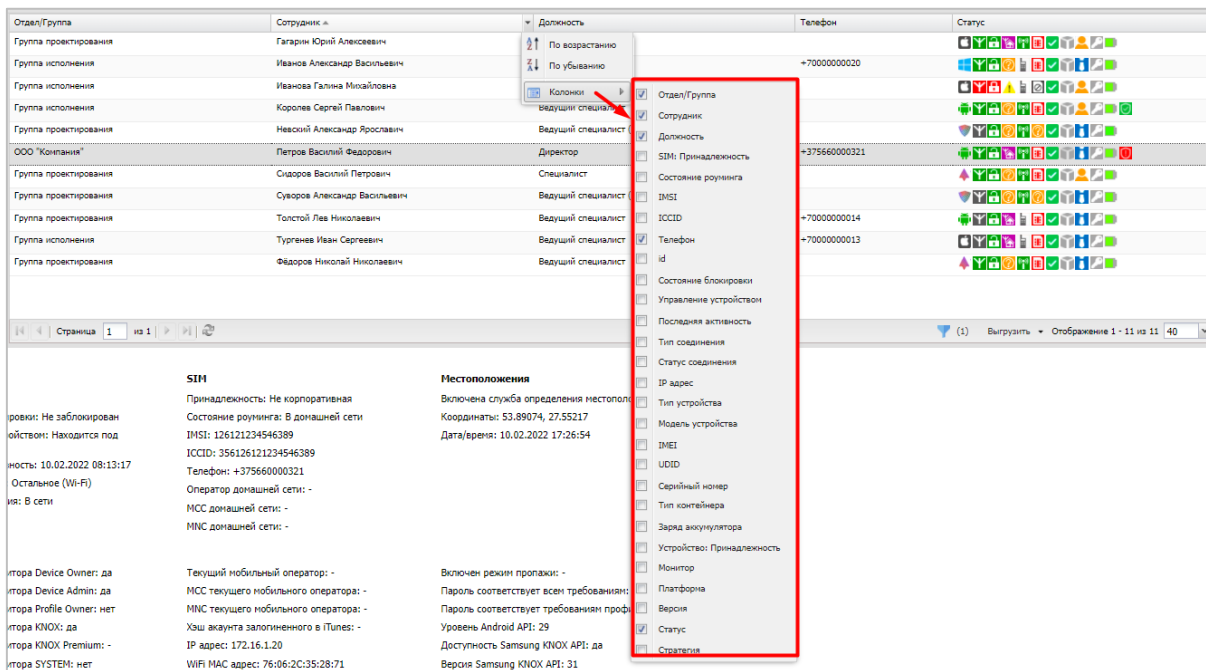


Рисунок 2.8 – Управление столбцами в главной таблице

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.

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 2.9.

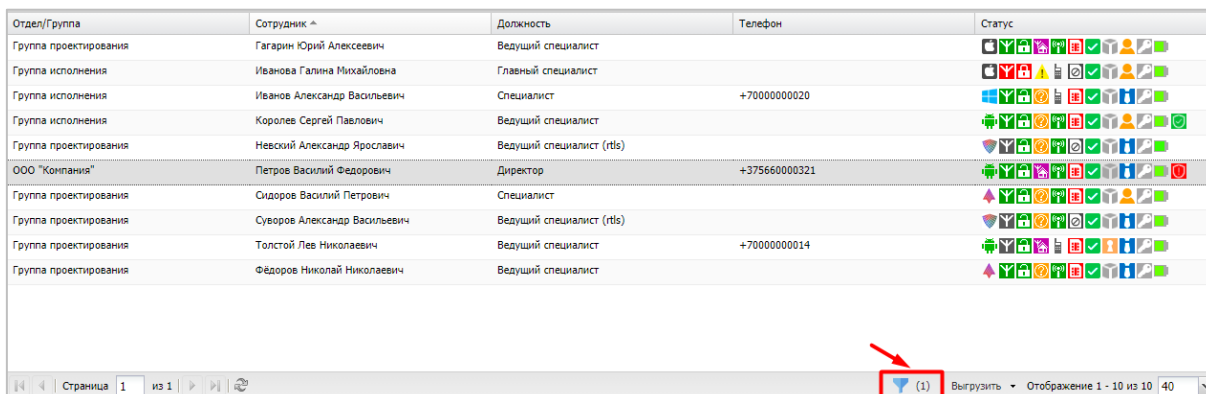


Рисунок 2.9 – Фильтрация записей в главной таблице

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 2.10.

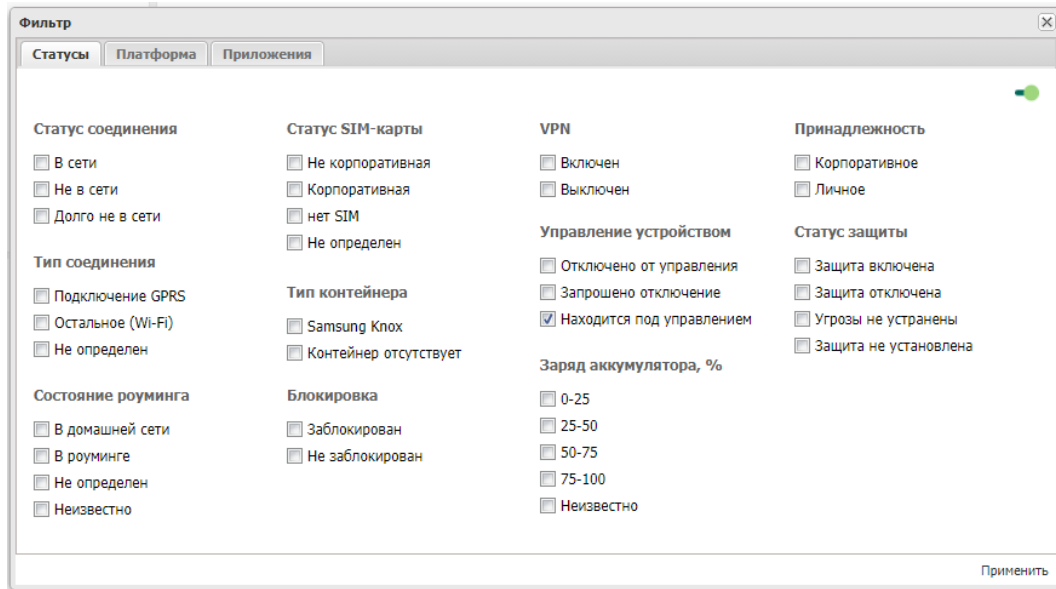


Рисунок 2.10 – Вкладка «Статусы»

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

Во вкладке «Платформа» (рисунок 2.11) можно задать фильтрацию записей в зависимости платформы МСК. По умолчанию фильтр «Платформа» выключен.

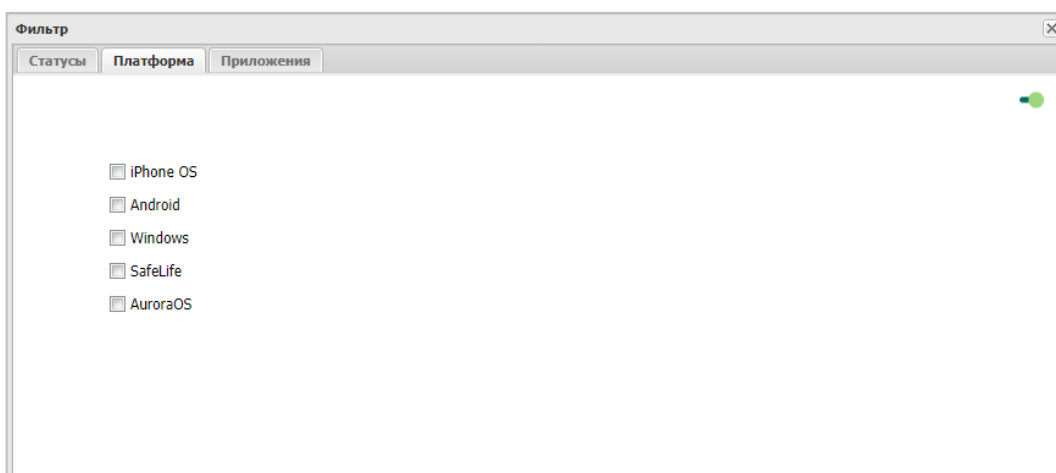


Рисунок 2.11 – Вкладка «Платформа»

Во вкладке «Приложения» можно задать фильтрацию записей в зависимости от

установленных/неустановленных приложений на МСК соответствии с рисунком 2.12. По умолчанию фильтр «Приложения» выключен.

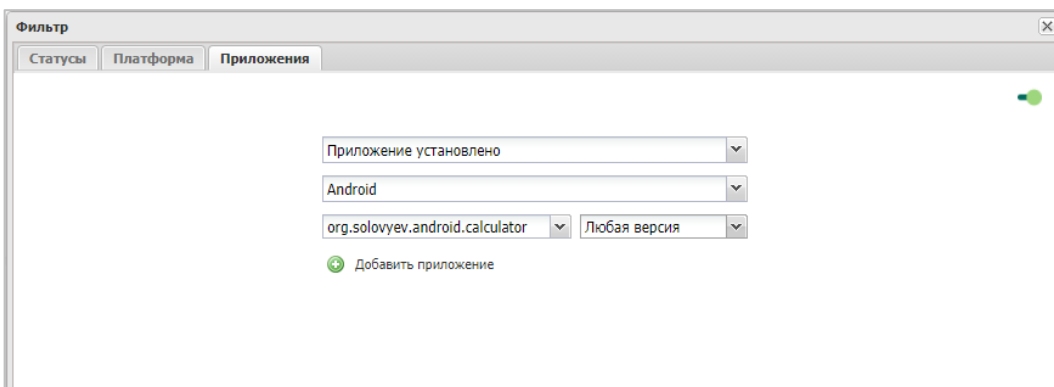


Рисунок 2.12 – Вкладка «Приложения»

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 2.13.

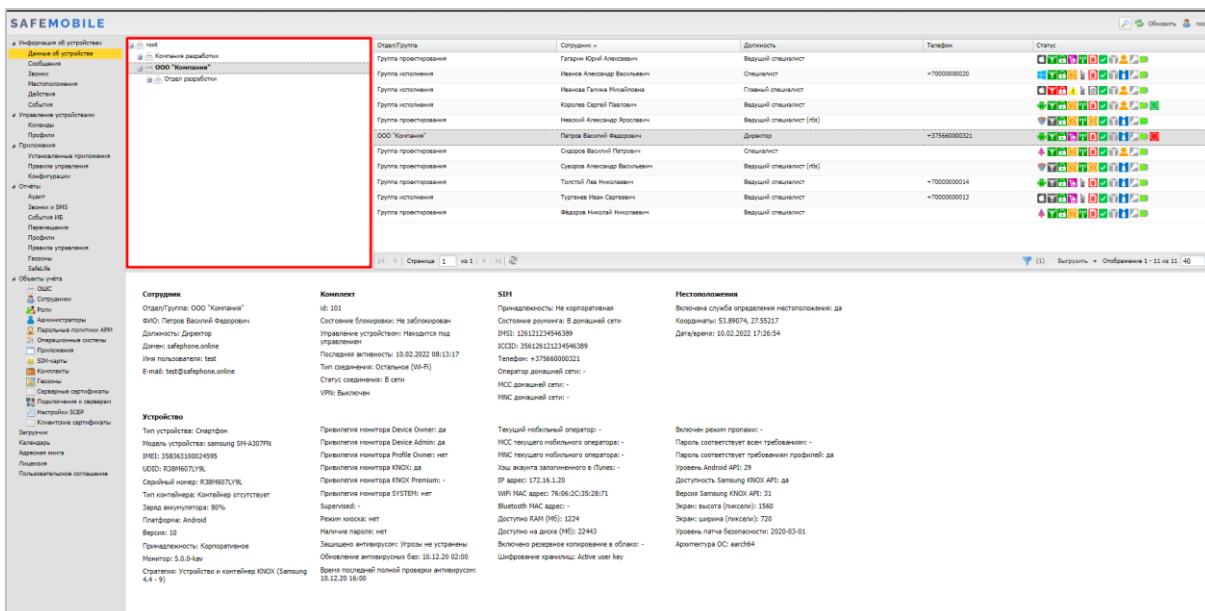


Рисунок 2.13 – Панель ОШС

Иерархический список подразделений позволяет выбрать подразделение, после чего в главной таблице справа отобразится список МСК, имеющих 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 2.14.

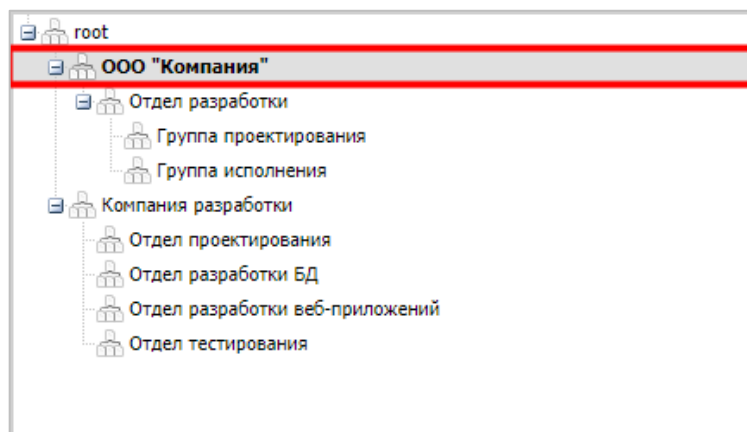


Рисунок 2.14 – Выбор корневого узла предприятия в панели ОШС

2.4 Главная таблица

В главной таблице (рисунок 2.15) 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.

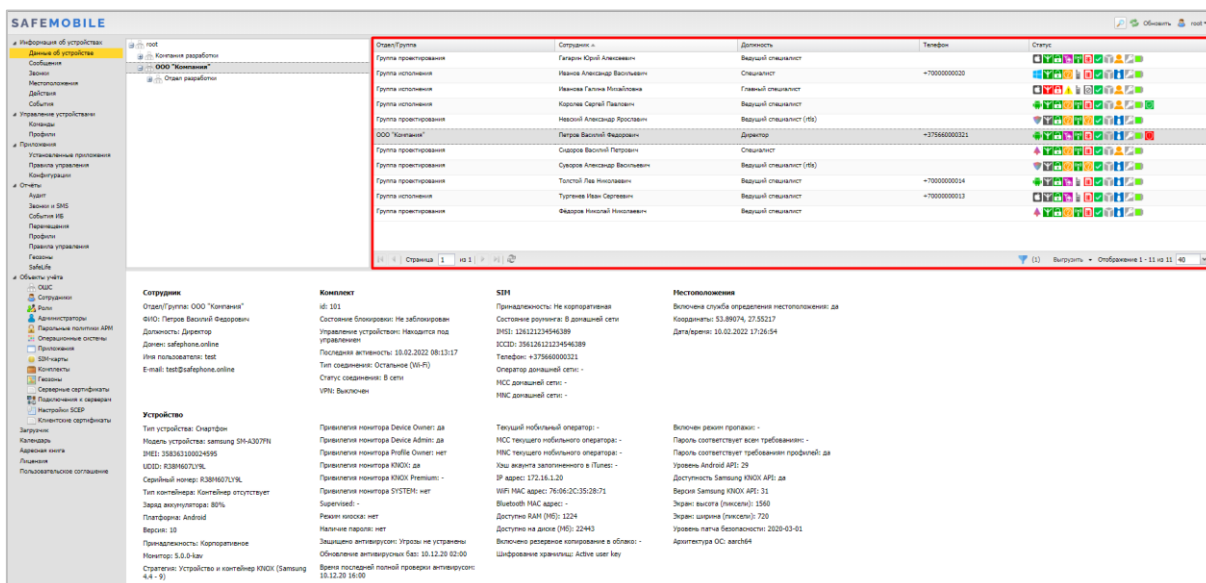








Рисунок 2.15 – Главная таблица

















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);
- **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;**
- **ICCID;**
- **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;
- **IMEI**;
- **UDID**;
- **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.

Таблица 2.1 – Состояния мобильного средства коммуникации

Значок	Значение
Платформа	
	Android
	iOS
	Windows
	Аврора
	SafeLife
Состояние соединения	
	В сети

Значок	Значение
	Не в сети
	Долго не в сети
Блокировка	
	Заблокирован
	Не заблокирован
Состояние роуминга	
	В домашней сети
	В роуминге
	Неизвестно
	Не определен
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

Значок	Значение
	Контейнер отсутствует
	Android for Work
Состояние батареи	
	Уровень заряда батареи
Управление устройствам	
	Отключено от управления
	Запрошено отключение
	Находится под управлением
Принадлежность устройства	
	Корпоративное
	Личное
VPN	
	Включен
	Выключен
Непрерывная защита KAV	
	Угрозы не устранены
	Непрерывная защита включена
	Непрерывная защита выключена

2.5 Информационная таблица

В информационной таблице, расположенной в нижней части главного окна APM Администратора в соответствии с рисунком 2.16, отображаются сведения по МСК, выбранному в главной таблице.

В информационной таблице воспроизводятся данные в зависимости от выбранных разделов главного меню, а именно:

- данные об устройстве;
- сообщения;
- звонки;
- местоположения;
- действия (результаты команд);
- события;
- команды;
- установленные приложения;
- отчёт «Перемещения»;
- отчет «Safelife».
- Объект учета «Клиентские сертификаты»

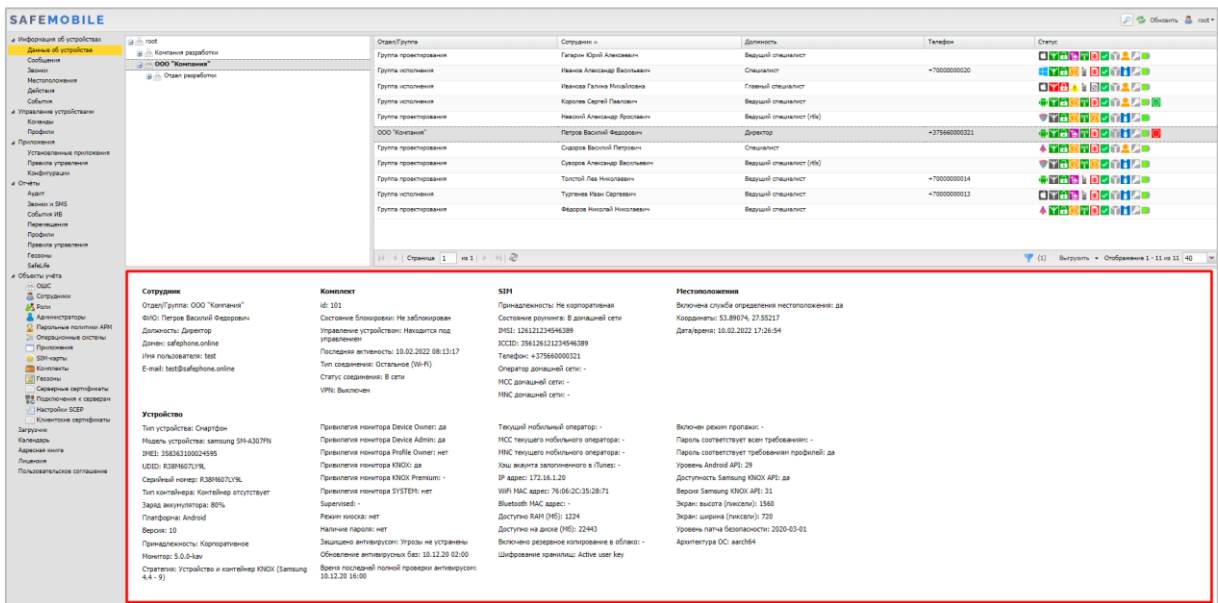


Рисунок 2.16 – Информационная таблица

2.6 Главное меню

В левой части главного окна APM Администратора SafeMobile в соответствии с рисунком 2.17 расположена панель главного меню, содержащая следующие разделы:

- **Информация об устройствах**
 - Данные об устройстве
 - Сообщения
 - Звонки
 - Местоположения

- Действия
- События
- Управление устройствами
 - Команды
 - Профили
- Приложения
 - Установленные приложения
 - Правила управления
 - Конфигурации
- Отчёты
 - Аудит
 - Звонки и SMS
 - События ИБ
 - Перемещения
 - Профили
 - Правила управления
 - Геозоны
 - SafeLife
- Объекты учёта
 - ОШС
 - Сотрудники
 - Роли
 - Администраторы
 - Парольные политики APM
 - Операционные системы
 - Приложения
 - SIM-карты
 - Комплект
 - Геозоны
 - Серверные сертификаты
 - Подключения к серверам
 - Настройки SCEP
 - Клиентские сертификаты
- Загрузчик
- Календарь

- Адресная книга
- Лицензия
- Пользовательское соглашение

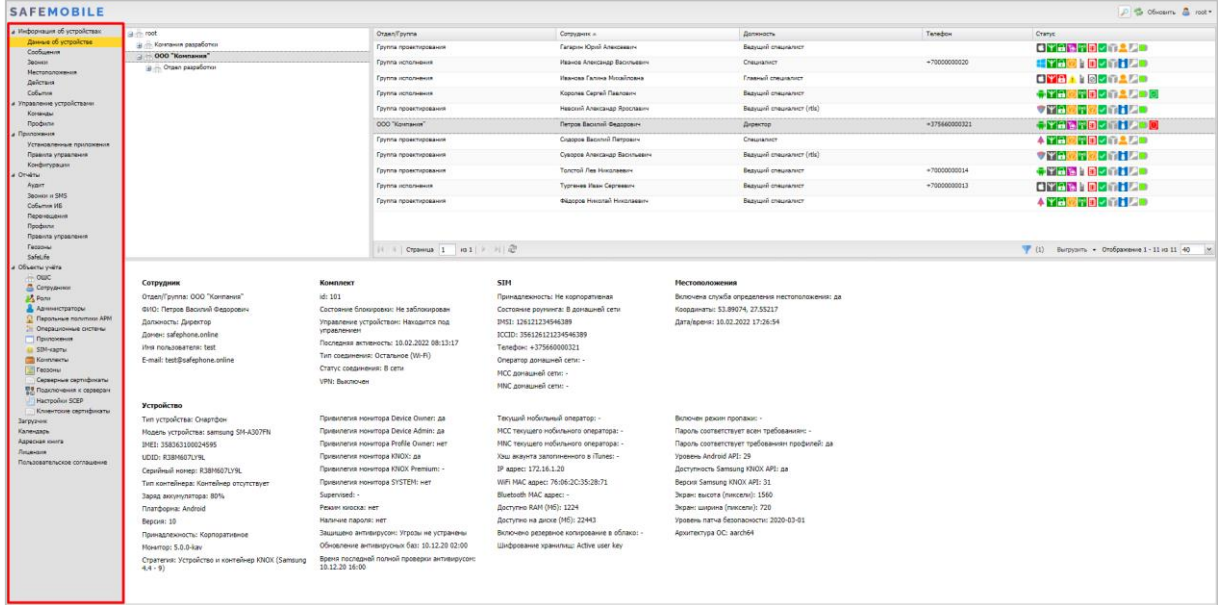


Рисунок 2.17 – Главное меню

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 2.18.

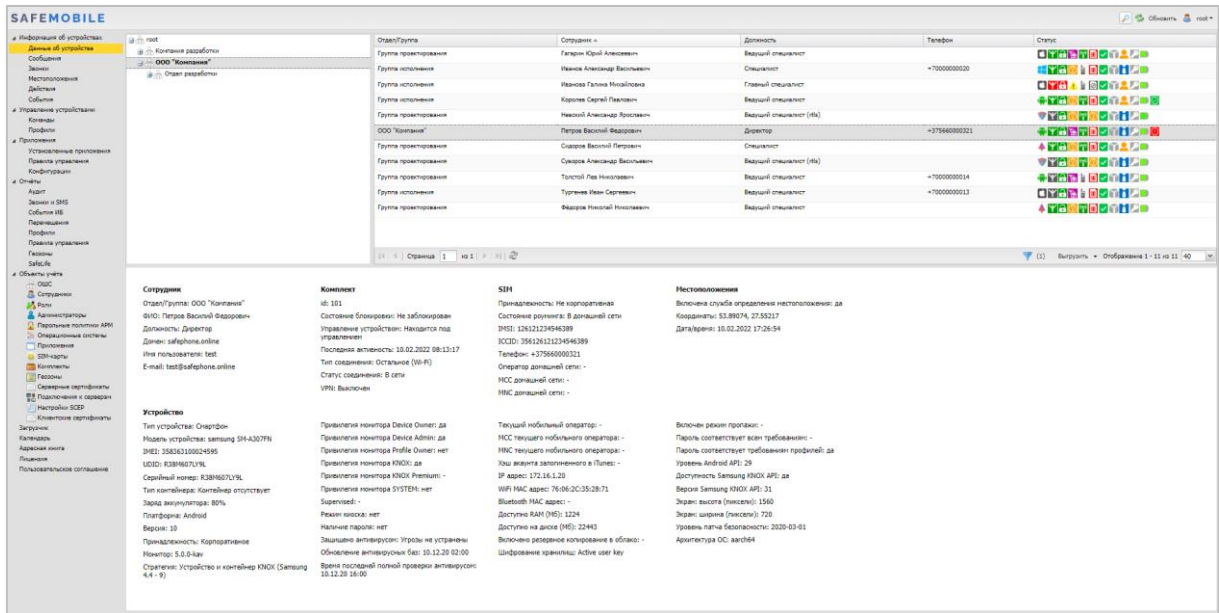


Рисунок 2.18 – Информация о параметрах комплекта

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);
- 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/не в сети/долго не в сети);
- VPN (включен/выключен);

• **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);
- 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 MCK на платформе iOS и Android);
- Тип контейнера (Samsung Кнох/Рабочий профиль Андроид/контейнер отсутствует);
- Заряд аккумулятора (от 0 до 100 %);
- Платформа;
- Версия (версия ОС);
- Принадлежность (корпоративное/личное);
- Монитор (версия монитора);
- Стратегия (устройство/устройство и контейнер KNOX/персональный 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);
- Защищено антивирусом: (да/угрозы не устранены/нет);
- Обновление антивирусных баз (дата и время);

- Время последней полной проверки антивирусом (дата и время);
- 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 MCK 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.

2.6.2 Раздел «Сообщения»

Пункт главного меню «Сообщения» предназначен для отображения зарегистрированных сообщений на MCK, выбранном в главном окне, включая SMS и внутренние сообщения (в том числе, фото и голосовые сообщения) согласно рисунку 2.19.

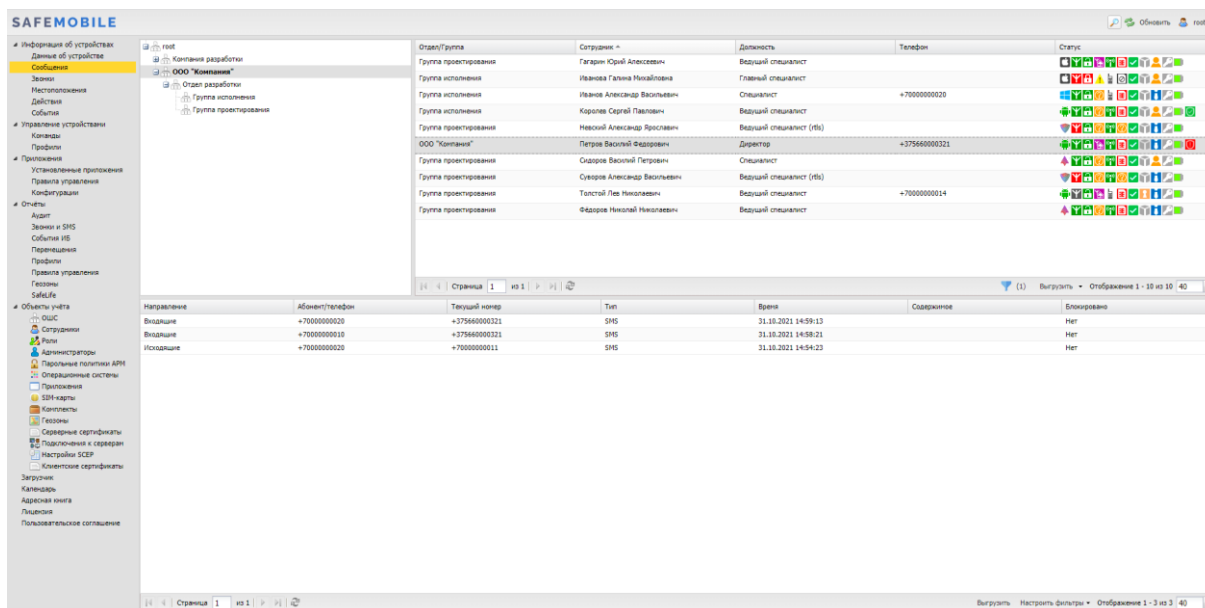


Рисунок 2.19 – Раздел «Сообщения»

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 заблокировано политиками безопасности; содержит «Нет», если сообщение не заблокировано.

В информационной таблице имеется возможность отображения сообщений в соответствии с выбранным фильтром (рисунок 2.20).

Направление	Абонт/телефон	Текущий номер	Тип	Время	Содержимое	Блокировано
Исходящие	Петров Василий Федорович	+70000000020	SMS	08.11.2018 10:53:46		Нет
Исходящие	+7000000011	+70000000020	SMS	08.11.2018 10:54:21		Нет
Исходящие	Администратор		Внутреннее	08.11.2018 10:54:29	Сообщение от Администратора SafePhone	Нет
Исходящие	Петров Василий Федорович	+70000000020	SMS	08.11.2018 11:00:14		Нет
Исходящие	Федоров Николай Николаевич	+70000000020	SMS	08.11.2018 11:00:31		Нет
Исходящие	Федоров Николай Николаевич	+70000000020	SMS	08.11.2018 11:02:07		Нет
Исходящие	Федоров Николай Николаевич		Голосовое	08.11.2018 11:02:43	🔊	Нет
Исходящие	Федоров Николай Николаевич		Фото	08.11.2018 11:02:43	📷	Нет
Исходящие	Федоров Николай Николаевич		Внутреннее	08.11.2018 11:02:43	Текст внутреннего сообщения	Нет

Направление
 Тип
 После
 До
 Внутреннее
 SMS
 Голосовое
 Фото

Рисунок 2.20 – 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 показывать 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 2.21.

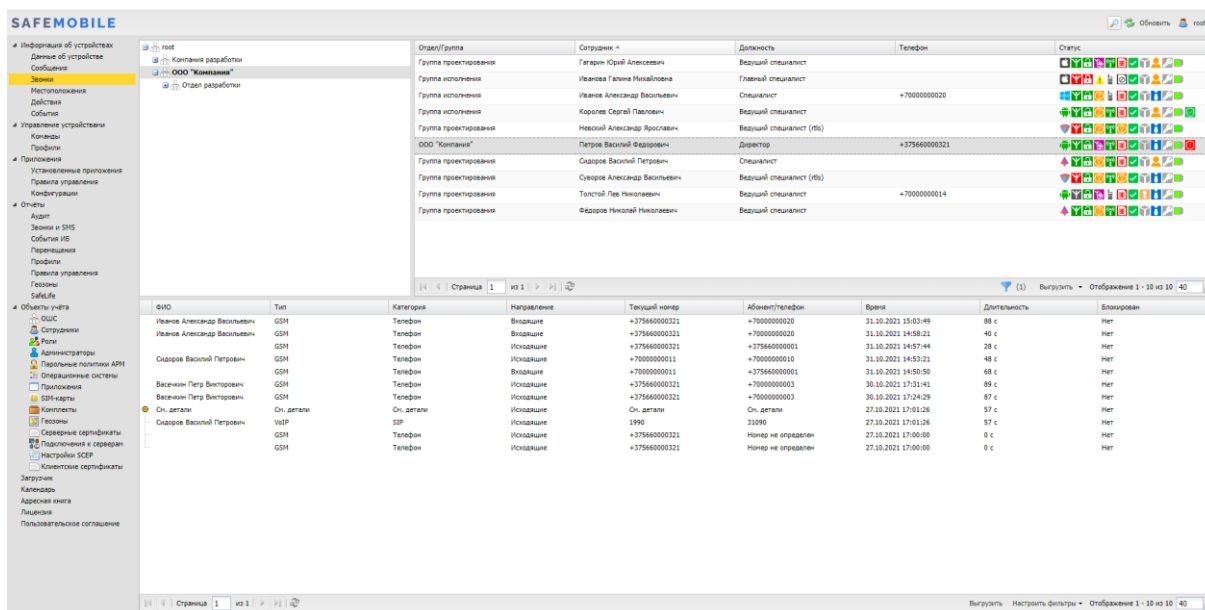


Рисунок 2.21 – Раздел «Звонки»

Информация о звонках доступна только для МСК на платформе Android версии не более 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 2.22).

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
Иванов Александр Васильевич	GSM	Телефон	Входящие	+70000000011	+37566000001	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
Сидоров Василий Петрович	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	См. детали	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
Федоров 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		Нет

Направление
 Категория
 Тип
 Блокировано
 После
 До

Телефон
 УПАТС
 SIP

Рисунок 2.22 – Фильтрация звонков

Чтобы открыть меню настройки фильтрации списка звонков, следует нажать в нижней панели информационной таблицы кнопку **Настроить фильтры**, после чего отобразится 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 2.23.

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	Исходящее	+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

Страница 1 из 1 | Настроить фильтры | Отображение 1 - 6 из 6 | 25

Рисунок 2.23 – 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 2.24.

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

Рисунок 2.24 – 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 2.25.

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.

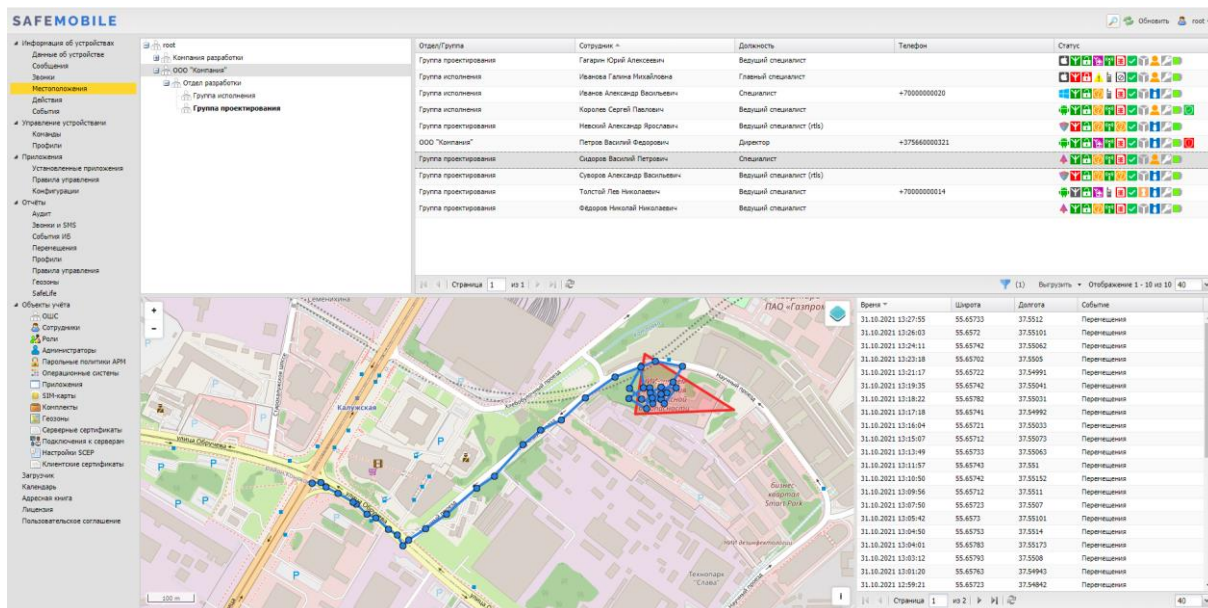



Рисунок 2.25 – Раздел «Местоположения»

При нажатии на значок  в правой верхней части карты отображается меню настройки отображения информации на карте (рисунок 2.26).

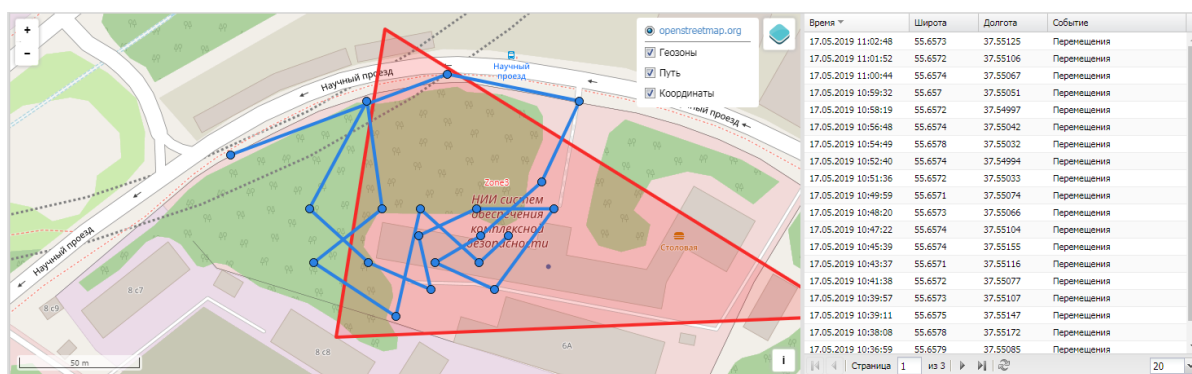


Рисунок 2.26 – Настройка режима отображения информации о местоположении абонента на карте

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 выбранным фильтром (рисунок 2.27).

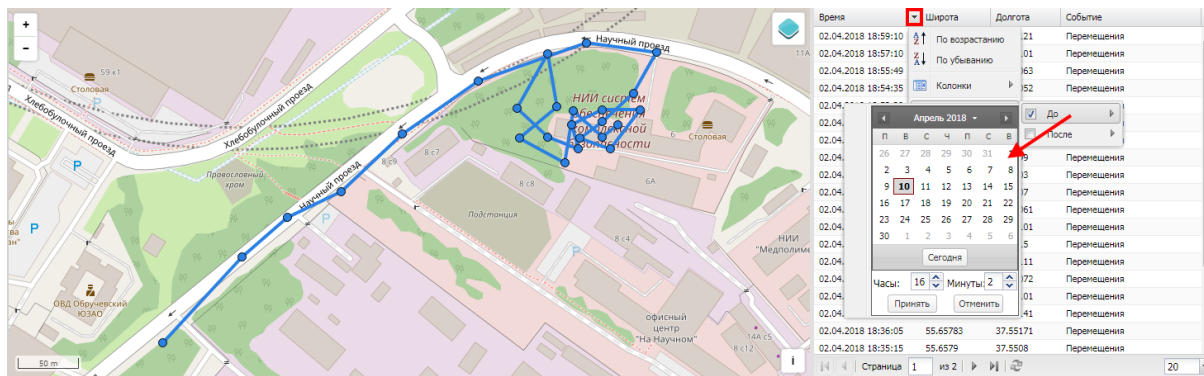



Рисунок 2.27 – Фильтрация местоположений абонента

Чтобы открыть меню настройки фильтрации реестра координат, нажмите кнопку  в заголовке столбца «Время». Затем наведите курсор мыши на пункт «Фильтр», после чего отобразятся следующие пункты меню в соответствии с рисунком 2.27:

- **До** – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке и на карте местоположения абонента до этой даты и времени;
- **После** – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке и на карте местоположения абонента после этой даты и времени.

По умолчанию в таблице показываются все местоположения без фильтрации (флажки в раскрывающемся меню «Фильтр» сняты).

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.2.10.

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 2.28).

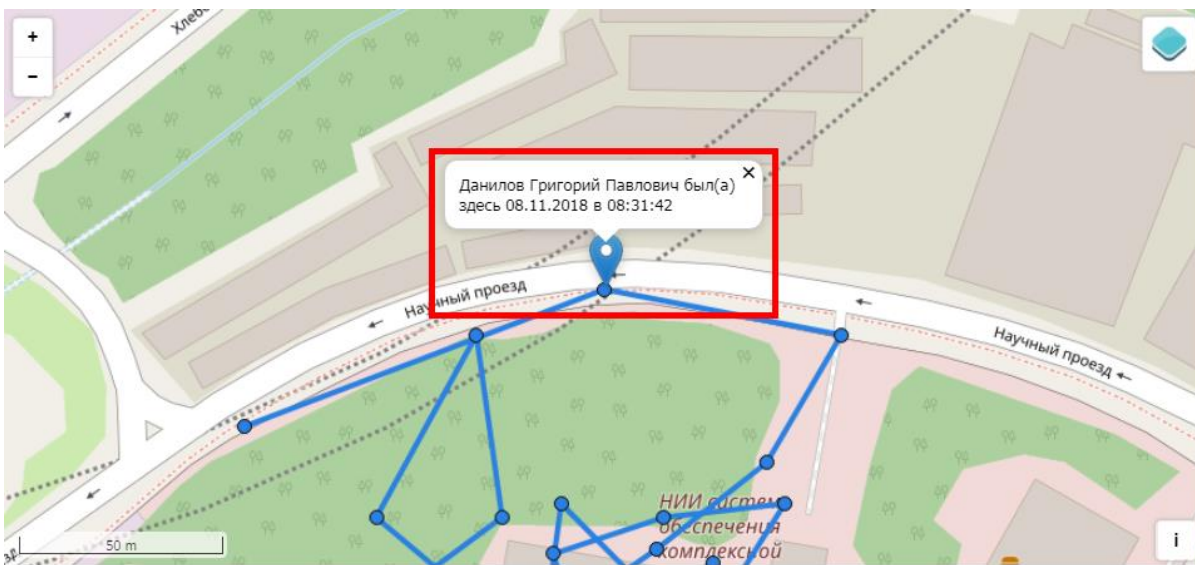


Рисунок 2.28 – Местонахождение сотрудника в выбранной точке траектории перемещения

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 2.29.

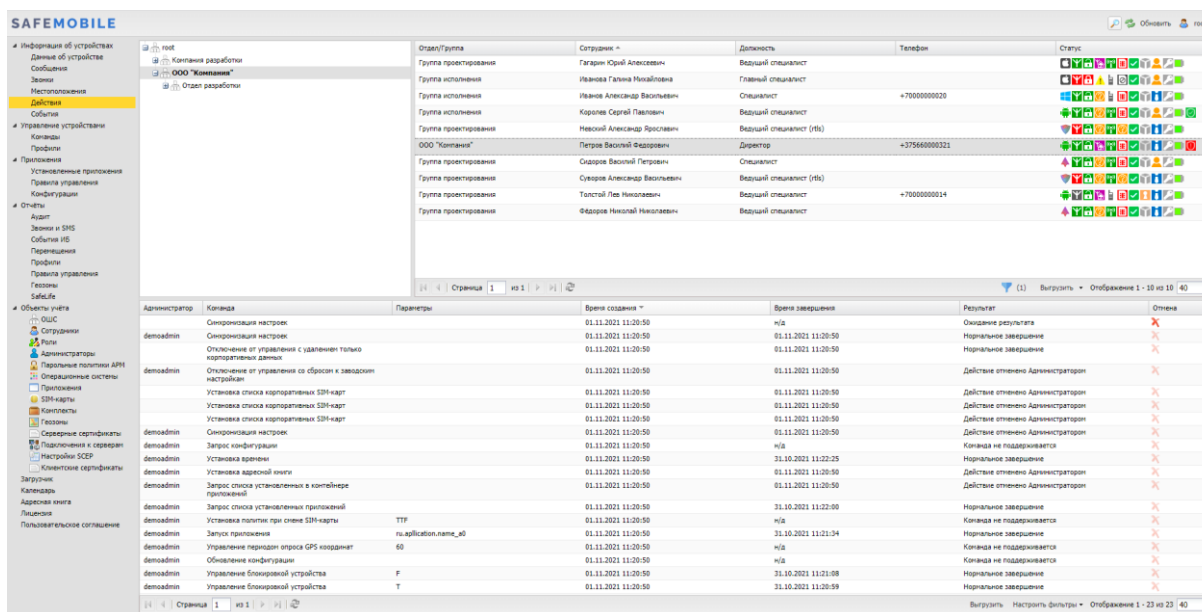


Рисунок 2.29 – Раздел «Действия»

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 2.30).

Администратор	Команда	Параметры	Время создания	Время завершения	Результат	Отмена
root	Синхронизация настроек		04.12.2018 18:34:57	04.12.2018 21:34:57	Нормальное завершение	
root	Переподключение	10	04.12.2018 18:34:57	04.12.2018 18:38:33	Команда была выдана на устройство, после чего устройство отключилось	
root	Установка списка сотовых операторов		04.12.2018 18:34:57	04.12.2018 18:38:24	Нормальное завершение	
root	Установка списка корпоративных SIM-карт		04.12.2018 18:34:57	04.12.2018 18:38:16	Нормальное завершение	
root	Установка политик при смене SIM-карты	TTT	04.12.2018 18:34:57	04.12.2018 18:38:07	Нормальное завершение	
root	Установка программы-монитора последней версии	13	04.12.2018 18:34:57	04.12.2018 18:37:41	Команда доставлена, ожидается результат	
root	Установка программы-монитора	9	04.12.2018 18:34:57	04.12.2018 18:37:41	Нормальное завершение	
root	Запрос конфигурации		04.12.2018 18:34:57	04.12.2018 18:37:24	Нормальное завершение	
root	Установка времени		04.12.2018 18:34:57	04.12.2018 18:37:15	Нормальное завершение	
root	Установка списка разрешенных точек доступа		04.12.2018 18:34:57	04.12.2018 18:37:07	Нормальное завершение	
root	Установка адресной книги		04.12.2018 18:34:57	04.12.2018 18:36:58	Ис	
root	Запрос списка установленных в контейнере приложений		04.12.2018 18:34:57	н/д	Ок	
root	Запрос списка установленных приложений		04.12.2018 18:34:57	04.12.2018 18:36:49	Нс	
root	Установка политик при смене SIM-карты	TTT	04.12.2018 18:34:57	04.12.2018 18:36:41	Нс	
root	Установка приложения	Приложение 1 1, ru.application_name_11, 1.1	04.12.2018 18:34:57	04.12.2018 18:36:23	Ок	
root	Удаление приложения	ru.application_name_10	04.12.2018 18:34:57	04.12.2018 18:36:15	Нс	
root	Запуск приложения	ru.application_name_10	04.12.2018 18:34:57	04.12.2018 18:35:57	Нс	

Рисунок 2.30 – Фильтрация действий

Чтобы открыть меню настройки фильтрации списка действий, нажмите кнопку **Настроить фильтры**, после чего отобразятся следующие пункты меню в соответствии с рисунком 2.30:

- **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, завершённые после этой даты и времени;
- **Завершено до** – установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, завершённые 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.

Порядок	Событие	Описание	Время
546	Ошибка определения SIM-карты	Причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=104	31.10.2021 07:50:50
542	Ошибка окончания приложения	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=103	31.10.2021 07:50:50
538	Ошибка удаления правила управления приложениями	Приложение: Приложение в 0, UID: ru.arifaction.lame_A0, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=102	31.10.2021 07:50:50
530	Обнаружена угроза	Объект API: UID: ru.lisoiy.klcc.android, права Device Admin: Нет, расположение: KATEINER, тип угрозы: MALWARE, уровень опасности: NEEDUPH, название: vlxah	31.10.2021 07:50:50
526	Ошибка антивируса KAV	Причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=99	31.10.2021 07:50:50
522	Ошибка синхронизации	Разрешение мониторинга: Устройство, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=98	31.10.2021 07:50:50
518	Нет доступа	some details	01.11.2021 11:20:50
514	Пуш-уведомление недоступно	Приложение: MCC-Android-new, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=95	31.10.2021 07:50:50
510	Приложение не может быть добавлено в ящик	Ошибка event_code=94	31.10.2021 07:50:50
506	Ошибка валидации Ключа ключа	Наименование ключевого дистрибутива: Virplet's dist name	31.10.2021 07:50:50
498	Установка ключевого дистрибутива Virplet	Причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=91	31.10.2021 07:50:50
494	Ошибка установки ключевого дистрибутива Virplet	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=90	31.10.2021 07:50:50
490	Ошибка подключения к Virplet	UID: Стопе, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=84	31.10.2021 07:50:50
466	Ошибка применения правила управления приложениями	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=82	31.10.2021 07:50:50
458	Ошибка удаления приложения из контейнера	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=81	31.10.2021 07:50:50
454	Ошибка установки приложения в контейнер	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=80	31.10.2021 07:50:50
450	Ошибка удаления приложения	Приложение: MCC-Android-new, версия: 2.4.1, UID: ru.lisoiy.klcc.android, причина ошибки: Неизвестная ошибка, описание: Ошибка event_code=79	31.10.2021 07:50:50
446	Ошибка установки приложения	Давление: 150 мм-рт. столба	31.10.2021 07:50:50
442	Показана барометра	Частота средних сокращений: 60 ударов в минуту	31.10.2021 07:50:50
438	Зафиксировано падение		31.10.2021 07:50:50
434	Регистрация пульса		31.10.2021 07:50:50

Рисунок 2.31 – Раздел «События»

Информационная таблица раздела «События» содержит следующие столбцы в соответствии с рисунком 2.31:

- **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 2.32).

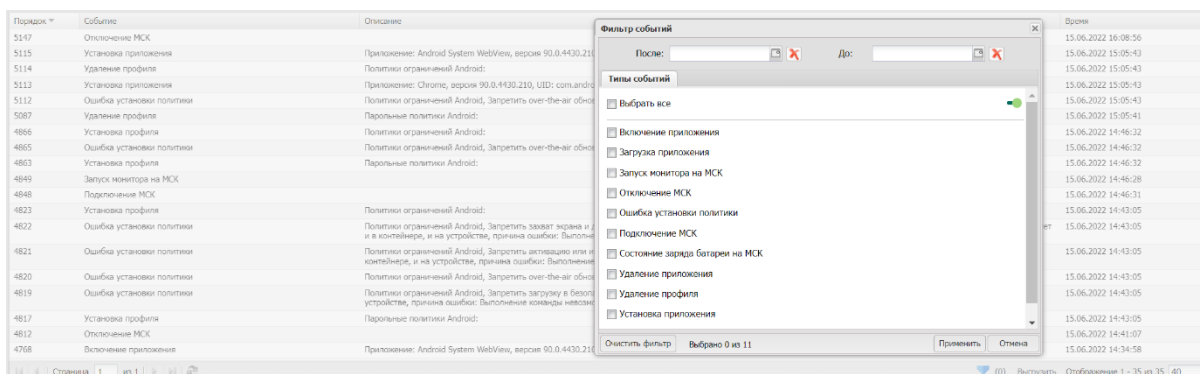


Рисунок 2.32 – Фильтрация событий

Чтобы открыть меню настройки фильтрации списка событий, нажмите кнопку **Настроить фильтры**, после чего отобразятся следующие пункты меню в соответствии с рисунком 2.32:

- **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 (Т – 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 (Т – 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 заводской прошивки, то создание контейнера будет невозможно, и в APM 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 барометра	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 Кнох 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
Обнаружена угроза	Да		Антивирус KAV в составе монитора обнаружил приложение или файл, которые могут представлять угрозу	Название файла, путь к файлу, UID приложения, права Device Admin (да / нет), устройство / контейнер, тип угрозы (ADWARE / MALWARE / RISKWARE / TROJAN_BANKER / UDS_MALWARE / UDS_PHISHING), уровень опасности (LOW / MEDIUM / HIGH / INFO), название вируса
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
Угроза устранена	Да		Антивирус KAV в составе монитора устранил угрозу от приложения или файла	Название файла, путь к файлу, UID приложения, права Device Admin (да / нет), устройство / контейнер, тип угрозы (ADWARE / MALWARE / RISKWARE / TROJAN_BANKER / UDS_MALWARE / UDS_PHISHING), уровень опасности (LOW / MEDIUM / HIGH / INFO), название вируса

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка антивируса KAV	Нет		Библиотека KAV не прошла проверку валидности лицензии на сервере Касперского, ошибки при подключении к серверу Касперского	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 применения 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 **«Команды»** и требуемую команду в информационной таблице в соответствии с рисунком 2.33.

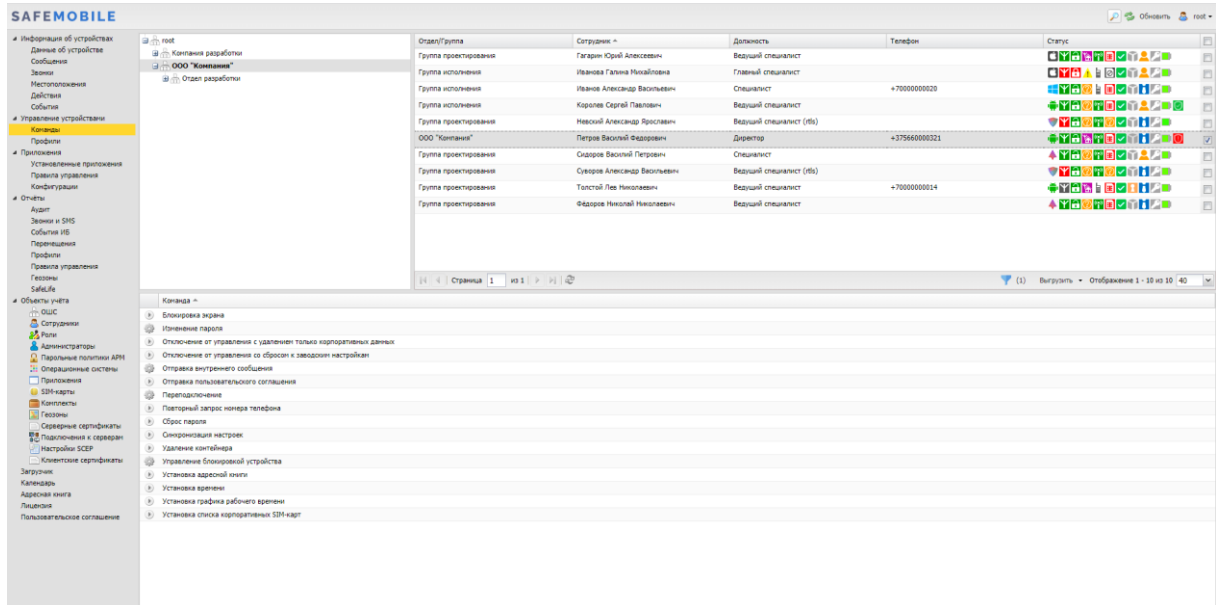



Рисунок 2.33 – Раздел «Команды»

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 2.34).

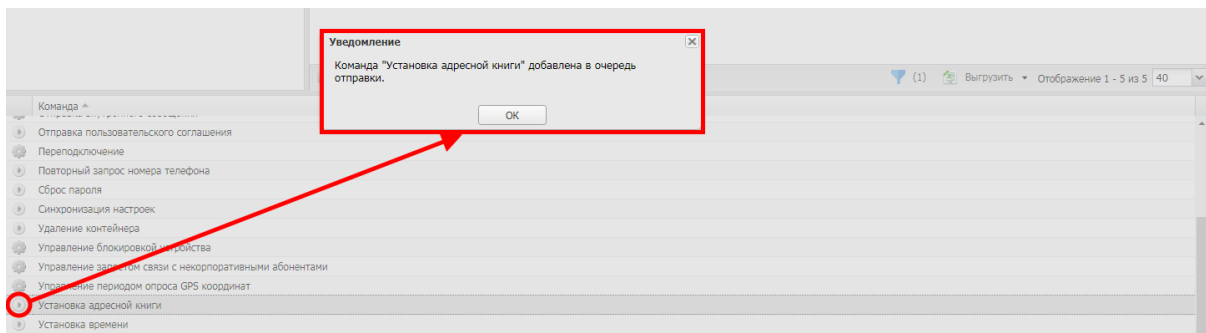


Рисунок 2.34 – Отправка команды без параметров

Если для выполнения команды  требуется указать ее параметры, слева от названия команды отображается значок  (рисунок 2.35). 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 2.35 – Отправка команды с параметрами

По умолчанию, столбец со значками отображается в таблице, но его можно скрыть, если убрать флажок в строке *Actions* при изменении состава отображаемых столбцов.

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	Платформа	Описание	Параметр команды	
			В разделе «Команды»	В разделе «Действия»
Управление блокировкой устройства	  	<p>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».</p> <p>При получении команды «Заблокировать устройство» осуществляется блокировка доступа к пользовательскому интерфейсу MCK</p>	Заблокировать устройство	T
	  	<p>При получении команды «Разблокировать устройство» осуществляется разблокировка устройства. Команда выполняется на устройствах с Supervised.</p> <p>При получении команды «Разблокировать устройство» осуществляется снятие блокировки доступа к пользовательскому интерфейсу MCK</p>	Разблокировать устройство	F
Блокировка экрана	  	При получении команды осуществляется блокировка экрана паролем пользователя	Отсутствуют	







Команда	Платформа	Описание	Параметр команды	
			В разделе «Команды»	В разделе «Действия»
Отправка внутреннего сообщения		На устройство отправляется созданное внутреннее сообщение	Текст сообщения	Порядковый номер сообщения
Установка адресной книги (сотруднику. подразделению)		На устройство отправляется актуальная адресная книга	Отсутствуют	
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	



Команда	Платформа	Описание	Параметр команды	
			В разделе «Команды»	В разделе «Действия»
Синхронизация времени устройства с сервером*		На устройство отправляется команда установки текущего времени на сервере SafeMobile	Отсутствуют	
Отключение от управления с удалением только корпоративных данных**	  	На MCK отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на MCK 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 сохраняются	Отсутствуют	
Отключение от управления со сбросом к заводским настройкам***	   	На MCK отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на MCK будут удалены корпоративные и личные данные (настройки, адресная книга, 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	Отсутствуют	

* Команда актуальна для MCK 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 проиля.

** 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 MCK с данными для ОС Windows 10.

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команды»	В разделе «Действия»
		периодической очистке БД. При повторном подключении устройства посредством КМЕ в указанный период команда отобразится с результатом «Нормальное завершение»		
Сброс пароля		На устройство отправляется команда сброса пароля. Если к устройству платформы Android уже предъявлены требования парольной политики, а именно: 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	Отсутствуют	
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
Удаление контейнера		На устройство отправляется команда удаления изолированной области на МСК для корпоративных приложений (данных)	Отсутствуют	
Синхронизация настроек		На устройство отправляются актуальные настройки ОС и приложений, заданные в профилях и конфигурациях	Отсутствуют	

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команды»	В разделе «Действия»
Повторный запрос номера телефона		МСК, получив команду, отправляет сообщение на номер телефона, заданный в профиле настроек монитора. По полученному сообщению, автоматически определяется номер телефона	Отсутствуют	
Отправить файл		На устройство отправляется файл. По получении пользователь уведомляется и файл выкладывается в папку «Загрузки».	Файл, предназначенный для отправки.	

2.6.8 Раздел «Профили»

Пункт меню «Профили» открывает окно (рисунок 2.36), 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;
- **Тип** – разновидность политик ОС;
- **Платформа** – платформа ОС;
- **Сущность** – инициатор сущности (собственный/делегированный);
- **Владелец** – администратор узла ОШС, назначенный владельцем сущности (по умолчанию, не отображается).

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

- **Политики;**
- **Условия/Условия (не заданы);**
- **Назначения;**
- **Владелец;**
- **Делегирование.**

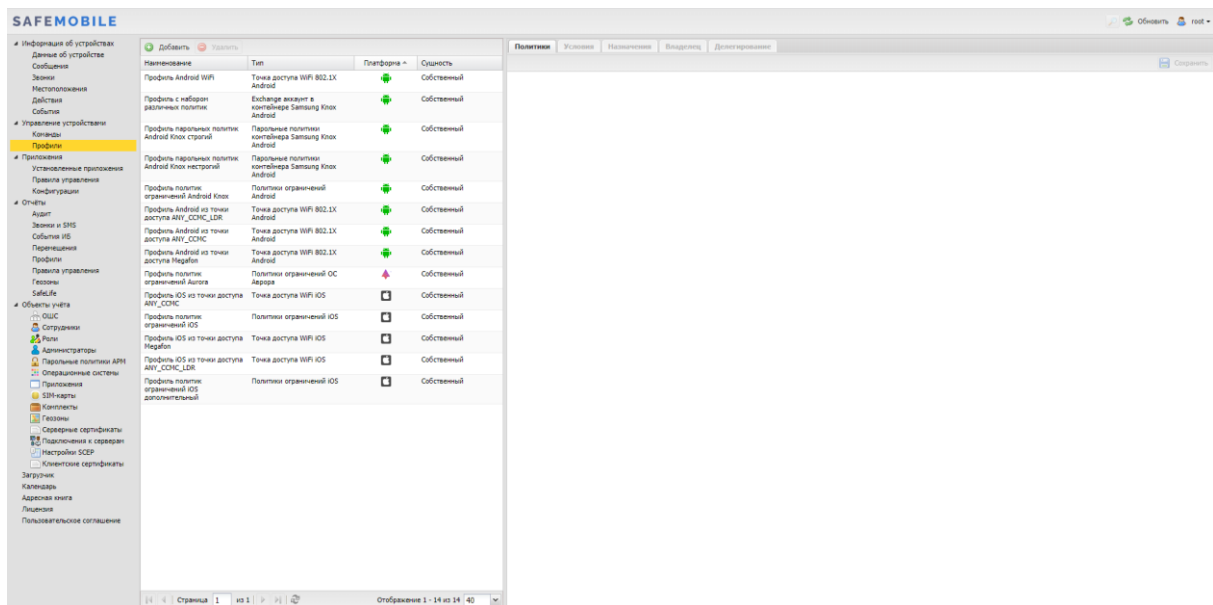


Рисунок 2.36 – Окно «Профили»

В верхней части таблицы находится панель инструментов со следующими кнопками:

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

2.6.8.1 Добавление профиля

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 2.37.

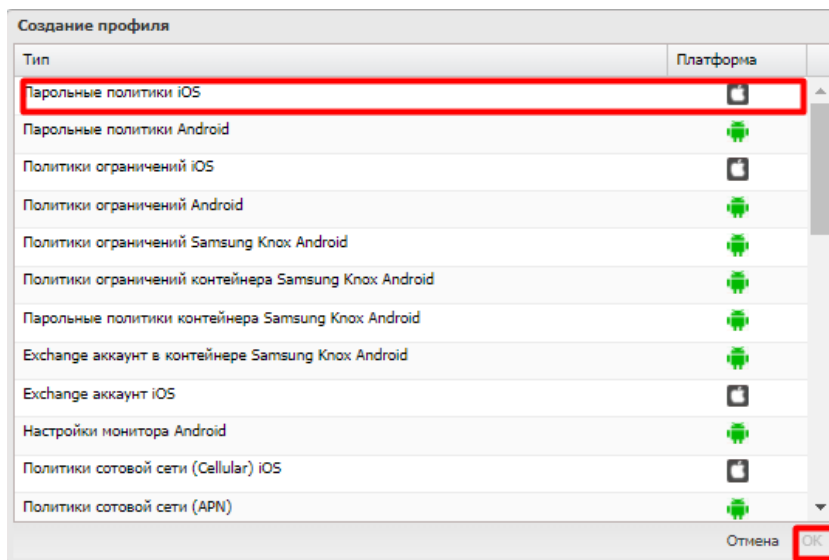


Рисунок 2.37 – Создание профиля

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.

• Платформа Android:

- Парольные политики. Требования к паролю доступа к МСК.
- Политики ограничений. Ограничение возможностей ОС и встроенных приложений.
- Настройки монитора. Параметры работы мобильного клиента SafeMobile.

- Политики сотовой сети (APN). Настройка мобильного интернета.
 - Режим киоска.
 - Политики управления датой и временем.
 - Точка доступа WiFi 802.1X.
 - Сетевые подключения.
 - Доверенный сертификат.
 - Защита устройства от угроз.
 - Дополнительно для устройств Samsung:
 - Политики ограничений Knox.
 - Парольные политики контейнера Knox1
 - Политики ограничений контейнера Knox1. Ограничения доступа приложений в контейнере к возможностям устройства и данным вне контейнера.
 - Exchange аккаунт контейнера Knox1.
 - Режим киоска Knox.
 - Ярлык рабочего стола Android. (Применение профиля требует подтверждения от пользователя. Ярлык создается в главном окне. Изменение ссылки (URL) не обновляет существующий ярлык, а приводит к удалению старого и созданию нового ярлыка).
 - Настройки сбора местоположений Android. (При выборе источника данных местоположения «Только датчик GPS» координаты будут собираться даже при отключенном Google Mobile Services).
- **Платформа Аврора**
 - Политики ограничений.
 - Настройки монитора.
 - **Платформа Windows**
 - Парольные политики.
 - Настройки bluetooth.
 - Политики сетевых подключений.
 - Политики ограничений.
 - Политики использования камеры.
 - Политики доступа к настройкам.
 - Политики Defender.
 - Настройки BitLocker.
-

¹ Для доступа к функциям контейнера Knox нужны лицензионные ключи Samsung Knox License key (SKL).

• Платформа SafeLife

- Настройки браслета.

Примечание – На устройствах производства Samsung следует применять политики ограничений Samsung Knox, а политики ограничений Android, следовательно, применять на MCK 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 2.38), следует указать требуемые значения.

The screenshot shows a web-based configuration interface for user profiles. The main tab is 'Политики' (Policies), with other tabs like 'Условия (не заданы)', 'Назначения', 'Владелец', and 'Делегирование'. A 'Сохранить' (Save) button is highlighted in the top right. The form contains the following fields:

- Тип: Парольные политики iOS
- * Наименование: (empty text box)
- Описание: (empty text box)
- Разрешить простые пароли: Нет
- Требовать PIN: Нет
- Пороговое значение неудачных попыток ввода пароля: 11
- Максимальное время неактивности до блокировки экрана паролем (мин): 3
- Срок действия пароля (сут): 93
- Минимальное количество спецсимволов: Не задано
- Минимальная длина пароля: 4
- Наличие букв: Нет
- Минимальное количество смен пароля до его повтора: 5
- Максимальное время, в течение которого доступна разблокировка без ввода пароля (мин): 0

Рисунок 2.38 – 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. Поддерживаются следующие подстановки:

- ***employee.surname*** – фамилия пользователя;
- ***employee.name*** – имя пользователя;
- ***employee.patronymic*** – отчество пользователя;
- ***employee.exchange.emp_email*** – адрес электронной почты;
- ***employee.exchange.emp_email_login*** – логин электронной почты;
- ***employee.exchange.emp_email_domain*** – домен.

В каждом строковом параметре допускается использование одной или нескольких подстановок. Подстановки указываются в двойных фигурных скобках. Например, для того чтобы значение параметра содержало домен\логин пользователя, нужно указать следующую строку:

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

Добавление идентификаторов приложений

При выборе «**Политики ограничений iOS**» для параметров «**Список идентификаторов приложений...**» требуется указать идентификатор(ы) одного или нескольких 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

The screenshot displays the 'Условия (не заданы)' (Conditions (not set)) tab. It contains the following elements:

- Ownership (Принадлежность МСК):** A dropdown menu set to 'Любая' (Any) with a delete icon (X).
- Strategy (Стратегия):** A dropdown menu with the text 'Выберите стратегию управления' (Select management strategy).
- Location inside geofence (Нахождения внутри геозоны):** A dropdown menu with the text 'Выберите геозону...' (Select geofence...).
- Location outside geofence (Нахождения вне геозоны):** A dropdown menu with the text 'Выберите геозону...' (Select geofence...).
- OS range selection (Выбор диапазонов ОС):** A section with a delete icon (X).
- Allowed OS range selection (Выбор диапазона разрешенных ОС):** Two dropdown menus for 'Выберите начальную версию ОС' (Select initial OS version) and 'Выберите конечную версию ОС' (Select final OS version), followed by a 'Создать' (Create) button.
- Forbidden OS range selection (Выбор диапазона запрещенных ОС):** Two dropdown menus for 'Выберите начальную версию ОС' (Select initial OS version) and 'Выберите конечную версию ОС' (Select final OS version), followed by a 'Создать' (Create) button.

Рисунок 2.39 – Условия применения профиля

После заполнения формы профиля нажать кнопку **«Сохранить»** и, после подтверждения действия, выбрать вкладку **«Условия»** в соответствии с рисунком 2.39.

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

- Принадлежность МСК (любая/личная/корпоративная);
- Стратегия (только устройство/устройство и контейнер KNOX/персональный рабочий профиль/корпоративный рабочий профиль);
- Нахождение внутри геозоны (название геозоны);
- Нахождение вне геозоны (название геозоны);

Для возможности применения геозона должна быть активирована. Описание работы с геозонами приведено в 2.8.10.

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»**.

2.6.8.4 Назначение профиля

Для назначения профиля во вкладке **«Назначения»** (рисунок 2.40) в окне ОШС выбрать подразделение(я)/сотрудника(ов) или в главной таблице выбрать одно или несколько МСК сотрудников.

msc	Телефон	Сотрудник	Должность	Отдел/Группа	Статус
109		Гагарин Юрий Алексеевич	Ведущий специалист	Группа проектирования	Назначено
104		Иванова Галина Михайловна	Главный специалист	Группа исполнения	Назначено
106	+70000000020	Иванов Александр Васильевич	Специалист	Группа исполнения	Назначено
108		Королев Сергей Павлович	Ведущий специалист	Группа исполнения	Назначено
112		Невский Александр Ярославич	Ведущий специалист (rtls)	Группа проектирования	Назначено
101	+375660000321	Петров Василий Федорович	Директор	ООО "Компания"	Исключено
105		Сидоров Василий Петрович	Специалист	Группа проектирования	Исключено
113		Суворов Александр Васильевич	Ведущий специалист (rtls)	Группа проектирования	Назначено

Рисунок 2.40 – 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 2.41 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 2.42. У объекта ОШС может быть только один владелец для управления сущностями.

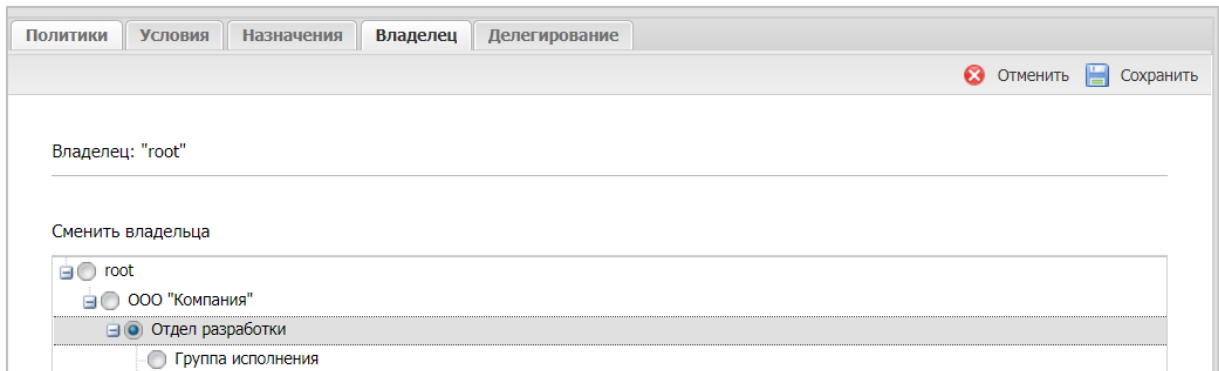


Рисунок 2.41 – Смена владельца сущности

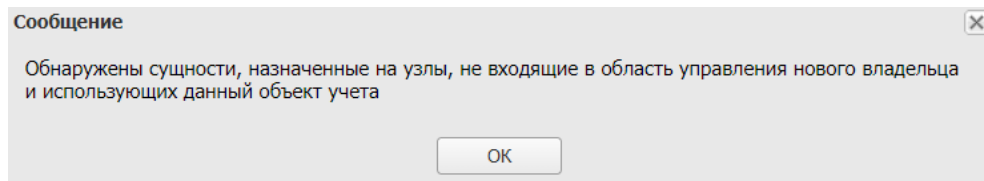


Рисунок 2.42 – Сообщение об ошибке при смене владельца сущности

Для отмены действий для смены владельца сущности следует нажать **«Отменить»**.

2.6.8.6 Делегирование сущности

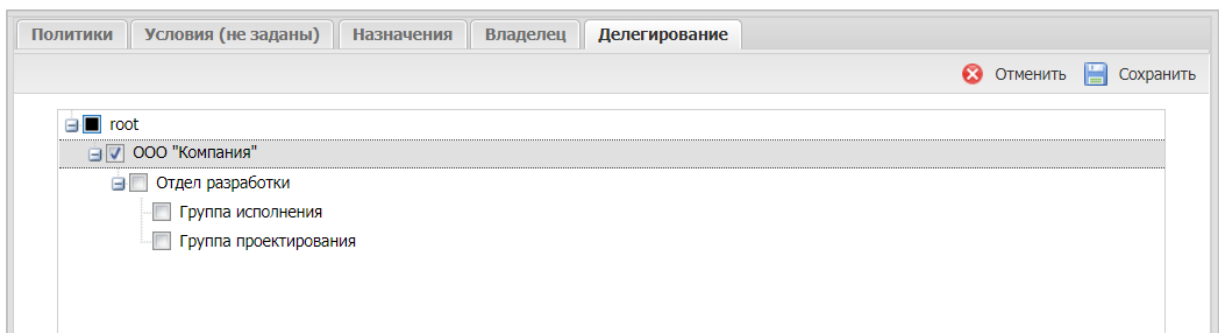


Рисунок 2.43 – Делегирование сущности

Во вкладке **«Делегирование»**, для передачи прав на управление назначением сущности администраторам узла ОШС (на рисунке 2.43 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 ARMe в окне с реестром профилей будет отображаться как «Делегированная» в столбце «Сущность».

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

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 следующих типов: 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, будут применяться политики назначенные на ближайшие к МСК родительские узлы в дереве ОШС;

–при назначении нескольких профилей следующих типов: Exchange аккаунт в контейнере Samsung Knox Android, Exchange аккаунт iOS, доверенный сертификат iOS, доверенный сертификат Android, точка доступа WiFi iOS, точка доступа WiF 802.1x Android, политики Cellular iOS на МСК будет применено то количество аккаунтов, которое было назначено;

–при назначении нескольких профилей типа Политики сотовой сети (APN) Samsung Knox Android, на МСК эти профили будут применены, но пользователю следует самостоятельно выбрать значения, которые будут действовать.

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 не применяются другие профили;
- устройство не выполняет команды, кроме блокировки и отключения от управления.

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 осуществляются 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.

2.6.9 Раздел «Установленные приложения»

Раздел **«Установленные приложения»** (рисунок 2.44) 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.

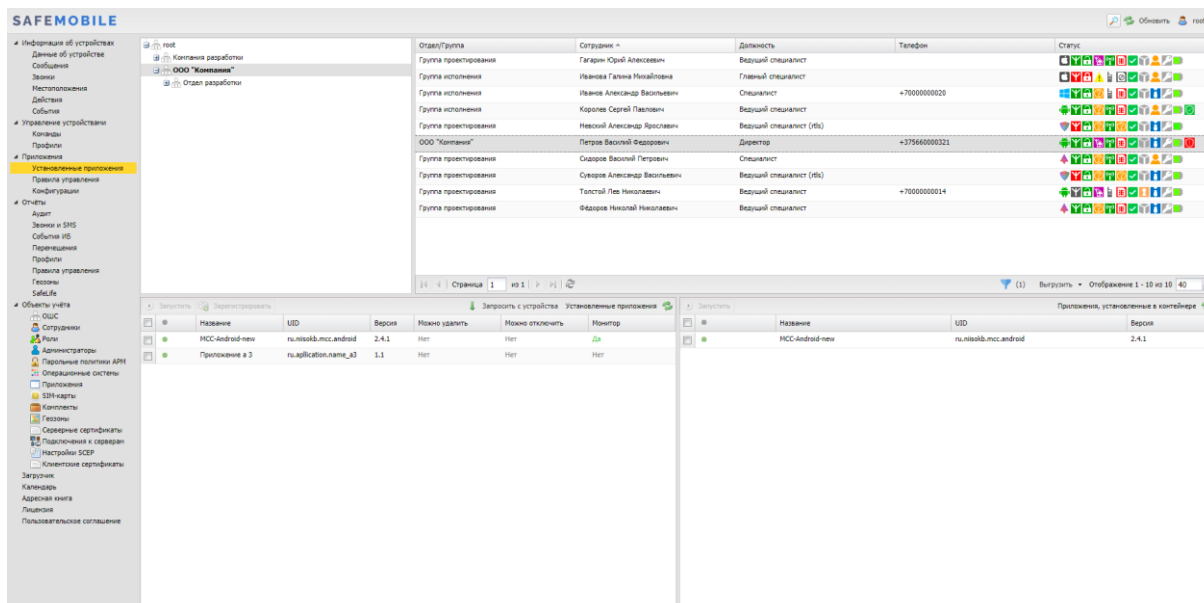


Рисунок 2.44 – Раздел «Управление приложениями»

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

Таблица «Установленные приложения» содержит следующие столбцы:

- – признак угрозы, по умолчанию, не отображается в форме;
- – состояние установленного приложения (– включено, – выключено).

Приложение на МСК устанавливается в состоянии «включено»;

- **Название** – название установленного приложения;
- **UID** – уникальный идентификатор приложения;
- **Версия** – версия установленного 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 2.6.10.

Кнопки, расположенные на панели таблицы «Установленные приложения», позволяют Администратору отправить с APM 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, регистрируется 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);
- **Название** – название установленного приложения;
- **UID** – уникальный идентификатор приложения;
- **Версия** – версия установленного приложения.

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

2.6.10 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»**.

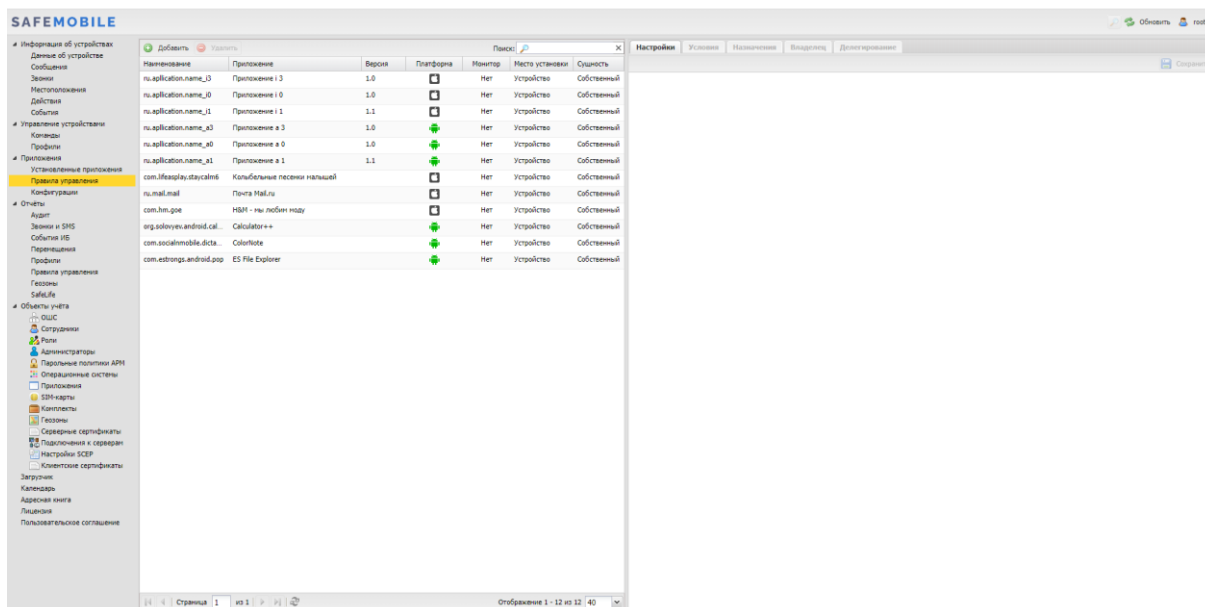


Рисунок 2.45 – Раздел «Правило управления»

В левой части окна «Правила управления» (рисунок 2.45) отображается форма с реестром созданных в системе ПУП, таблица реестра содержит следующие столбцы:

- **Наименование** – название правила (по умолчанию, отображается в форме);
- **Приложение** – название приложения (по умолчанию, отображается в форме);
- **UID** – уникальный идентификатор приложения, которому назначено ПУП;
- **Версия** – версия приложения (по умолчанию, отображается в форме);
- **Платформа** – платформа ОС (по умолчанию, отображается в форме);
- **Монитор** – мобильный клиент SafeMobile (Да/Нет; по умолчанию, отображается в форме);
- **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)
- **Место установки** – Выбор места установки приложения доступен только для платформы Android. Для прочих платформ место установки всегда – «устройство». (устройство / контейнер по умолчанию, отображается в форме).
- **Приложение должно быть включено** – только для МСК на платформе Android (Да/Нет/Не задано);
- **Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении** – только для МСК на платформе Android (Да/Нет);
- **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);

- **Сущность** – инициатор сущности (собственный/делегированный; по умолчанию, отображается в форме);

- **Владелец** – администратор узла ОШС, назначенный владельцем сущности.

В правой части окна отображается форма для настройки параметров ПУП с 5 вкладками:

- **Настройки;**
- **Условия/Условия (не заданы);**
- **Назначения;**
- **Владелец;**
- **Делегирование.**

В верхней части таблицы находится панель инструментов со следующими кнопками:

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

2.6.10.1 Добавление ПУП

Для добавления нового ПУП в реестр нажмите кнопку **«Добавить»**, после чего откроется новая форма во вкладке **«Настройки»** в соответствии с рисунком 2.46. Поля, отмеченные * обязательные для заполнения.

The screenshot shows the 'Настройки' (Settings) tab for creating a new configuration profile for Android. The form contains the following fields and options:

- Название** (Name): An empty text input field.
- Платформа** (Platform): A dropdown menu set to 'Android'.
- Место установки** (Location): A dropdown menu set to 'Устройство' (Device).
- Тип приложения** (Application Type): A dropdown menu set to 'Корпоративное' (Corporate).
- UID**: A text input field containing 'ru.niisokb.mcc.android'. Below it, the text 'Приложение: "MCC-Android-new". Версия: 2.4.1' is displayed.
- Описание** (Description): An empty text area.
- Приложение должно быть установлено** (Application must be installed): A dropdown menu set to 'Да' (Yes).
- Удалить с устройства при отключении от управления** (Delete from device when management is turned off): A dropdown menu set to 'Да' (Yes).
- Приложение должно быть включено** (Application must be enabled): A dropdown menu set to 'Да' (Yes).

A 'Сохранить' (Save) button is located in the top right corner of the settings panel.

Рисунок 2.46 – Форма новой конфигурации (для платформы Android)

Форма для создания новой конфигурации различна для МСК на платформе iOS и Android. Зависимость параметров ПУП при выборе платформы приведена в таблице 2.4.

Публикация приложения в SafeStore

Установка в SafeStore доступна только для корпоративных приложений. Для этого, при добавлении ПУП во вкладку «Настройки» следует выбрать параметр **«Приложение должно быть установлено»** со значением **«Доступно в SafeStore»** в соответствии с таблицей 2.4. Для функционирования SafeStore на платформе Android, на МСК должно быть установлено приложение SafeStore, в то же место на устройстве, где был установлен Монитор. Для стратегий управления устройством: корпоративный / персональный рабочий профиль, местом установки приложений Монитор и SafeStore должен быть контейнер. Для стратегий: только устройство / устройство и контейнер KNOX, местом установки приложений Монитор и SafeStore должно быть устройство. Для исключения попадания приложения SafeStore в контейнер KNOX рекомендуется для ПУП SafeStore с местом установки «Контейнер» задавать условие применения стратегии: корпоративный и персональный рабочие профили.

Параметры ПУП в таблице 2.4 расположены в приоритетном порядке слева направо, а именно: выбор значений в столбцах слева может определить значения для параметров в последующих столбцах. В этом случае в поле приведено только одно значение, без возможности выбора.

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	
	Некорпоративное	Да (по умолчанию) Не задано		Да (по умолчанию) Нет		Да (по умолчанию) Нет	Да (по умолчанию) Нет Не задано
		Нет		Нет		Нет	Нет
	Корпоративное	Да (по умолчанию)	-	-	-	-	-

При создании ПУП необходимо учитывать следующие правила:

- а) если в таблице для приложения стоит значение «Нет» для параметра «Приложение должно быть на устройстве», то приложение, установленное пользователем, будет автоматически удалено с устройства, а при невозможности удаления – отключено;
- б) если в таблице для приложения на МСК платформы iOS без «supervised» стоит значение «Да», то для действия с ним будет запрошено подтверждение пользователя;
- в) для исключения несанкционированного распространения корпоративных данных через некорпоративные приложения, установленные на МСК платформы iOS в ПУП следует установить значения «Да» для параметров: **«Приложение можно настраивать удалённо»**, **«Удалить с устройства при отключении от управления»**, **«Запрещено резервное копирование данных»**.
- г) 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.

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

2.6.10.2 Задание условий применения ПУП

После заполнения формы ПУП и сохранения настроек выбрать условия применения ПУП во вкладке **«Условия»** (рисунок 2.47) в соответствии с описанием задания условий применения профиля раздел 2.6.8.3

Рисунок 2.47 – Условия применения ПУП

2.6.10.3 Назначение ПУП

Для назначения ПУП во вкладке **«Назначения»** (рисунок 2.48) 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.

msc	Телефон	Сотрудник	Должность	Отдел/Группа	Статус
109		Гагарин Юрий Алексеевич	Ведущий специалист	Группа проектирования	[Icons]
104		Иванова Галина Михайловна	Главный специалист	Группа исполнения	[Icons]
106	+70000000020	Иванов Александр Васильевич	Специалист	Группа исполнения	[Icons]
108		Королев Сергей Павлович	Ведущий специалист	Группа исполнения	[Icons]
112		Невский Александр Ярославич	Ведущий специалист (rtls)	Группа проектирования	[Icons]
101	+375660000321	Петров Василий Федорович	Директор	ООО "Компания"	[Icons]

Рисунок 2.48 – Назначение ПУП

Для сохранения назначения ПУП в системе нажать на кнопку **«Сохранить»**.

2.6.10.4 Смена владельца сущности

Для смены владельца сущности во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.49) в окне ОШС в соответствии с 2.6.8.5.

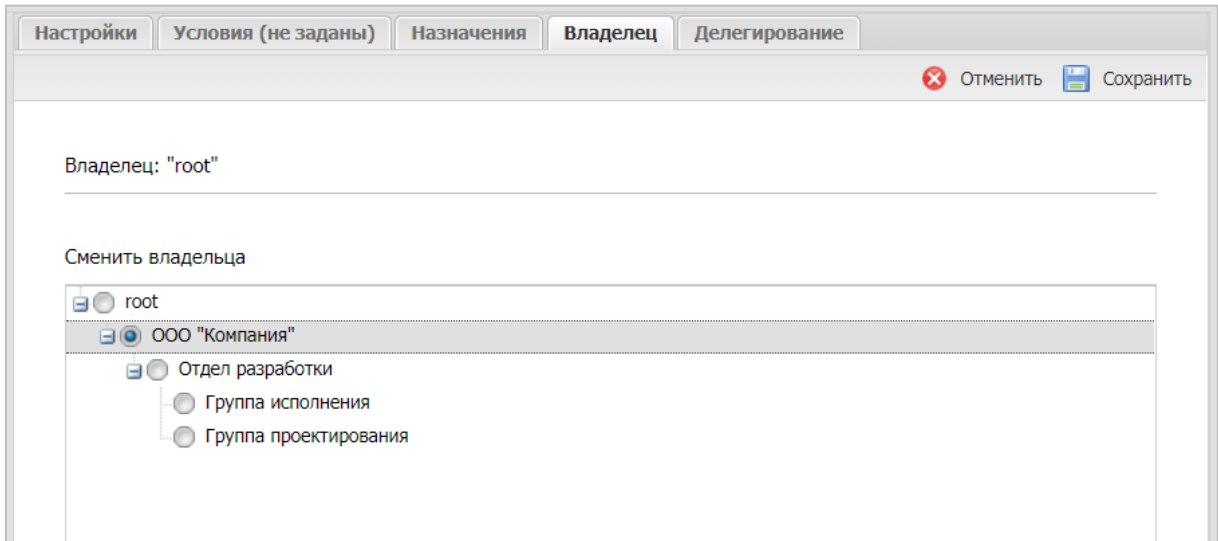


Рисунок 2.49 – Смена владельца сущности

2.6.10.5 Делегирование сущности

Для делегирования сущности во вкладке **«Делегирование»** следует выбрать один или несколько объектов ОШС (рисунок 2.50) в окне ОШС в соответствии с 2.6.8.6.

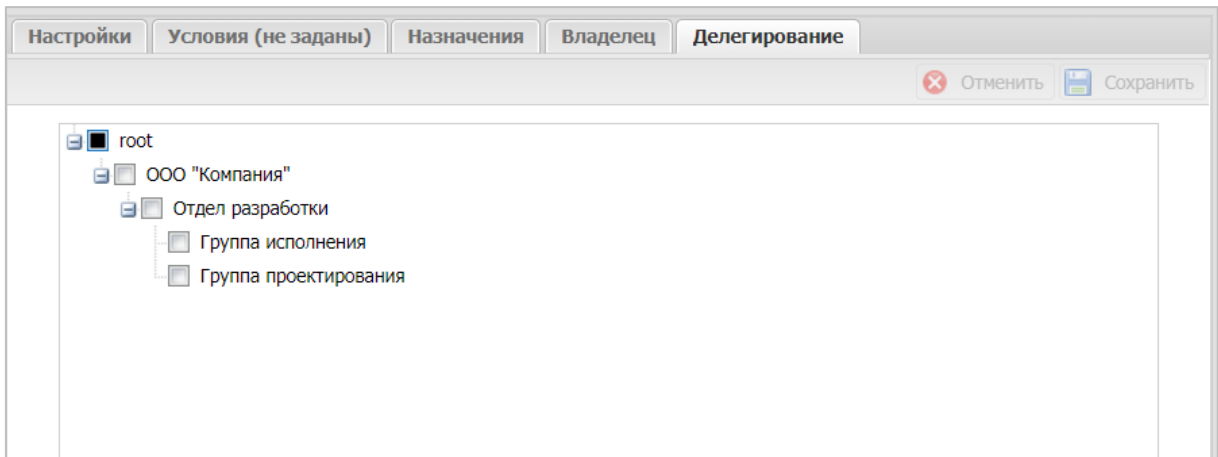


Рисунок 2.50 – Делегирование сущности

2.6.10.6 Применение ПУП

При добавлении ПУП следует учитывать, что профили имеют больший приоритет перед ПУП. Например, если в примененном профиле присутствуют политики, запрещающие отдельные приложения, в ПУП эти приложения разрешает, то в этом случае приложение будет запрещено.

Для приложений на МСК платформы iOS после применения ПУП с параметром **«Приложение можно настраивать удалённо»**, невозможно обратное действие: сделать приложение неуправляемым.

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.

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.

2.6.10.7 Особенности при удалении ПУП

Для приложений на МСК платформы Android существует следующая особенность корпоративного ПУП, предназначенного для обновления системного приложения (встроенного приложения от производителя устройства). Если удалить данный 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.

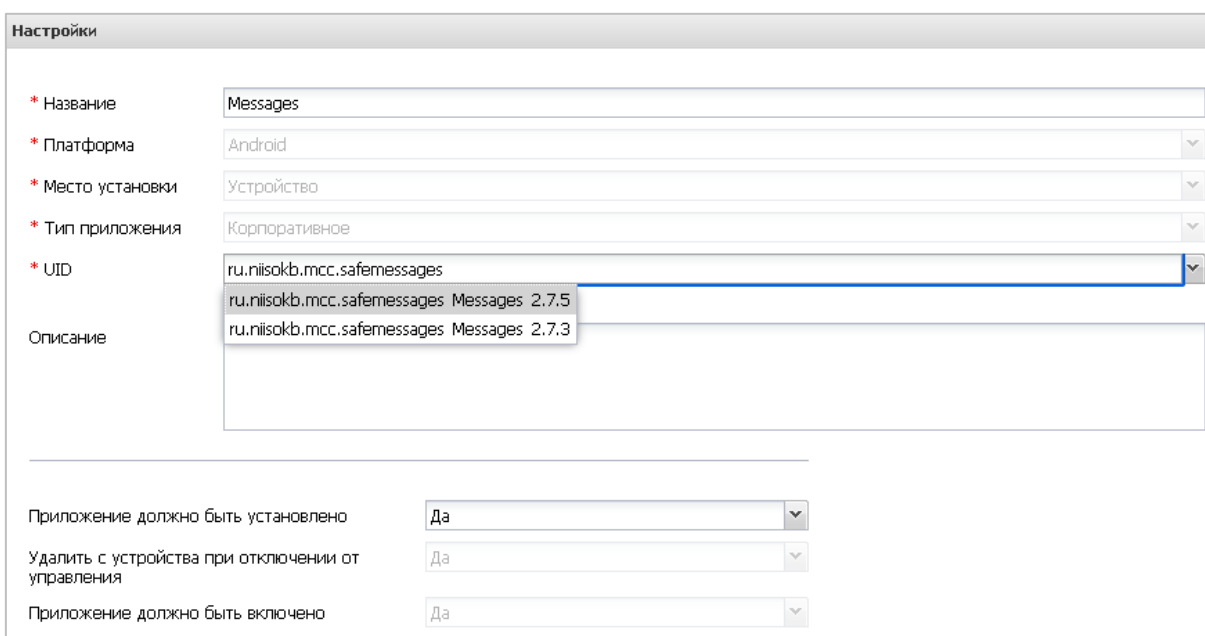
2.6.10.8 Особенности обновления приложений

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 **Ошибка! Источник ссылки не найден..**



Настройки

* Название: Messages

* Платформа: Android

* Место установки: Устройство

* Тип приложения: Корпоративное

* UID: ru.niisokb.mcc.safemessages

Описание: ru.niisokb.mcc.safemessages Messages 2.7.5
 ru.niisokb.mcc.safemessages Messages 2.7.3

Приложение должно быть установлено: Да

Удалить с устройства при отключении от управления: Да

Приложение должно быть включено: Да

Рисунок 2.51 – 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.

2.6.11 Раздел «Конфигурации»

Пункт меню «**Конфигурации**» открывает окно (рисунок 2.52), 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.

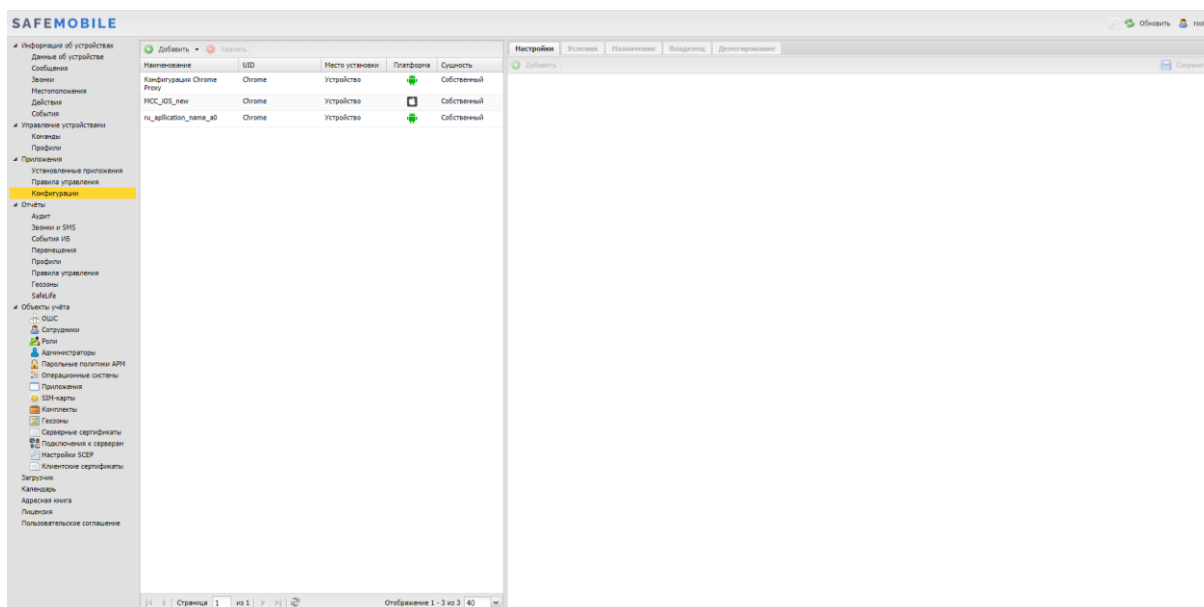


Рисунок 2.52 – Окно «Конфигурации»

Управление конфигурациями приложений осуществляется для МСК следующих платформ:

- iOS версий 10 и выше;
- с Device Owner на платформе Android версии 6.0 и выше;
- с Knox версии 2.7 и выше на платформе Android версии 5.0 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.

2.6.11.1 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 2.53. Поля, отмеченные * обязательные для заполнения.

Настройка	Значение
* Название	Конфигурация Chrome Proxy
* Платформа	Android
* Место установки	Устройство
* UID	com.android.chrome
Описание	Конфигурация

Рисунок 2.53 – Форма новой конфигурации

Для добавления параметров настройки приложения нажать кнопку «Добавить», после чего отобразится форма (рисунок 2.54).

Создание настройки конфигурации

* Ключ: alwaysOn

* Название: Автозапуск VPN после перезагрузки устройства

Описание:

* Тип значений: Логический

Строка

Логический

Целое число

Вещественное число

Массив целых чисел

Массив вещественных чисел

Массив строк

Отмена ОК

Рисунок 2.54 – 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.

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 2.55) доступен список с уже созданными шаблонами настроек.

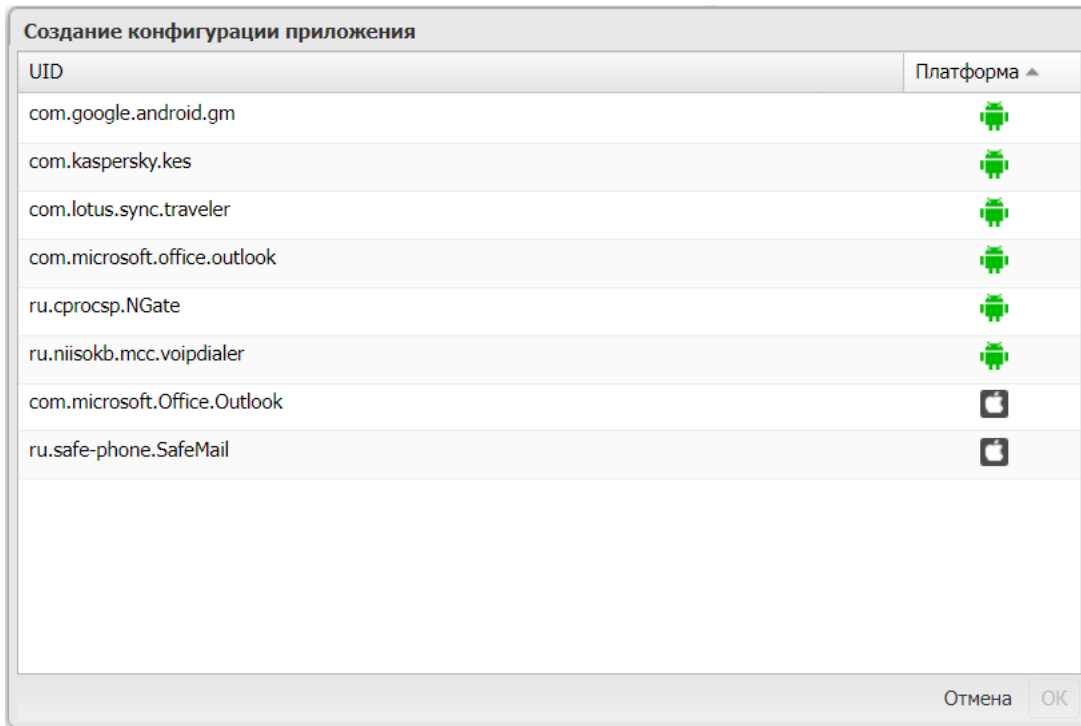


Рисунок 2.55 – Создание конфигурации приложения

В системе представлены следующие шаблоны с настройками приложений:

- com.google.android.gm – Gmail (android);
- com.kaspersky.kes – Антивирус Касперского (android);
- com.lotus.sync.traveler – Клиент Lotus (android);
- com.microsoft.office.outlook – Microsoft Outlook (android);
- ru.cprosp.NGate – VPN (android);
- ru.niisokb.mcc.voipdialer – ЗАС-Телефон (android);
- com.microsoft.Office.Outlook – Microsoft Outlook (iOS);
- ru.safe-phone.SafeMail – ЗАС-Почта (iOS).

В списке следует выбрать требуемый шаблон, нажать кнопку «**OK**» для продолжения настроек конфигурации в форме (рисунок 2.53) и возможности редактирования параметров. Параметры конфигурации в форме будут зависеть от выбранного шаблона

Пример шаблона КП **SafeMail** с параметрами приведен на рисунке 2.56.

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

* Название	<input type="text" value="Почта"/>
* Платформа	<input type="text" value="Android"/>
* Место установки	<input type="text" value="Устройство"/>
* UID	<input type="text" value="com.microsoft.office.outlook"/>
Описание	<input type="text"/>
Отображаемое имя	<input type="text" value="{{employee.exchange.emp_email}}"/>
Адрес электронной почты (user@companyname.com)	<input type="text" value="{{employee.exchange.emp_email}}"/>
Логин пользователя на сервере (user)	<input type="text" value="{{employee.exchange.emp_email_login}}"/>
Способ аутентификации (SSL)	<input type="text" value="SSL"/>
Имя сервера (exchange.companyname.com)	<input type="text" value="Не задано"/>
Имя домена (companyname)	<input type="text" value="{{employee.exchange.emp_email_domain}}"/>
Тип учетной записи (BasicAuth)	<input type="text" value="BasicAuth"/>
UPN учетной записи Office365 ()	<input type="text" value="Не задано"/>

Рисунок 2.56 – Шаблон КП SafeMail

2.6.11.2 Назначение конфигурации

Для назначения конфигурации во вкладке **«Назначения»** (рисунок 2.57) 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.

Настройки Условия (не заданы) Назначения Владелец Делегирование							Сохранить	
msc	Телефон	Сотрудник ^	Должность	Отдел/Группа	Статус			
109		Гагарин Юрий Алексеевич	Ведущий специалист	Группа проектирования		<input type="checkbox"/>		
104		Иванова Галина Михайловна	Главный специалист	Группа исполнения		<input type="checkbox"/>		
106	+70000000020	Иванов Александр Васильевич	Специалист	Группа исполнения		<input type="checkbox"/>		
108		Королев Сергей Павлович	Ведущий специалист	Группа исполнения		<input type="checkbox"/>		
112		Невский Александр Ярославич	Ведущий специалист (rtls)	Группа проектирования		<input type="checkbox"/>		
101	+375660000321	Петров Василий Федорович	Директор	ООО "Компания"		<input type="checkbox"/>		
105		Сидоров Василий Петрович	Специалист	Группа проектирования		<input type="checkbox"/>		
113		Суворов Александр Васильевич	Ведущий специалист (rtls)	Группа проектирования		<input type="checkbox"/>		
111	+70000000014	Толстой Лев Николаевич	Ведущий специалист	Группа проектирования		<input type="checkbox"/>		
107		Фёдоров Николай Николаевич	Ведущий специалист	Группа проектирования		<input type="checkbox"/>		

Рисунок 2.57 – Назначение конфигурации

Для сохранения назначения конфигурации в системе нажать на кнопку **«Сохранить»**.

2.6.11.3 Смена владельца сущности

Для смены владельца сущности во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.58) в окне ОШС в соответствии с 2.6.8.5.

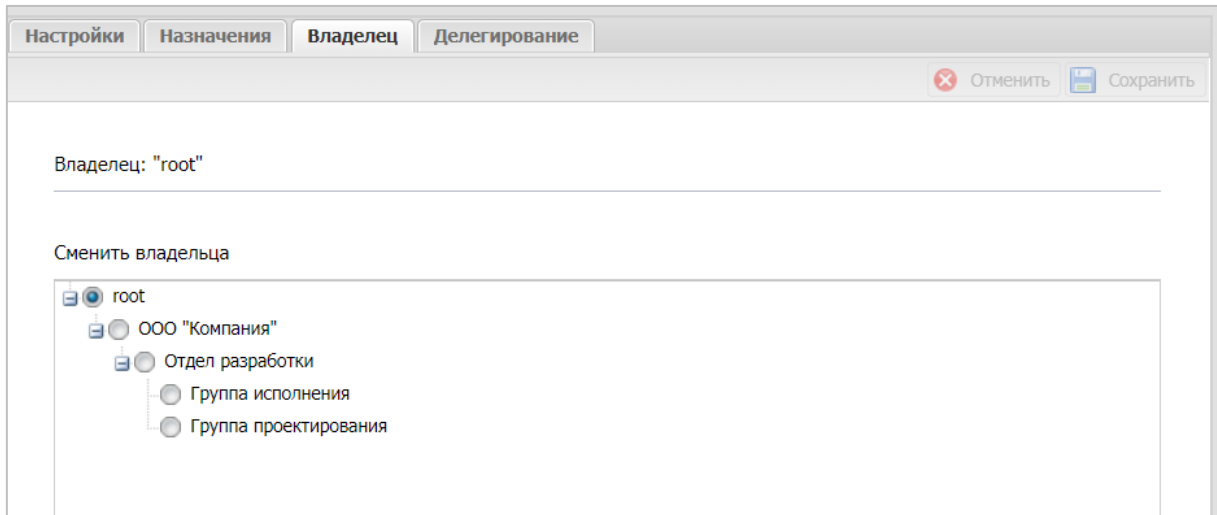


Рисунок 2.58 – Смена владельца сущности

2.6.11.4 Делегирование сущности

Для делегирования сущности во вкладке **«Делегирование»** следует выбрать один или несколько объектов ОШС (рисунок 2.59) в окне ОШС в соответствии с 2.6.8.6.

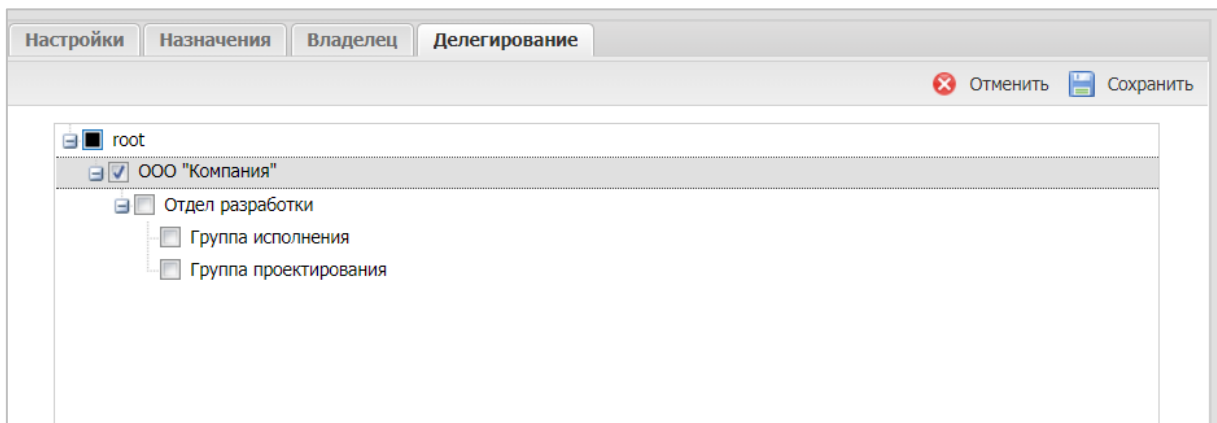


Рисунок 2.59 – Делегирование сущности

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;
- 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 2.60.

Администратор	Имя пользователя	Место работы	Должность	Область управления	Действие	Тип операции	Время	Результат
Администратор	root	Внешний		root	Проверка необходимости смены пароля администратора	Чтение	01.11.2021 19:25:48	Успешное завершение
Администратор	root	Внешний		root	Регистрация результата логина администратора	Запись	01.11.2021 19:25:48	Успешное завершение
Администратор	root	Внешний		root	Аутентификация администратора	Запись	01.11.2021 19:25:48	Успешное завершение
Администратор	root	Внешний		root	Выход администратора	Запись	01.11.2021 19:22:22	Успешное завершение
Администратор	root	Внешний		root	Запрос списка сотрудников	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Запрос списка сотрудников	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Запрос списка сотрудников	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Запрос списка паролей (loc)	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Отчет События информационной безопасности	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение списка сертификатов для соединения с сервером EMM	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Отчет о вкладах/выпадах из геозоны	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:23	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение
Администратор	root	Внешний		root	Получение области управления администратора или поддерева OUS внутри области управления	Чтение	01.11.2021 18:51:24	Успешное завершение


Рисунок 2.60 – 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;
- **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 2.61), открывающееся нажатием кнопки **«Настроить фильтры»** в верхней панели инструментов.

В окне настроек параметров отчёта можно выбрать период, для которого создаётся отчёт. Для этого 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 конца отчёта по аудиту действий администраторов в системе.

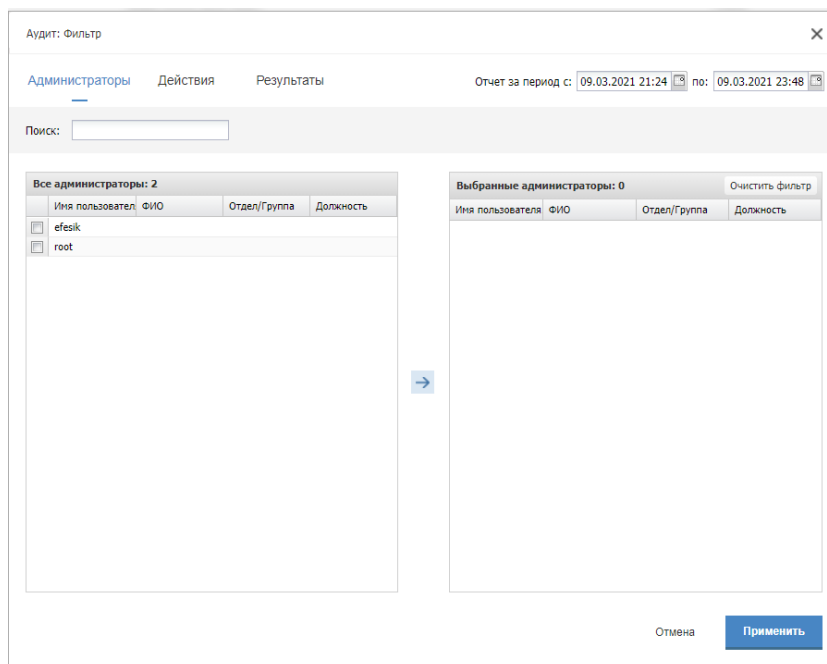


Рисунок 2.61 – Окно настроек параметров отчёта «Аудит»

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 2.62) 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.

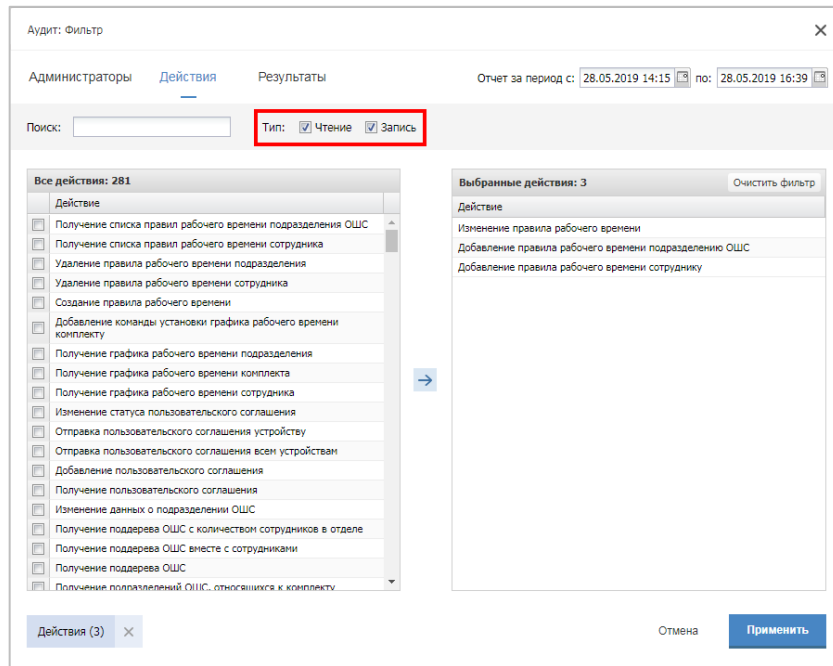


Рисунок 2.62 – Окно «Действия» в настройках параметров отчёта «Аудит»

Для осуществления поиска по ключевому слову в реестрах параметров отчёта «Аудит» предназначено окно «Поиск» (рисунок 2.63).

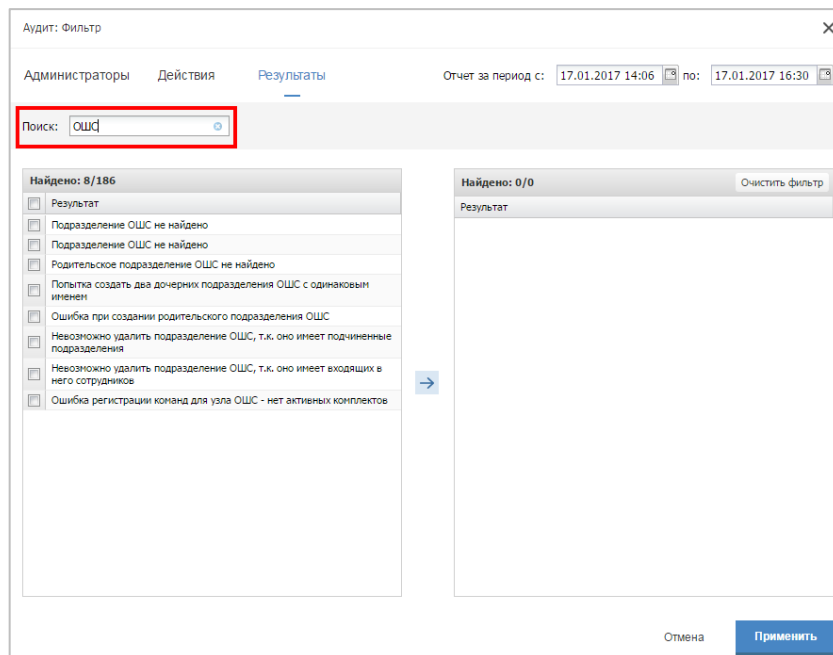


Рисунок 2.63 – Окно «Поиск» в настройках параметров отчёта «Аудит»

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 2.64) отображается таблица с перечнем звонков и SMS-сообщений за заданный период времени.

Сотрудник	Телефон	Исходящие			Входящие		
		Количество	Время	SMS	Количество	Время	SMS
Василин Пётр Викторович	+70000000003	1	1	0	0	0	0
Петров Василий Петрович	+37566000321	7	6	1	3	4	2
Сидоров Василий Петрович		1	2	1	3	4	0
Семенов Николай Николаевич		2	3	4	1	2	0

Рисунок 2.64 – 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;
- **Телефон** – номер телефона SIM-карты устройства;
- **Количество** – количество входящих и исходящих звонков;
- **Время** – общая продолжительность входящих и исходящих соединений;
- **SMS** – количество входящих и 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 2.65.

id	Время	Описание	Сотрудник
103	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Василен Петр Викторович
103	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Василен Петр Викторович
103	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Василен Петр Викторович
103	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Василен Петр Викторович
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
109	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Гагарин Юрий Алексеевич
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
102	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Данилов Григорий Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
108	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Королев Сергей Павлович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович
101	01.11.2021 11:20:50	Сброс MTC к заводским настройкам	Петров Василий Федорович

Рисунок 2.65 – 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.

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 2.66.

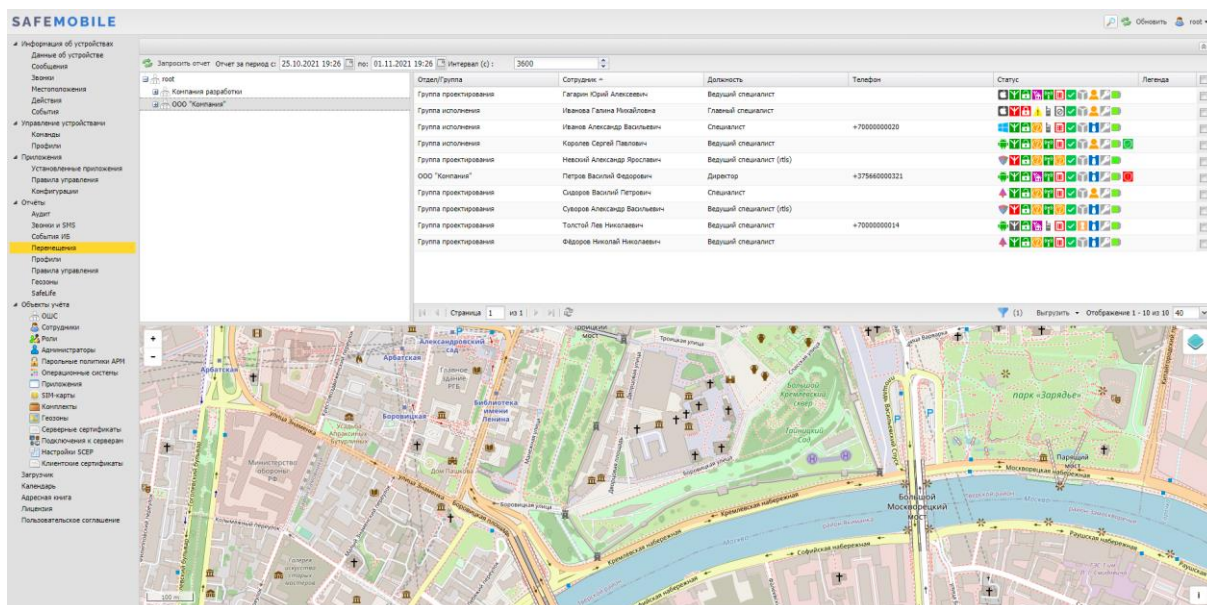


Рисунок 2.66 – Окно «Перемещения»

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, применённых на подключённых к системе МСК. Отчёт состоит из двух таблиц: верхняя таблица с реестром назначенных и применённых профилей; а в нижней таблице воспроизводятся установленные и применённые на МСК значения параметров политик выбранного профиля в соответствии с рисунком 2.67.

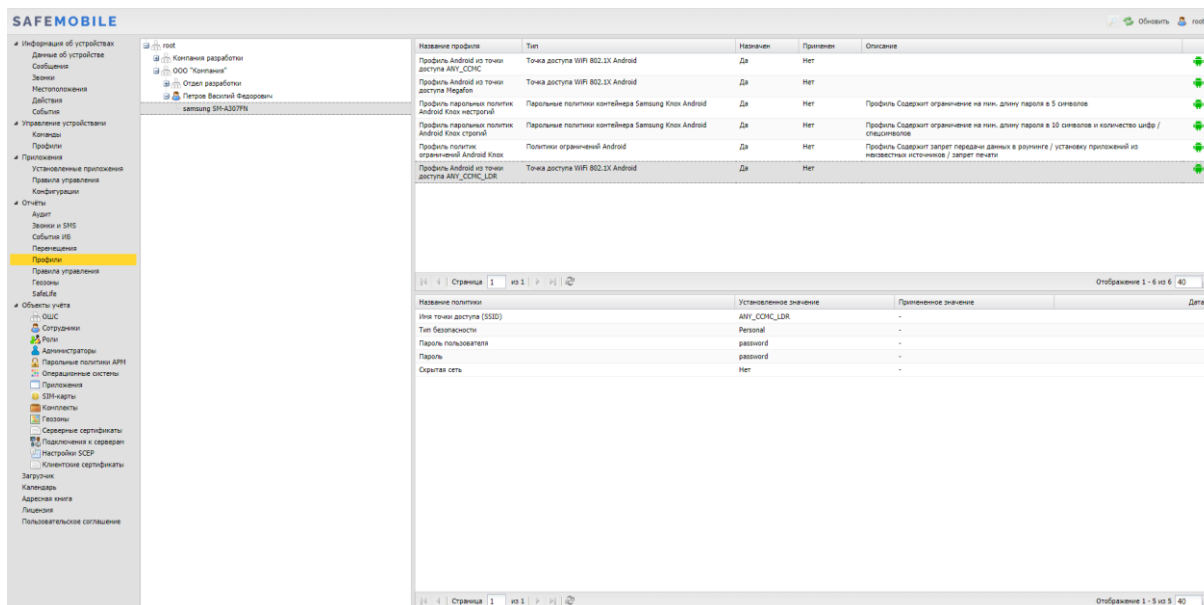


Рисунок 2.67 – Окно отчёта «Профили»

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.

Нижняя таблица отчёта содержит следующие столбцы:

- **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.

2.7.6 Отчёт «Правила управления»

В отчёте отображается информация о ПУП, применённых 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 применённые на МСК значения параметров ПУП в соответствии с рисунком Рисунок 2.68.

Правило управления	Приложение	UID	Контейнер	Цель	Платформа	Описание	Условия	На устройстве
ru.application.name_a3	Приложение в 3	ru.application.name_a3	Устройство	доступно в Safemobile	Android		Выполнено	1.1
ru.application.name_a0	Приложение в 0	ru.application.name_a0	Устройство	1.0	Android		Выполнено	
ru.application.name_a1	Приложение в 1	ru.application.name_a1	Устройство	1.1	Android		Выполнено	
com.safemobile.dictapps.notes.colonote	Colofite	com.safemobile.dictapps.notes.colonote	Устройство	Некорректна...	Android		Выполнено	

Настройка	Значение
Приложение должно быть установлено	Да
Удалить с устройства при отключении от управления	Да
Приложение должно быть включено (Android)	Да
Приложение должно быть в контейнере (Android)	Нет

Рисунок 2.68 – Окно отчёта «Правила управления»

Верхняя таблица отчёта содержит следующие столбцы:

- **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;
- **Статус** – Managed / Unmanaged;

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 «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 2.69).

Отдел/Группа	ФИО	Должность	ИМEI	Серийный номер	Платформа	Дата/время	Название геозоны	Событие
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 23:06:09	Zone3	Выход
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 23:01:20	Zone3	Вход
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 22:59:30	Zone3	Выход
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 22:56:46	Zone3	Вход
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 22:55:31	Zone3	Выход
Группа проектирования	Неской Александр Ярославич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 22:40:18	Zone3	Вход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:35:42	Zone3	Выход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:29:27	Zone3	Вход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:27:42	Zone3	Выход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:24:43	Zone3	Вход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:23:01	Zone3	Выход
Группа проектирования	Сукоро Александр Васильевич	Ведущий специалист (ИБ)			SafeLife	31.10.2021 20:09:44	Zone3	Вход
Группа проектирования	Фадоро Николай Николаевич	Ведущий специалист	86735203207696		Android	31.10.2021 13:27:33	Zone3	Выход
Группа исполнения	Иванова Александра Васильевна	Специалист	01269301243344		Windows	31.10.2021 13:26:57	Zone3	Вход
Группа проектирования	Фадоро Николай Николаевич	Ведущий специалист	86735203207696		Android	31.10.2021 13:26:26	Zone3	Выход
Группа исполнения	Иванова Александра Васильевна	Специалист	01269301243344		Windows	31.10.2021 13:24:59	Zone3	Выход
Группа исполнения	Турганев Иван Сергеевич	Ведущий специалист	657364070023209		iPhone OS	31.10.2021 13:24:50	Zone3	Вход
Группа проектирования	Фадоро Николай Николаевич	Ведущий специалист	86735203207696		Android	31.10.2021 13:23:59	Zone3	Вход
Группа исполнения	Турганев Иван Сергеевич	Ведущий специалист	657364070023209		iPhone OS	31.10.2021 13:23:47	Zone3	Выход
Группа исполнения	Иванова Александра Васильевна	Специалист	01269301243344		Windows	31.10.2021 13:23:38	Zone3	Вход
Группа проектирования	Сукоро Александр Васильевич	Специалист	38992080348473		Android	31.10.2021 13:23:18	Zone3	Вход
Группа исполнения	Турганев Иван Сергеевич	Ведущий специалист	657364070023209		iPhone OS	31.10.2021 13:22:23	Zone3	Вход
Группа проектирования	Гардин Юрий Алексеевич	Ведущий специалист	990003078369550	MD52ZRS	iPhone OS	31.10.2021 13:22:16	Zone3	Вход
Группа исполнения	Иванова Александра Васильевна	Специалист	01269301243344		Windows	31.10.2021 13:21:55	Zone3	Выход
Группа проектирования	Толстой Лев Николаевич	Ведущий специалист	269864070027813		Android	31.10.2021 13:21:45	Zone3	Вход
Группа проектирования	Фадоро Николай Николаевич	Ведущий специалист	86735203207696		Android	31.10.2021 13:21:29	Zone3	Выход
Группа проектирования	Сукоро Александр Васильевич	Специалист	38992080348473		Android	31.10.2021 13:21:17	Zone3	Выход
Группа исполнения	Иванова Галина Николаевна	Главный специалист	013372014452344	445234	iPhone OS	31.10.2021 13:20:50	Zone3	Вход
Группа проектирования	Гардин Юрий Алексеевич	Ведущий специалист	990003078369550	MD52ZRS	iPhone OS	31.10.2021 13:20:26	Zone3	Вход
Группа проектирования	Толстой Лев Николаевич	Ведущий специалист	269864070027813		Android	31.10.2021 13:19:38	Zone3	Выход
Группа проектирования	Сукоро Александр Васильевич	Специалист	38992080348473		Android	31.10.2021 13:19:35	Zone3	Вход
Группа проектирования	Васюнин Петр Викторович	Специалист	013372014452344	445234	Android	31.10.2021 13:19:26	Zone3	Вход
Группа исполнения	Турганев Иван Сергеевич	Ведущий специалист	657364070023209		iPhone OS	31.10.2021 13:19:24	Zone3	Вход
Группа исполнения	Королев Сергей Павлович	Ведущий специалист	358363300024595	R389607L9YL	Android	31.10.2021 13:19:03	Zone3	Вход
Группа исполнения	Иванова Галина Николаевна	Главный специалист	013372014452344	445234	iPhone OS	31.10.2021 13:18:50	Zone3	Вход
Группа проектирования	Гардин Юрий Алексеевич	Ведущий специалист	990003078369550	MD52ZRS	iPhone OS	31.10.2021 13:18:43	Zone3	Вход
Группа проектирования	Толстой Лев Николаевич	Ведущий специалист	269864070027813		Android	31.10.2021 13:18:26	Zone3	Вход
Группа исполнения	Королев Сергей Павлович	Ведущий специалист	358363300024595	R389607L9YL	Android	31.10.2021 13:18:12	Zone3	Выход
Группа проектирования	Васюнин Петр Викторович	Специалист	013372014452344	245377	Android	31.10.2021 13:18:10	Zone3	Выход

Рисунок 2.69 – 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;
- **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.

2.7.8 Отчет «SafeLife»

Отчет предназначен для отображения информации по сотрудникам, использующим браслеты «SafeLife» за заданный промежуток времени (рисунок 2.70).

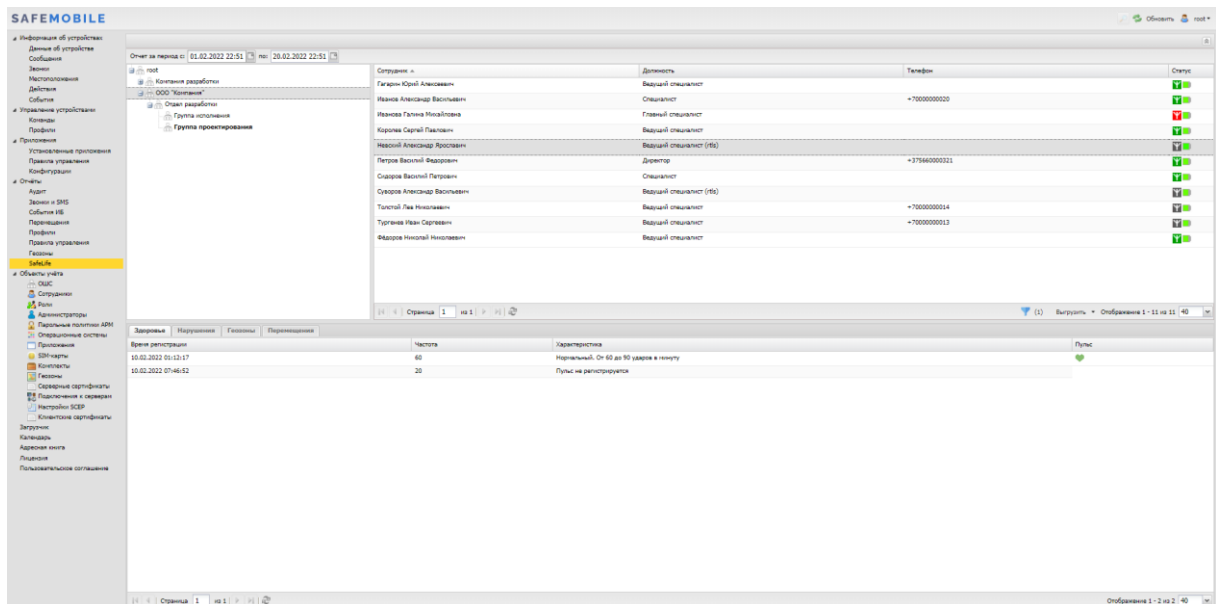


Рисунок 2.70 – Окно «SafeLife»

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 2.71.

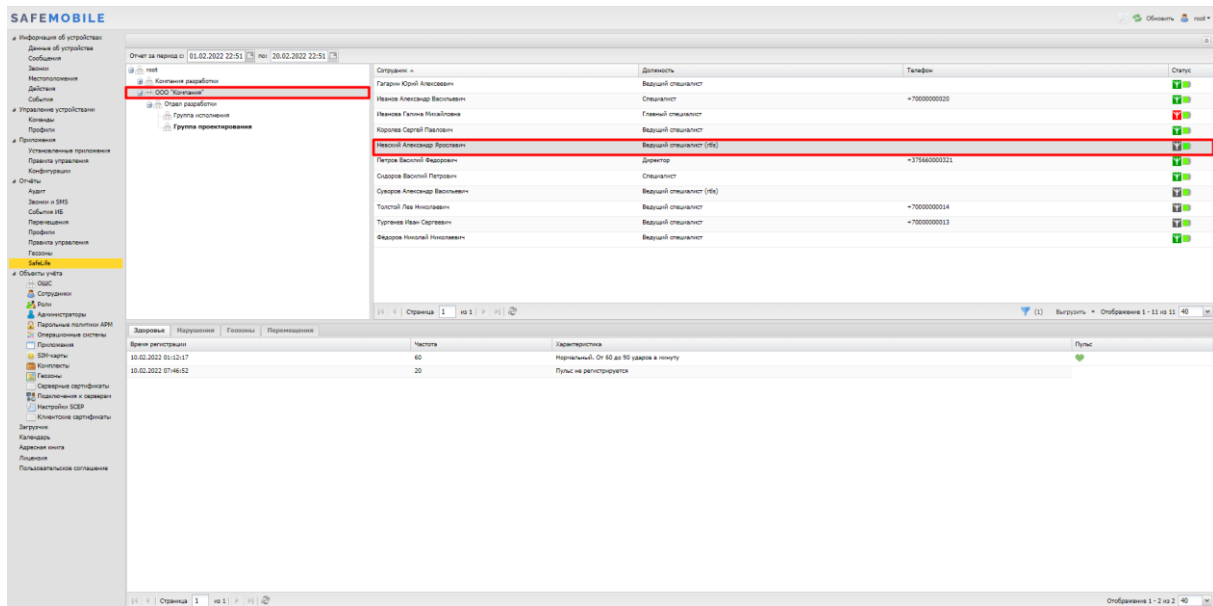


Рисунок 2.71 – Выбор сотрудника для просмотра отчета «SafeLife»

В нижней части расположено окно с отчетами со следующими вкладками:

- **Здоровье;**
- **Нарушения;**
- **Гезоны;**
- **Перемещения.**

На вкладке **«Здоровье»** отображается таблица с показаниями пульса (рисунок 2.72:

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

Время регистрации	Частота	Характеристика	Пuls
10.02.2022 01:12:17	60	Нормальный. От 60 до 90 ударов в минуту	✔
10.02.2022 07:46:52	20	Пuls не регистрируется	

Рисунок 2.72 – Вкладка «Здоровье»

На вкладке «Нарушения» отображается таблица со следующими столбцами (рисунок 2.73):

- **Время регистрации;**
- **Нарушения и уведомления** – наименование нарушения или уведомления: puls не регистрируется/нет движения/puls 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.

Время регистрации	Нарушения и уведомления	Геозоны
10.02.2022 07:46:52	Пuls и движение не регистрируются	-
10.02.2022 07:46:52	Пuls не регистрируется. Меньше 25 ударов в минуту.	-
10.02.2022 07:45:36	Нет движения	-
10.02.2022 07:44:40	Зафиксировано падение	-

Рисунок 2.73 – Вкладка «Нарушения»

На вкладке «Геозоны» отображается таблица учета времени пребывания в гео зонах и карта с гео зонами. Таблица содержит следующие столбцы (рисунок 2.74):

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

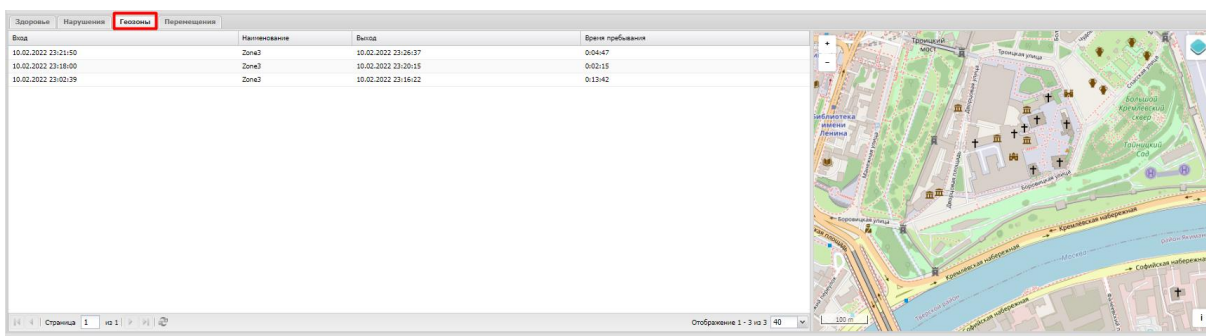


Рисунок 2.74 – Вкладка «Геозоны»

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 2.75):

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

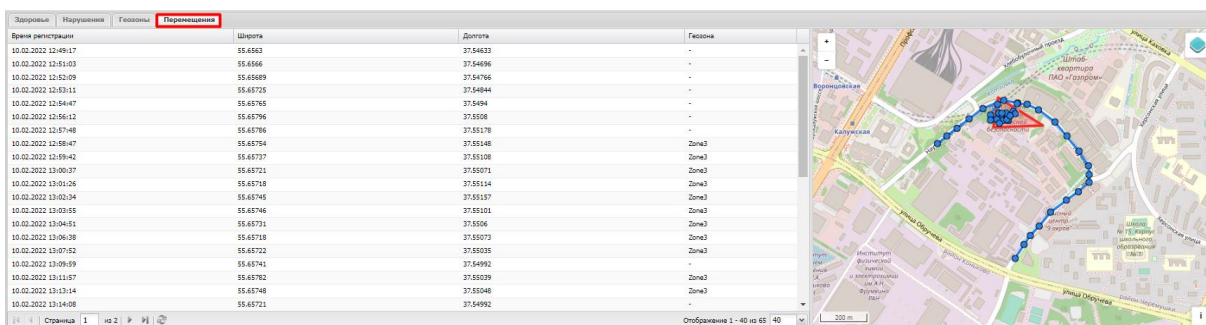


Рисунок 2.75 – Вкладка «Перемещения»

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 APM;**
- **Операционные системы;**

- Приложения;
- SIM-карты;
- Комплекты;
- Геозоны;
- Серверные сертификаты;
- Подключения к серверам;
- Настройки SCEP;
- Клиентские сертификаты.

2.8.1 Организационно-штатная структура

Пункт меню «ОШС» открывает окно в соответствии с рисунком 2.76, в котором отображаются подразделения организации в виде иерархической структуры.

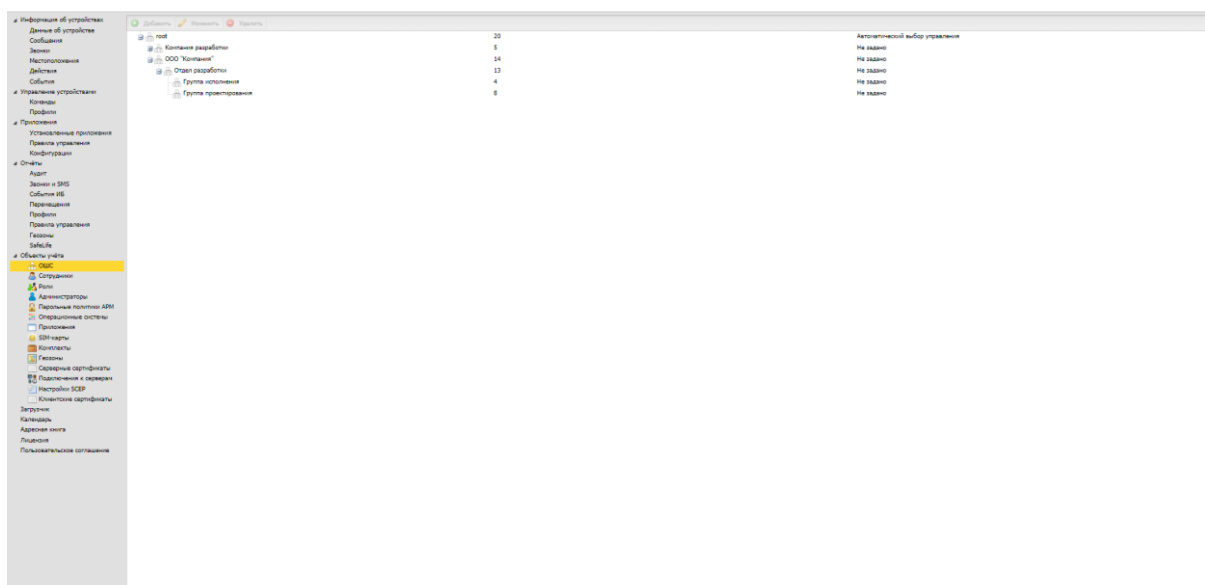


Рисунок 2.76 – Окно «ОШС»

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 2.77.

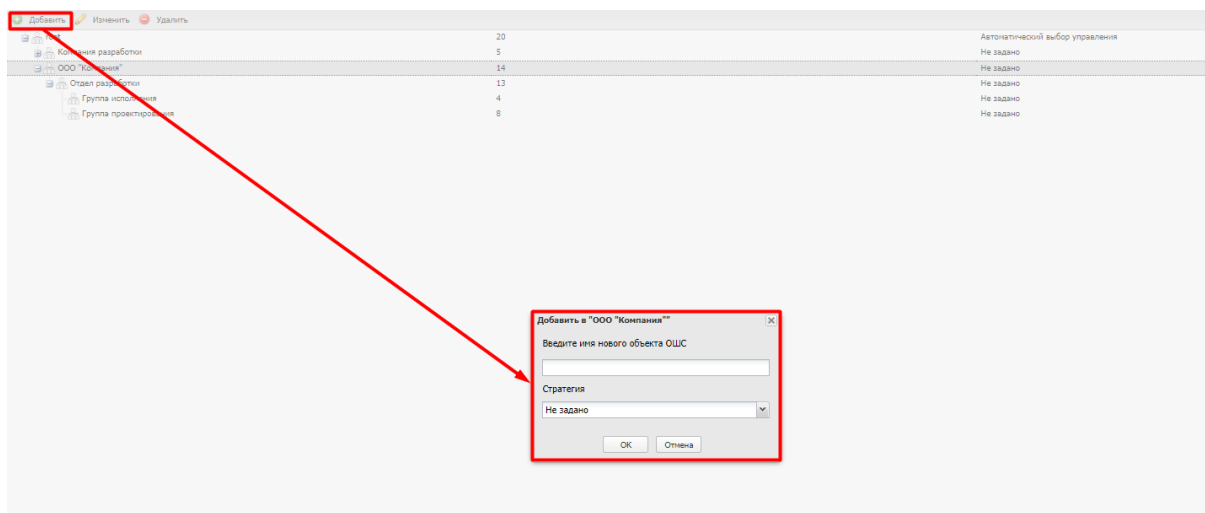


Рисунок 2.77 – Добавление подразделения в ОШС

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 **«ОК»**. 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 2.78.

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

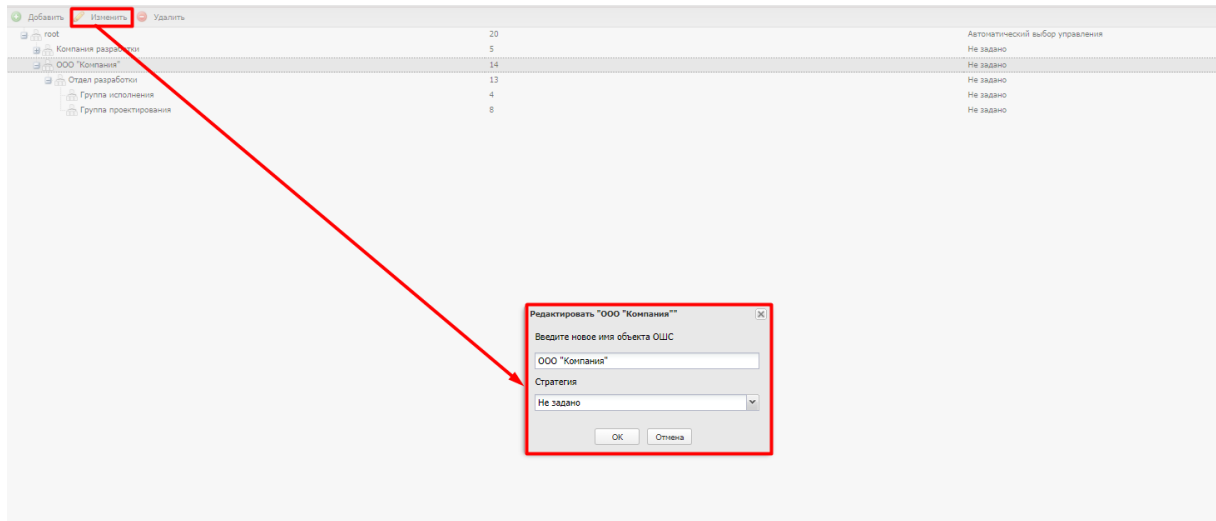


Рисунок 2.78 – Изменение подразделения в ОШС

Для удаления выбранного подразделения из структуры организации нажмите кнопку **«Удалить»**, после чего появится окно в соответствии с рисунком 2.79.

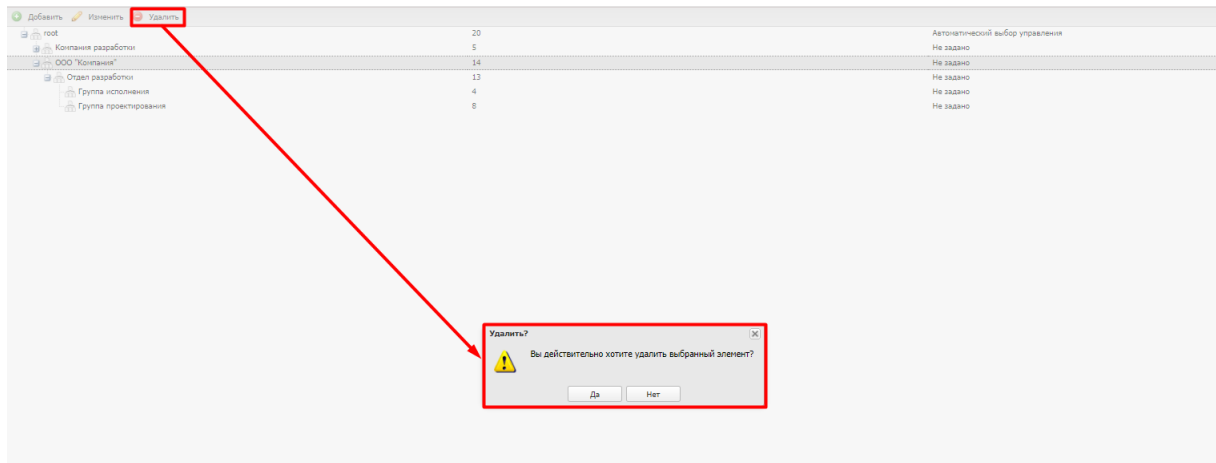


Рисунок 2.79 – Удаление подразделения в ОШС

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

2.8.2 Сотрудники

Справочник сотрудников ведется для учёта абонентов МСК. Перед созданием комплектов МСК в «UEM SafeMobile» необходимо внести данные о сотрудниках организации, используя окно **«Сотрудники»**, открывающееся нажатием соответствующего пункта главного меню.

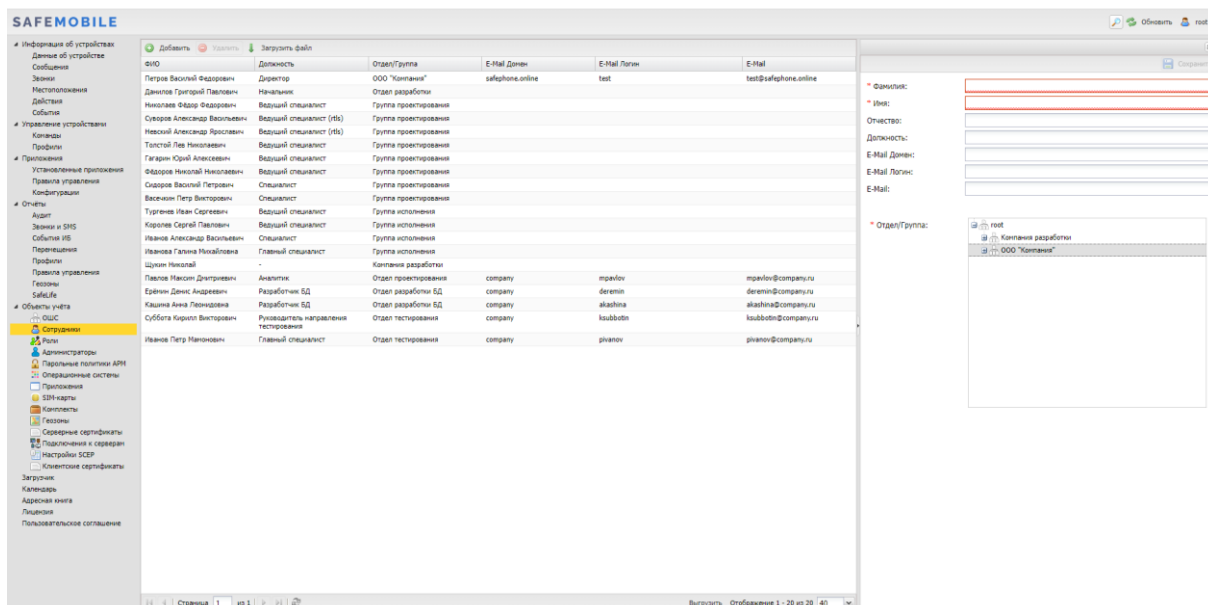


Рисунок 2.80 – Окно «Сотрудник»

Окно содержит список сотрудников организации в виде таблицы со следующими столбцами в соответствии с рисунком 2.80:

- **id** – номер сотрудника с комплектом с в системе (по умолчанию, в таблице не отображается);
- **ФИО** – фамилия, имя и отчество сотрудника;
- **Должность** – должность сотрудника;
- **Отдел/Группа** – подразделение организации, в котором работает сотрудник;
- **E-mail Домен** – доменное имя организации пользователя;
- **E-mail Логин** – имя пользователя (логин) в электронной почте;
- **E-mail** – адрес электронной почты;
- **Структурное подразделение**;
- **Табельный номер**;
- **Номер заявки**.

Для добавления записи используется кнопка «Добавить». Затем в правой части окна следует заполнить форму, содержащую информацию о сотруднике (рисунок 2.81). Для этого необходимо ввести сведения в обязательные поля: «Фамилия», «Имя». Кроме того, в списке ОШС, расположенном ниже поля «Отдел/группа», выбрать подразделение, в котором работает сотрудник.

После заполнения формы нажать кнопку «Сохранить», и запись о новом сотруднике будет добавлена в систему.

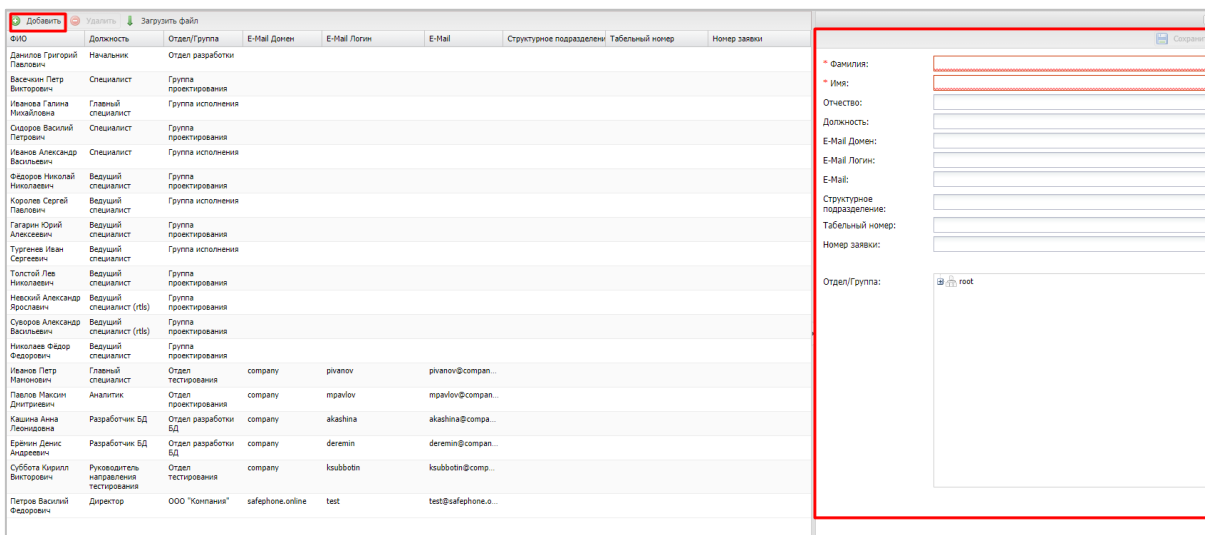


Рисунок 2.81 – Создание записи о сотруднике

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. 2.10, 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.

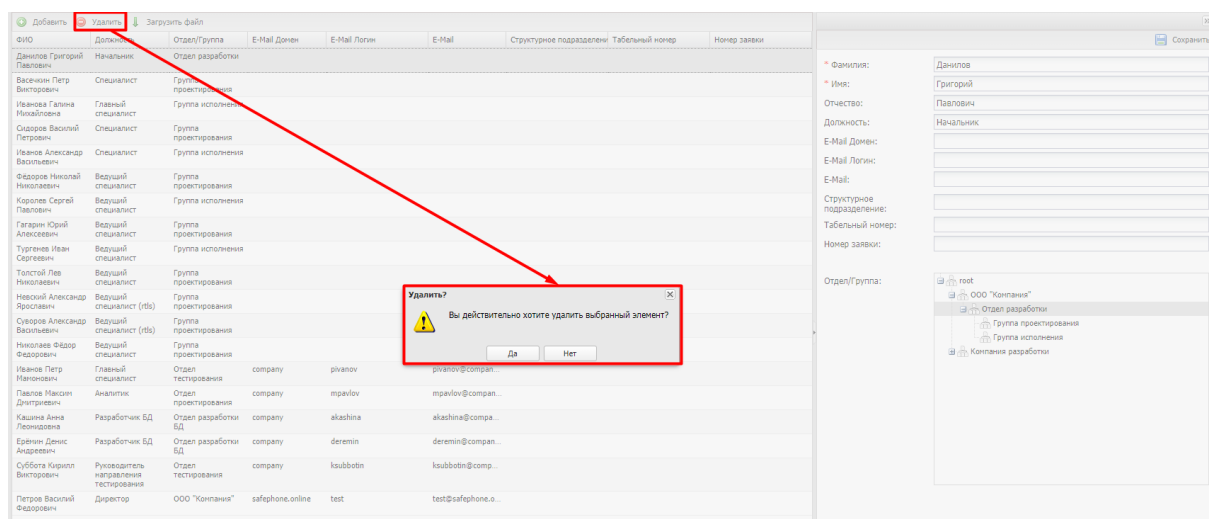


Рисунок 2.82 – Удаление сотрудника

Для удаления объекта учёта необходимо выбрать в таблице (рисунок 2.82) соответствующую ему запись и нажать кнопку «Удалить». После подтверждение выполняемого действия, выбранная запись удаляется из базы при отсутствии связанных объектов учёта.

Кнопка «Загрузить файл» предназначена для загрузки списка сотрудников из файла формата «xlsx» (рисунок 2.83).

1	2	3	4	5	6	7	8	9	10
ObjectGUID	Фамилия	Имя	Отчество	Должность	Домен	Имя пользователя	E-mail	Место работы 1	Место работы 2
4f2e6658-a9a4-46fc-8a14-4a4d3bfd9a72	Иванов	Игорь	Евгеньевич	разработчик	domain	ivanov	ivanov@domain.ru	root	Отдел разработки
4B9DFC01-C3C4-40C0-BD94-D0CAFE783520	Сидоров	Артём	Васильевич	разработчик	domain	sidorov	sidorov@domain.ru	root	Отдел разработки

Рисунок 2.83 – Список сотрудников в файле формата «xlsx»

В данном файле обязательные для заполнения следующие поля:

- Фамилия;
- Имя;
- Должность;
- Место работы.

2.8.3 Роли

Пункт меню «Роли» открывает окно, предназначенное для управления ролями Администраторов «UEM SafeMobile».

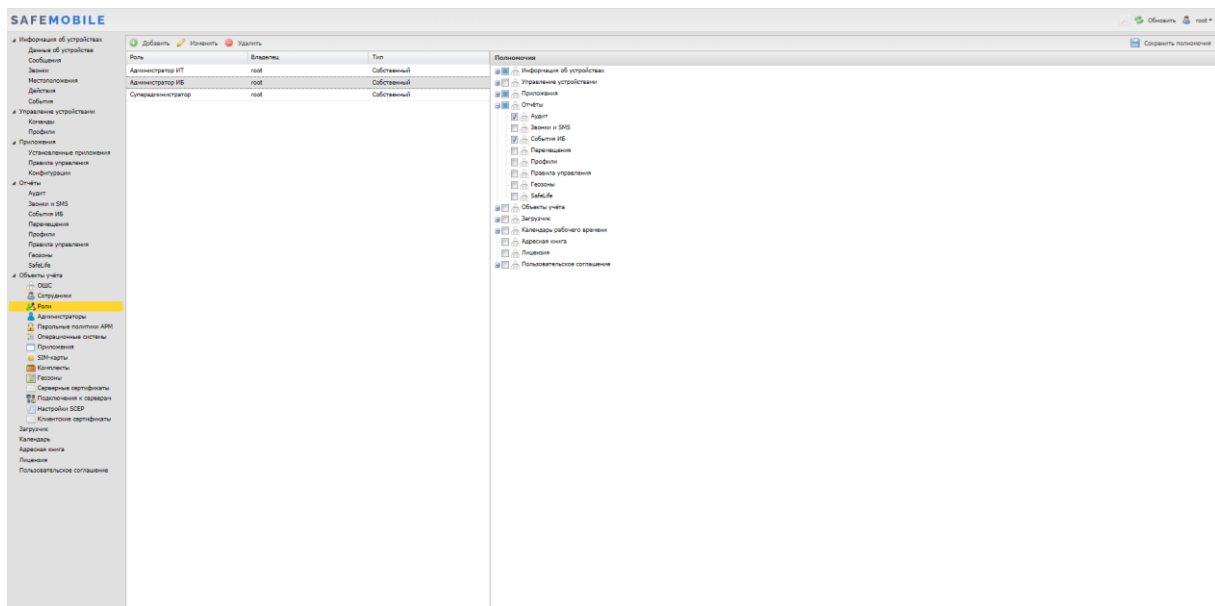


Рисунок 2.84 – Окно «Роли»

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.

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

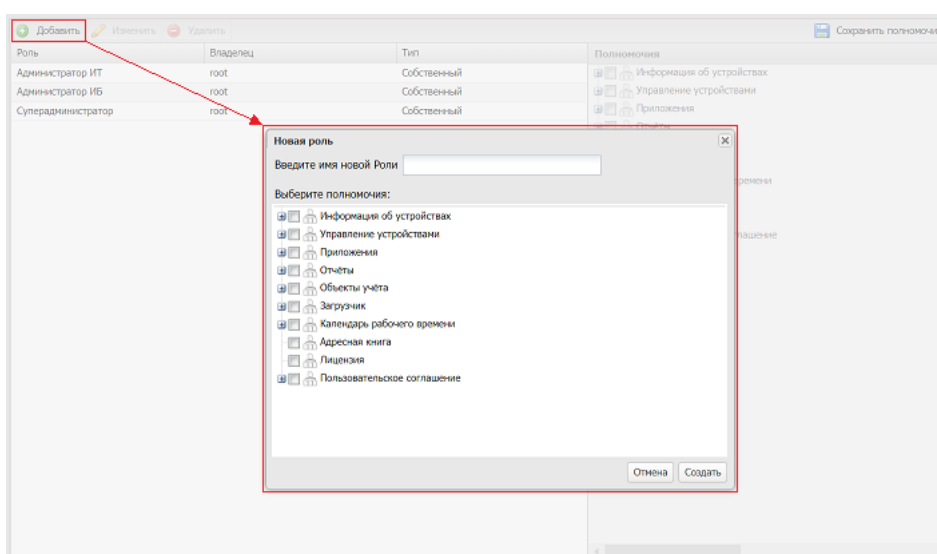


Рисунок 2.85 – Создание роли Администратора

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: «Адресная книга» и «Парольные политики АРМ».
- 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», «Лицензия». Прочие администраторы могут ее только просматривать.

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»**, после чего появится окно в соответствии с рисунком 2.86. После редактирования, для подтверждения изменения, необходимо нажать кнопку **«ОК»**.

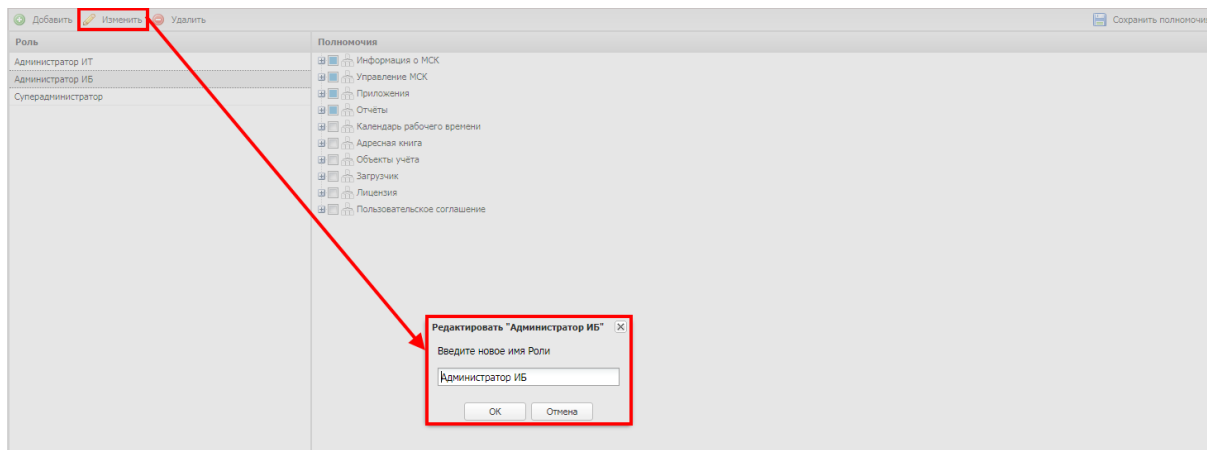


Рисунок 2.86 – Изменение роли Администратора

Для удаления существующей роли требуется нажать кнопку **«Удалить»**. После подтверждения действия (рисунок 2.87) роль будет удалена.

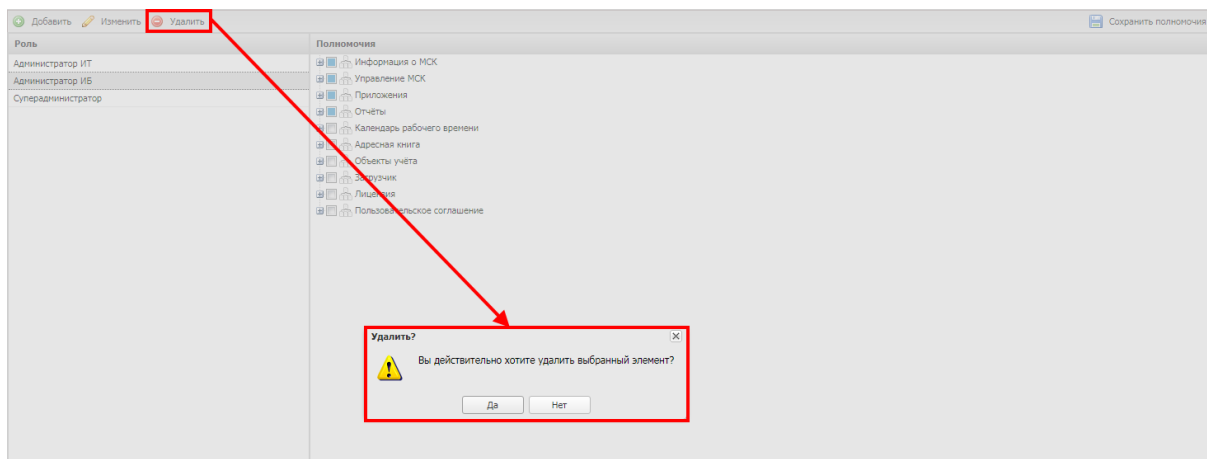


Рисунок 2.87 – Удаление роли Администратора

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

Пункт меню **«Администраторы»** открывает таблицу (рисунок 2.88), предназначенную для управления списком администраторов «UEM SafeMobile» в организации.

Имя пользователя	ФИО	Статус	Корень области управления	Электронная почта	Должность	Место работы	Срок действия учетной записи	Последняя активность
root		Разблокирован	ООО "Юпитера"			Внешней		20.02.2022 23:33:42

Рисунок 2.88 – Окно «Администратор»

В таблице в левой части окна отображаются следующие столбцы:

- **Имя пользователя** – регистрационное имя администратора (логин);
- **ФИО** – фамилия, имя и отчество сотрудника, назначенного администратором;
- **Статус** – состояние учётной записи администратора: заблокирована или не заблокирована. Статус администратора можно изменить с помощью кнопок **«Заблокировать»** и **«Разблокировать»**, расположенных в верхней панели инструментов окна;
- **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).

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 Администратора;

- **Разблокировать** – предназначена для разблокирования выбранной учётной записи Администратора (кнопка доступная только для заблокированных учётных записей).

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 2.89. Область управления – это поддерево ОШС, на которое администратор может влиять, начиная с узла, на который он назначен и заканчивая устройствами. В дальнейшем для администратора интерфейс будет отображаться только из своей области управления в соответствии с ролью и предоставленным правам. Обязательные для заполнения поля отмечены * . На вкладке **«Область управления»** выбрать корень области управления.

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

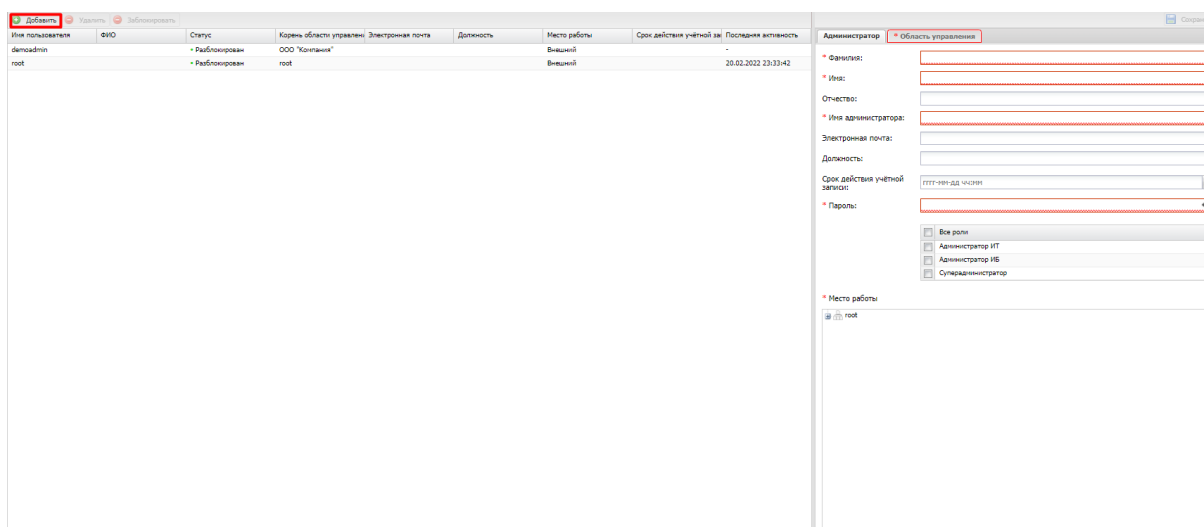


Рисунок 2.89 – Создание Администратора

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»** 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.

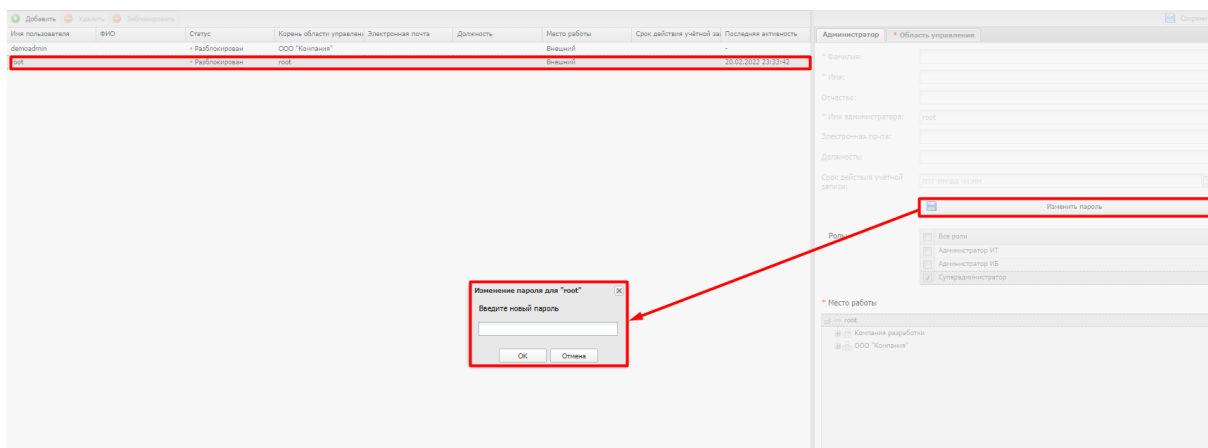


Рисунок 2.90 – Изменение пароля Администратора

2.8.5 Парольные политики APM

Для настройки параметров пароля и учетной записи при входе в «UEM SafeMobile» следует открыть пункт меню **«Парольные политики APM»** (рисунок 2.91).

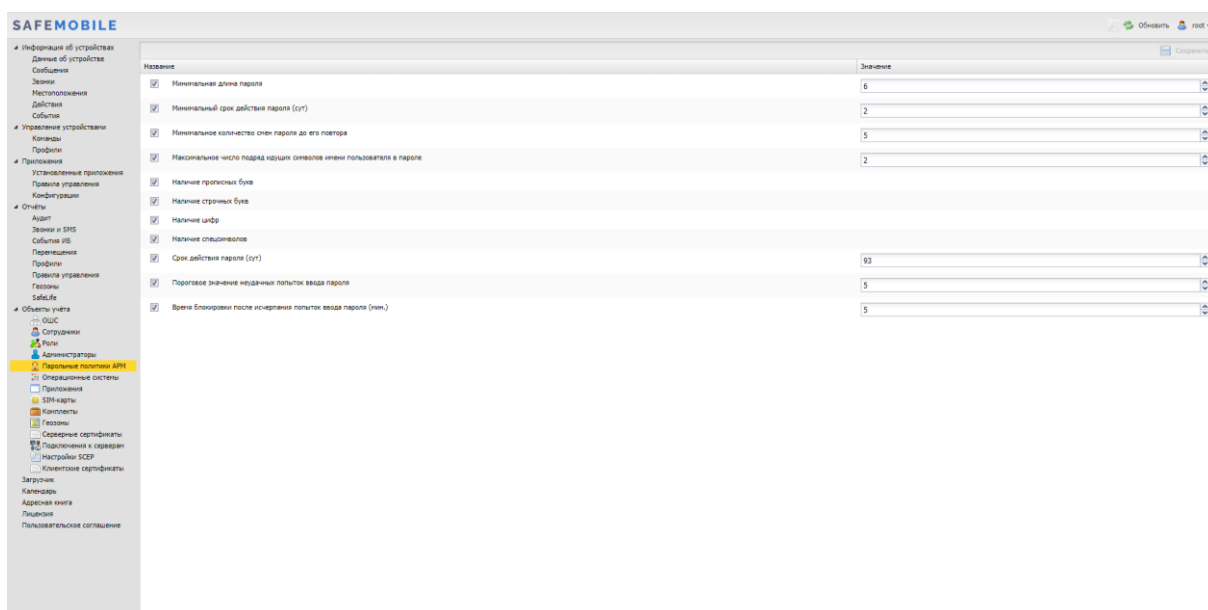


Рисунок 2.91 – Окно «Парольные политики APM»

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 APM 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	
Наличие строчных букв	
Наличие цифр	
Наличие спецсимволов	
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»**.

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 2.92. Поле **«id»** с номером операционной системы в системе, по умолчанию, в таблице не отображается.

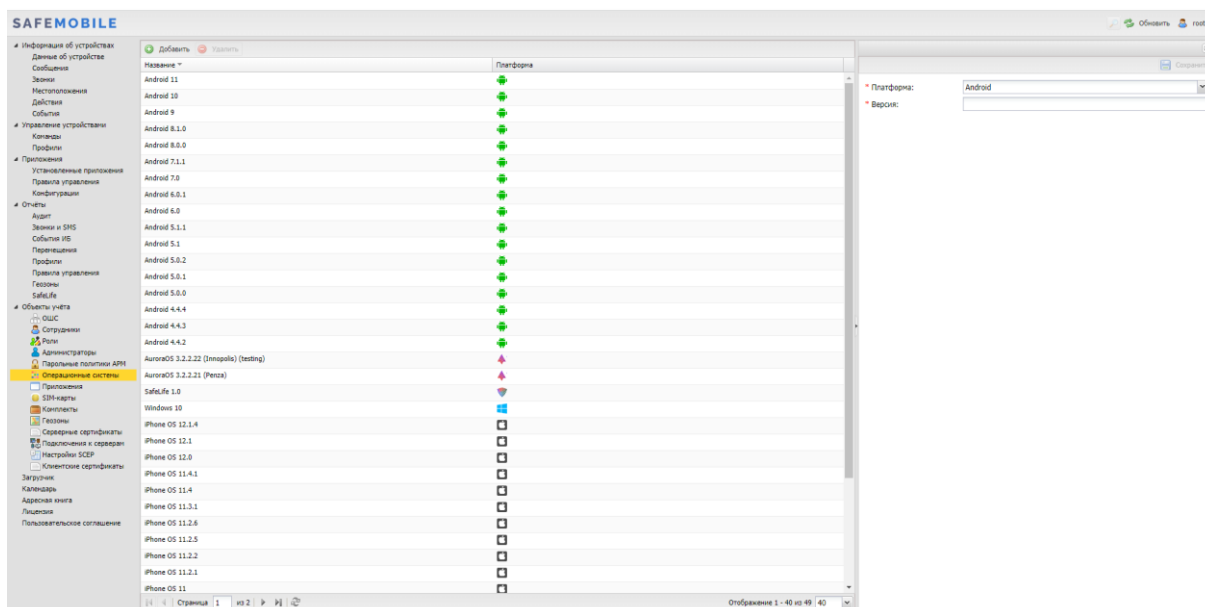


Рисунок 2.92 – Окно «Операционные системы»

Для добавления новой ОС в «UEM SafeMobile» используется кнопка **«Добавить»** в панели инструментов окна (рисунок 2.93), которая позволяет в правой части окна выбрать мобильную платформу в поле **«Платформа»** и указать версию добавляемой ОС в поле **«Версия»**.

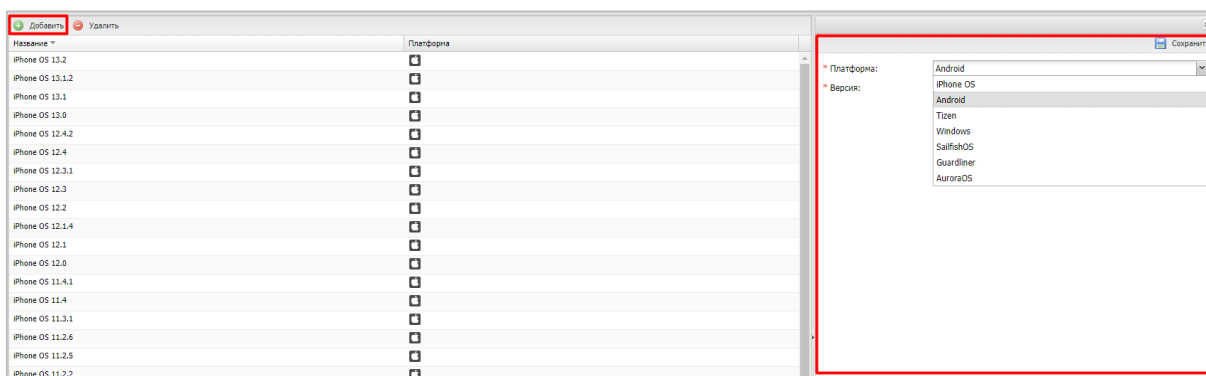


Рисунок 2.93 – Добавление ОС

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

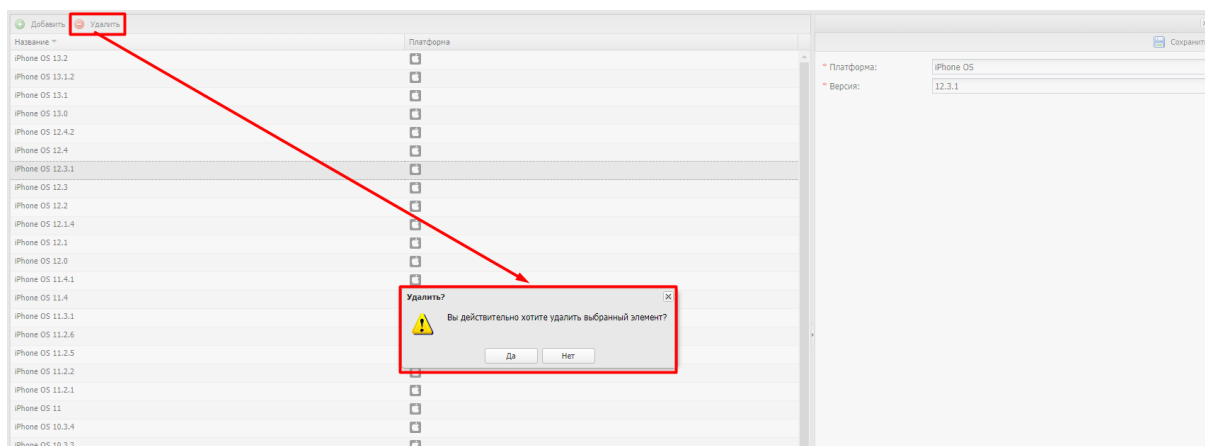


Рисунок 2.94 – Удаление ОС

При нажатии кнопки **«Удалить»** (рисунок 2.94) запрашивается подтверждение выполняемого действия, и выбранная запись об ОС удаляется из базы при отсутствии связанных объектов учёта.

2.8.7 Приложения

Репозиторий приложений ведётся для учёта и распространения приложений. Перечень приложений, зарегистрированных в «UEM SafeMobile», отображается в окне **«Приложения»** раздела **«Объекты учёта»** в соответствии с рисунком 2.95.

Таблица приложений содержит следующие столбцы:

- **id** – номер приложения в системе (по умолчанию, в таблице не отображается);
- **Имя** – наименование приложения;
- **UID** – уникальный идентификатор приложения;
- **Монитор** – мобильный клиент SafeMobile **«Да/Нет»**;
- **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.

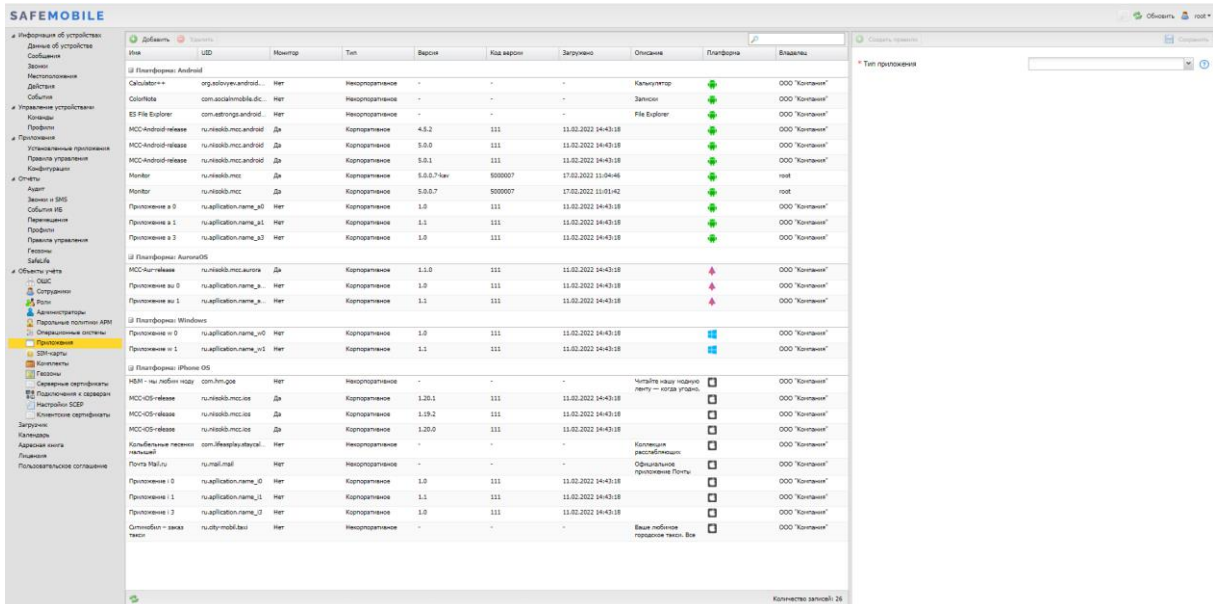


Рисунок 2.95 – Окно «Приложения»

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 2.96. В этом случае записи сгруппируются по версии приложений. Для разгруппировки записей приложений необходимо в раскрывающемся меню снять флажок в строке «Группировать».

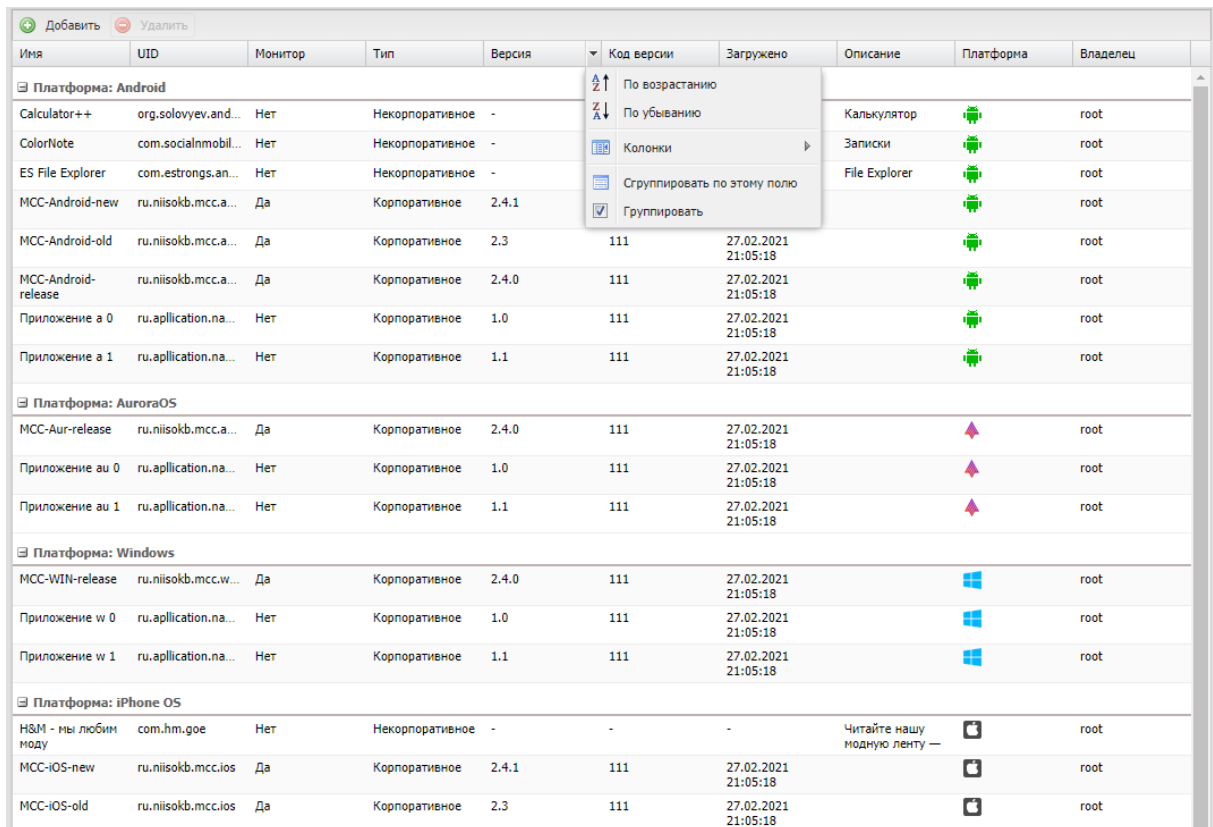


Рисунок 2.96 – Группировка приложений

Для добавления в систему записи о приложении используется кнопка «**Добавить**» в верхней панели инструментов окна. Затем в правой части окна (рисунок 2.97) следует выбрать «**Тип приложения**».

Формы для корпоративных и некорпоративных приложений различны.

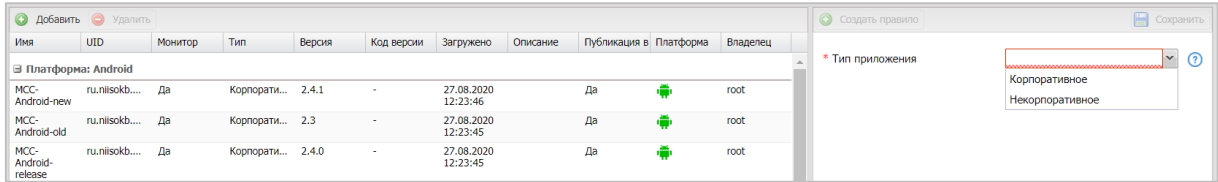


Рисунок 2.97 – Добавление приложения

При добавлении **некорпоративного** приложения необходимо заполнить форму в соответствии с рисунком 2.98, содержащую перечень параметров добавляемого приложения. Поля, обозначенные * – обязательные для заполнения.

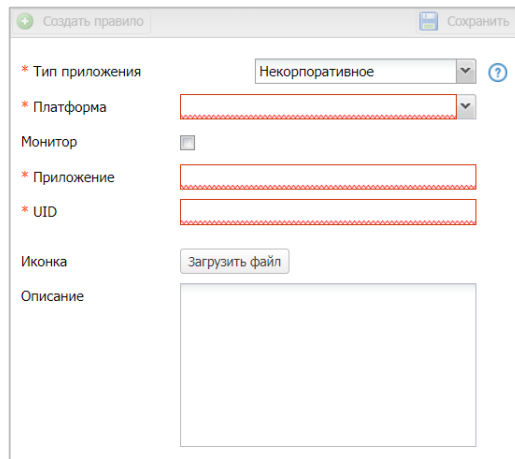


Рисунок 2.98 – Форма некорпоративного приложения

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 2.99.

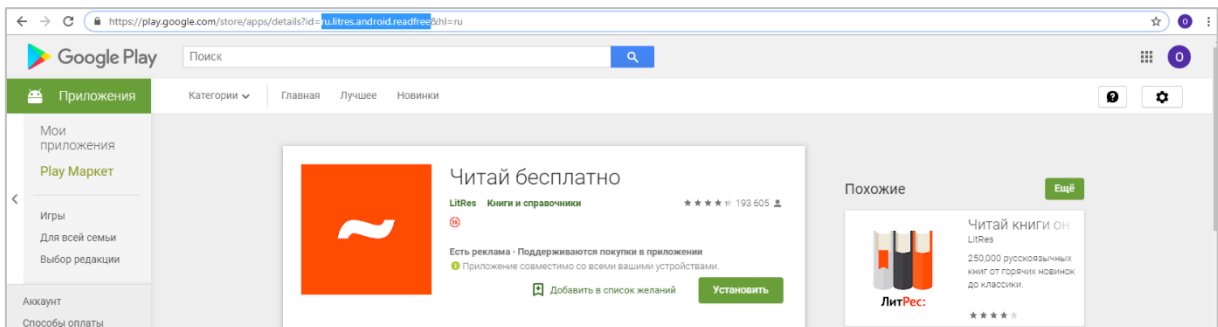


Рисунок 2.99 – Добавление приложения из Google Play

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 2.6.10.

Добавление приложения на MCK платформы Windows

Приложения на MCK платформы Windows загружаются в 2 этапа:

- 1 Необходимо подготовить файл с метаданными. 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 метаданными <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 MCK пользователя, то процедура добавления записи в систему аналогична процедуре в разделе **«Приложения/Управления приложениями»** при нажатии кнопки **«Зарегистрировать»**.

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**.

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

Примечание – 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.

После заполнения всех обязательных полей и загрузки файла, необходимо 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 2.6.10.

Для приложения, выбранного в левой части окна, можно изменить в соответствии с рисунком 2.100. После нажатия кнопки **«Сохранить»** внесенные изменения сохраняются в БД.

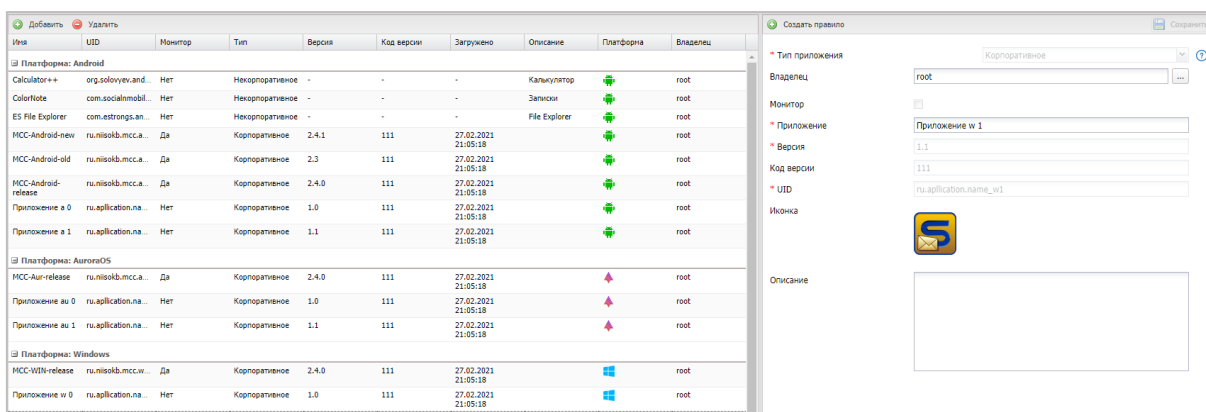


Рисунок 2.100 – Редактирование приложения

Для удаления приложения необходимо выбрать в таблице соответствующую ему запись в соответствии с рисунком 2.101 и нажать кнопку **«Удалить»**.

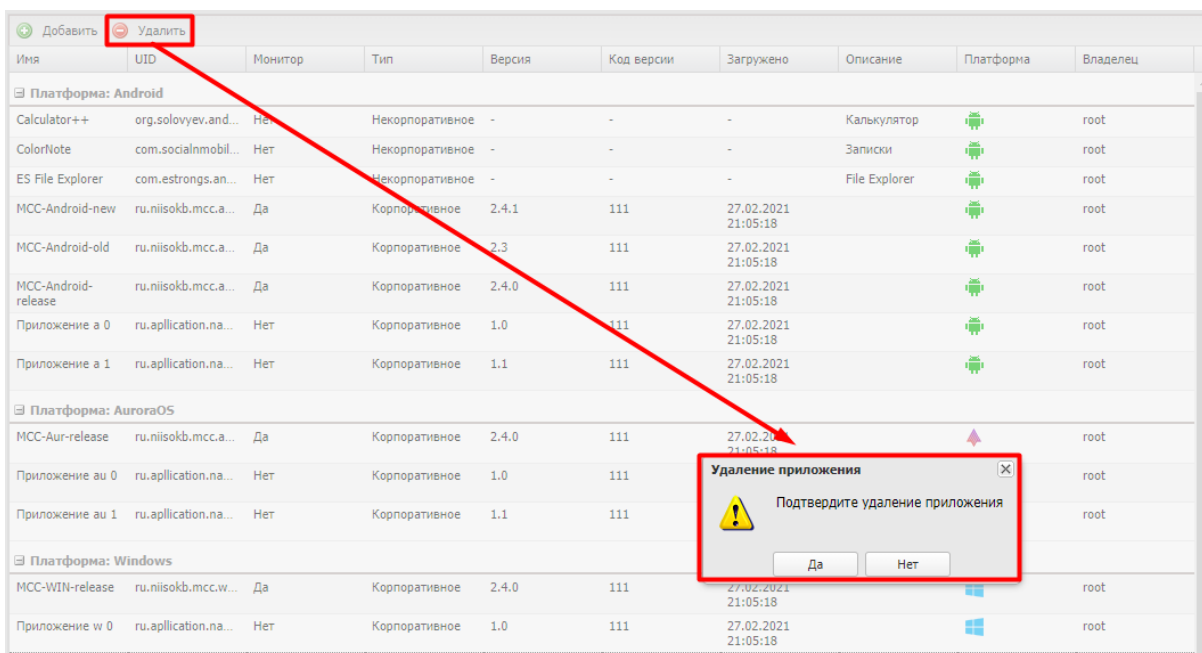


Рисунок 2.101 – Удаление приложения

После подтверждения 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 2.102.

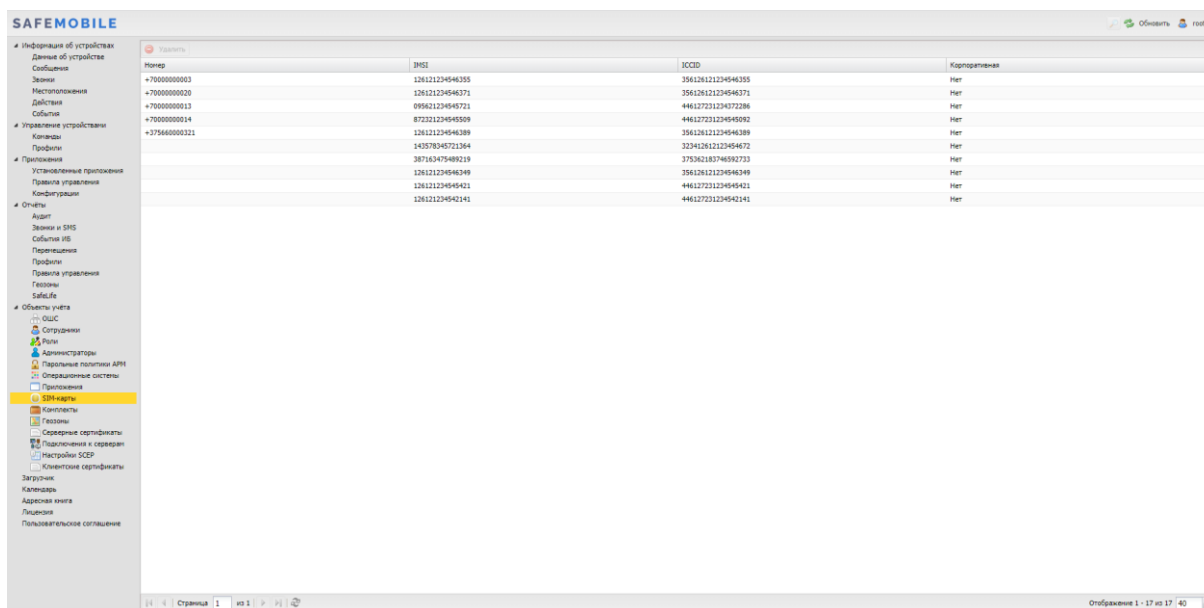


Рисунок 2.102 – Окно SIM-карты

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 2.103). Изменение полей IMSI и ICCID недоступно. После изменения параметров SIM-карты нажмите кнопку **«Сохранить»**, в результате чего изменения будут сохранены в системе.

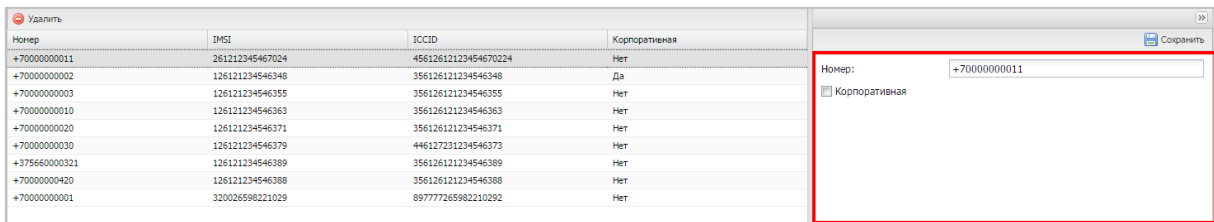


Рисунок 2.103 – Изменение записи о SIM-карте

Для удаления имеющейся SIM-карты выберите ее в таблице и нажмите кнопку **«Удалить»** (рисунок 2.104).

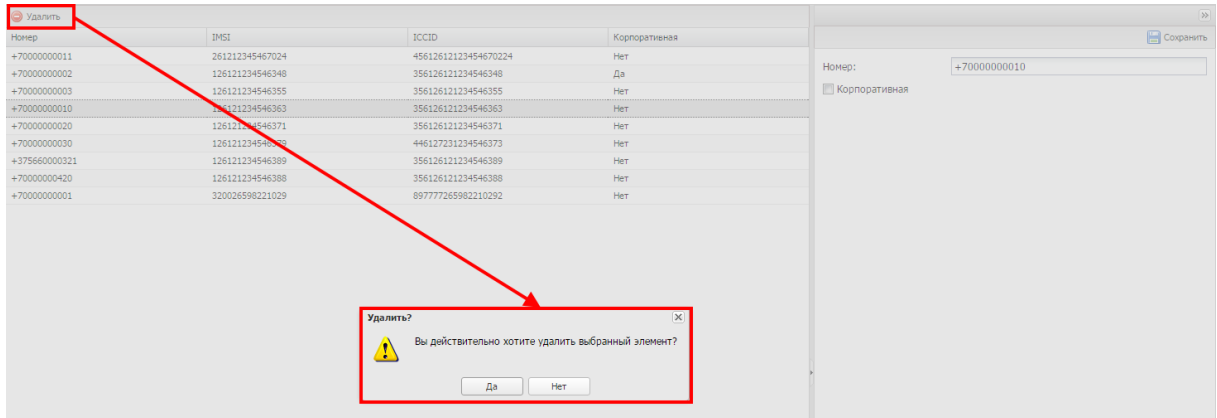


Рисунок 2.104 – Удаление записи о SIM-карте

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

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.

Сотрудник	Отдел/Группа	Телефон	IMEI	Серийный номер	Монитор	Статус
Василин Петр Викторович	Группа проектирования	+7000000003	013327002453779	245377	2.4.0.9998	[Icons]
Гагарин Юрий Алексеевич	Группа проектирования		990003070369550	HD52285	2.4.0.9999	[Icons]
Демченко Григорий Павлович	Отдел разработки		990003070369549	HD52285	1.55.9999	[Icons]
Еренин Денис Андреевич	Отдел разработки БД		841325697021403			[Icons]
Иванова Галина Николаевна	Группа исполнения		013372014452344	445234	2.4.0.9997	[Icons]
Иванов Александр Владимирович	Группа исполнения	+70000000020	012691011243344		2.4.0.9995	[Icons]
Иванов Петр Иванович	Отдел тестирования		654235854123586			[Icons]
Кашкина Анна Леонидовна	Отдел разработки БД		851245365296874			[Icons]
Королев Сергей Павлович	Группа исполнения		35834310024595	R38M607L9L	4.5.0.1-kav	[Icons]
Насосов Александр Александрович	Группа проектирования					[Icons]
Николаев Федор Федорович	Группа проектирования		86732031207496		1.0.0.9996	[Icons]
Павлов Максим Дмитриевич	Отдел проектирования		954236475124586			[Icons]
Петров Василий Федорович	ООО "Компани"	+375640000321	35834310024595	R38M607L9L	4.5.0.1-kav	[Icons]
Сидоров Василий Петрович	Группа проектирования		358902080348473		1.0.2	[Icons]
Суббота Кирилл Викторович	Отдел тестирования		320645014795365			[Icons]
Суров Александр Владимирович	Группа проектирования					[Icons]
Талстой Лев Николаевич	Группа проектирования	+70000000014	26984670027813		2.4.0.9999	[Icons]
Турчинов Иван Сергеевич	Группа исполнения	+70000000013	657364670023209		2.4.0.9999	[Icons]
Федоров Николай Николаевич	Группа проектирования		86732031207496		1.0.2	[Icons]

Рисунок 2.105 – Окно «Комплекты»

В таблице окна в соответствии с рисунком 2.105 имеются следующие столбцы:

- **Сотрудник** (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.**

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 2.106, в которой необходимо выбрать ФИО сотрудника, которому будет назначен добавляемый комплект.

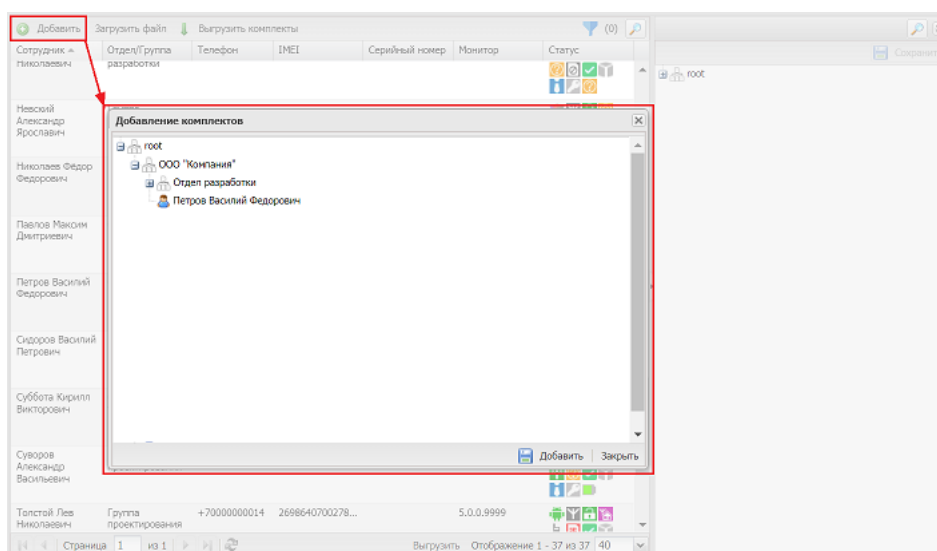



Рисунок 2.106 – Создание комплекта, вкладка «Сотрудник»

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 2.107). В которой необходимо выбрать подразделение, в которое будут импортированы комплекты и файл с комплектами.

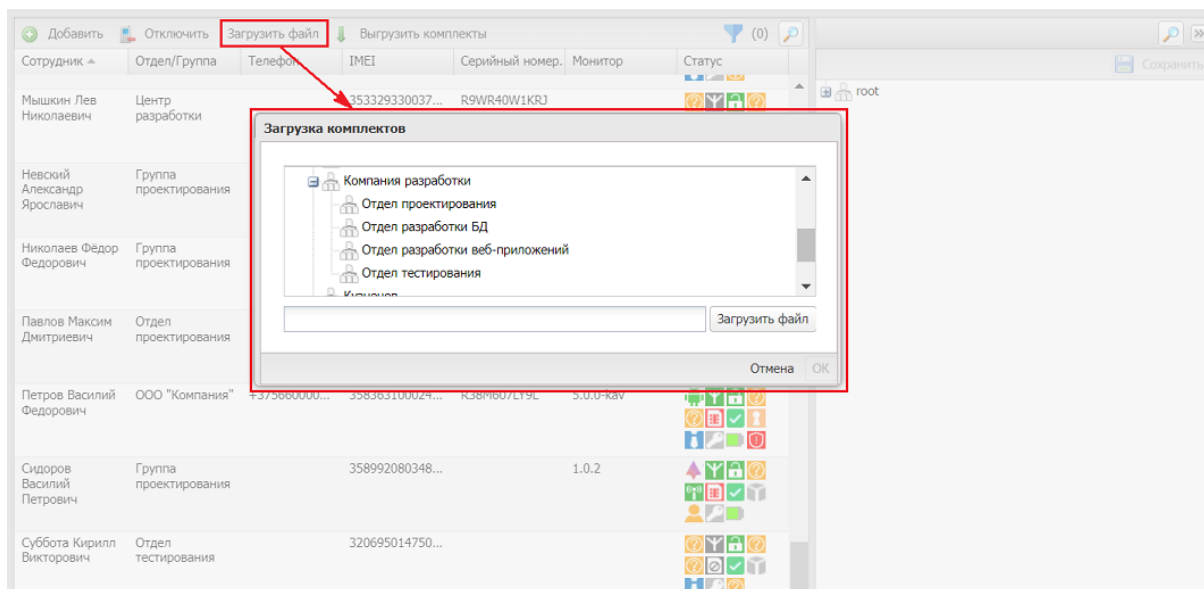


Рисунок 2.107 – Загрузка комплектов

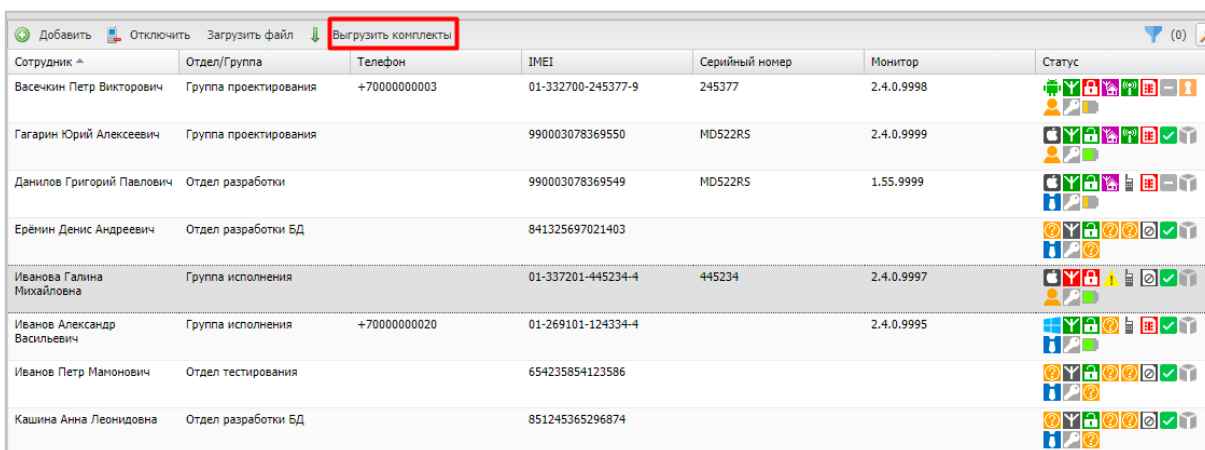
Загружаемый файл может иметь формат CSV или XLSX. Первая строка должна содержать название колонок в следующем составе:

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

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 2.108.



The screenshot shows a software interface with a menu bar at the top containing: 'Добавить', 'Отключить', 'Загрузить файл', and 'Выгрузить комплекты' (highlighted with a red box). Below the menu is a table with the following columns: 'Сотрудник ^', 'Отдел/Группа', 'Телефон', 'IMEI', 'Серийный номер', 'Монитор', and 'Статус'. The table contains eight rows of employee data, each with a set of status icons on the right.

Сотрудник ^	Отдел/Группа	Телефон	IMEI	Серийный номер	Монитор	Статус
Васечкин Петр Викторович	Группа проектирования	+70000000003	01-332700-245377-9	245377	2.4.0.9998	[Icons]
Гагарин Юрий Алексеевич	Группа проектирования		990003078369550	MD522RS	2.4.0.9999	[Icons]
Данилов Григорий Павлович	Отдел разработки		990003078369549	MD522RS	1.55.9999	[Icons]
Ерёмин Денис Андреевич	Отдел разработки БД		841325697021403			[Icons]
Иванова Галина Михайловна	Группа исполнения		01-337201-445234-4	445234	2.4.0.9997	[Icons]
Иванов Александр Васильевич	Группа исполнения	+70000000020	01-269101-124334-4		2.4.0.9995	[Icons]
Иванов Петр Мамонович	Отдел тестирования		654235854123586			[Icons]
Кашина Анна Леонидовна	Отдел разработки БД		851245365296874			[Icons]

Рисунок 2.108 – 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 2.109. Затем требуется подтвердить действие, нажав на кнопку **«Применить»**.

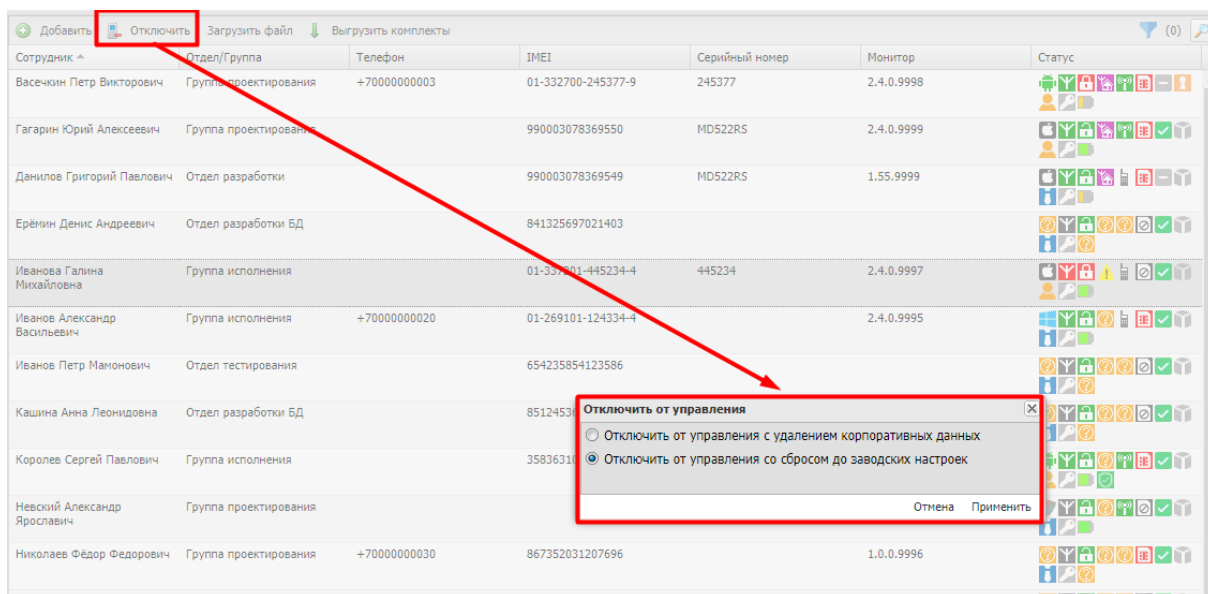


Рисунок 2.109 – Отключение комплекта от управления

После отключения от управления комплект можно будет удалить из системы. Для этого необходимо выбрать в таблице соответствующую ему запись, нажать кнопку «**Удалить**» (рисунок 2.110), после подтверждения выполняемого действия выбранная запись удалится из БД.

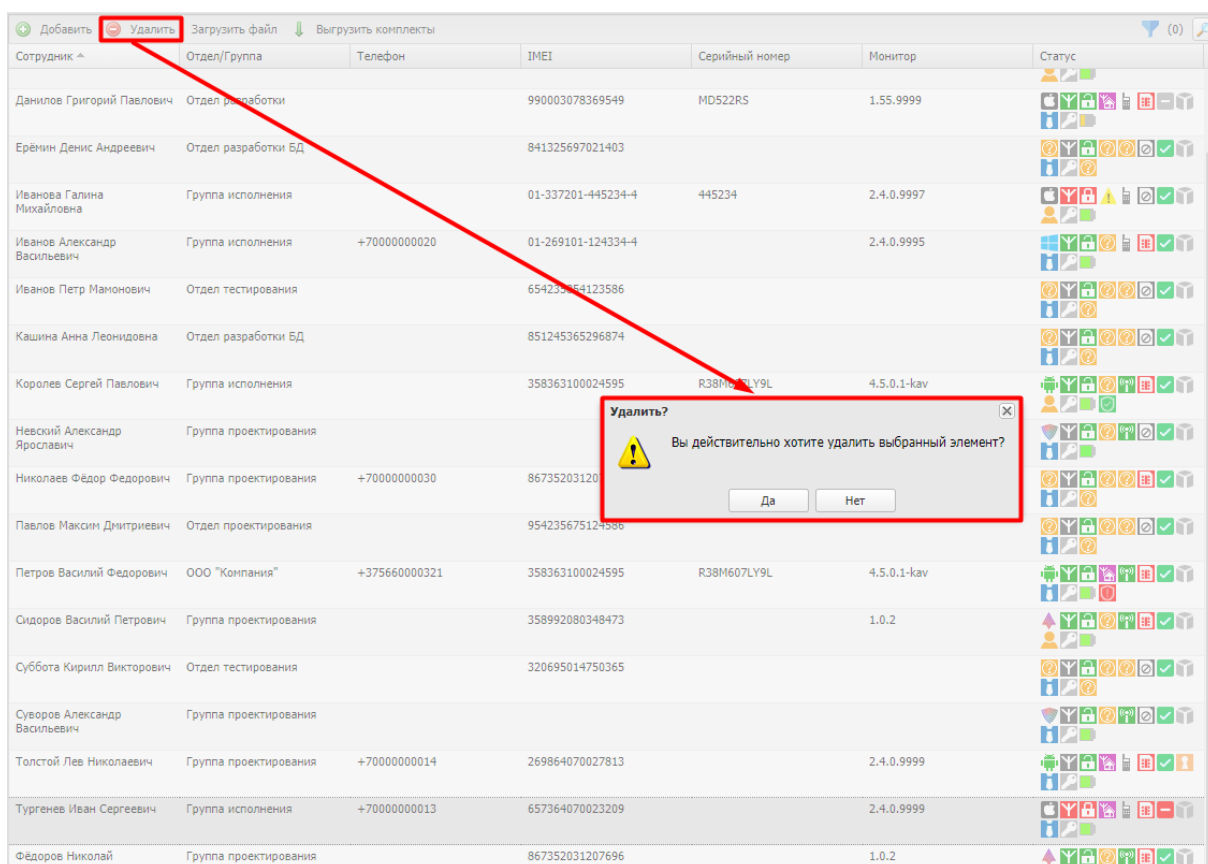


Рисунок 2.110 – Удаление комплекта

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

1Для 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.

2Если 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 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 2.111.

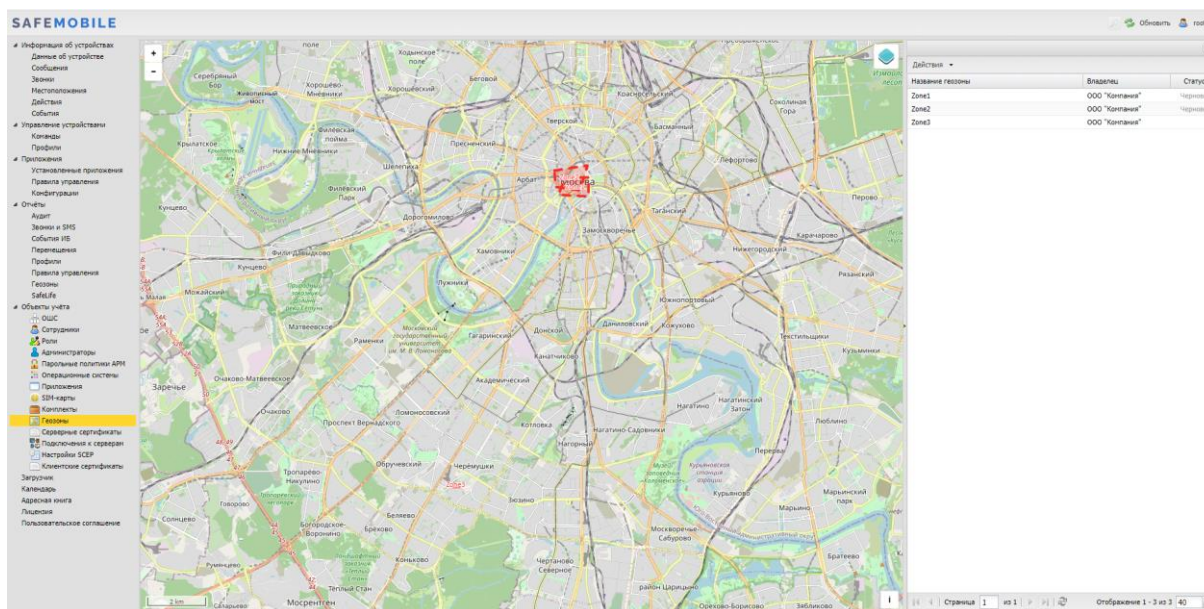



Рисунок 2.111 – Окно «Геозоны»

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 2.112).

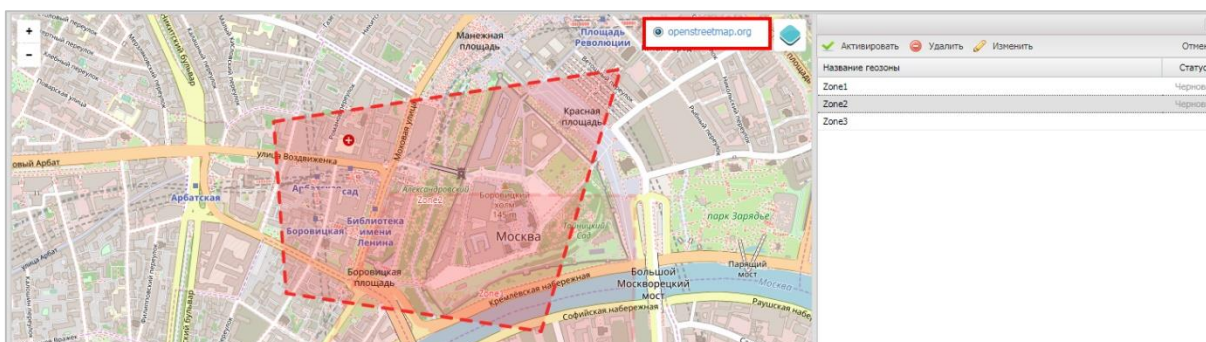


Рисунок 2.112 – Настройка режима отображения информации о геозонах на карте

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 2.113 ввести имя новой геозоны, которое должно отличаться от уже созданных, и нажать **«ОК»**. Созданная геозона отобразится в реестре со статусом «Черновик».

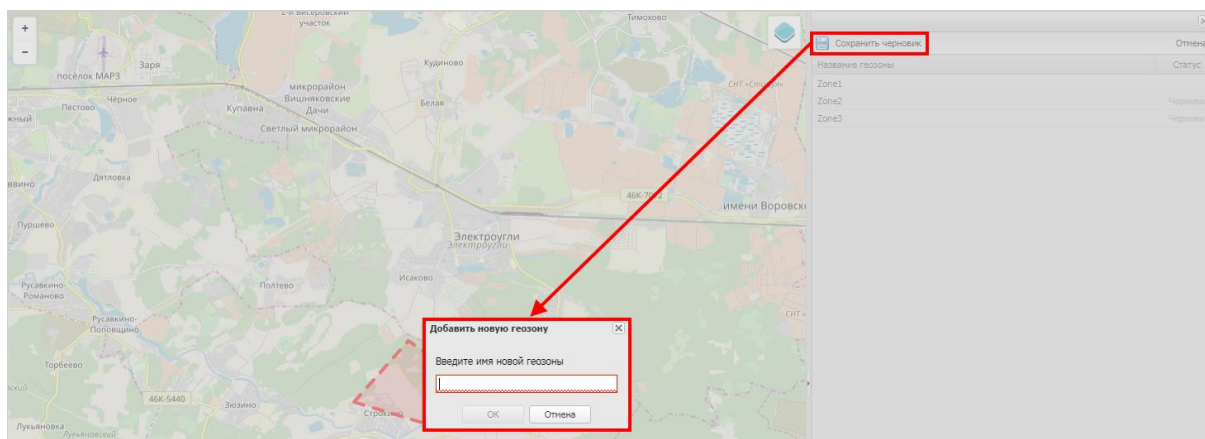


Рисунок 2.113 – Добавление геозоны

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 «Действия», выбрать **«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*.

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»**.

2.8.11 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 2.114.

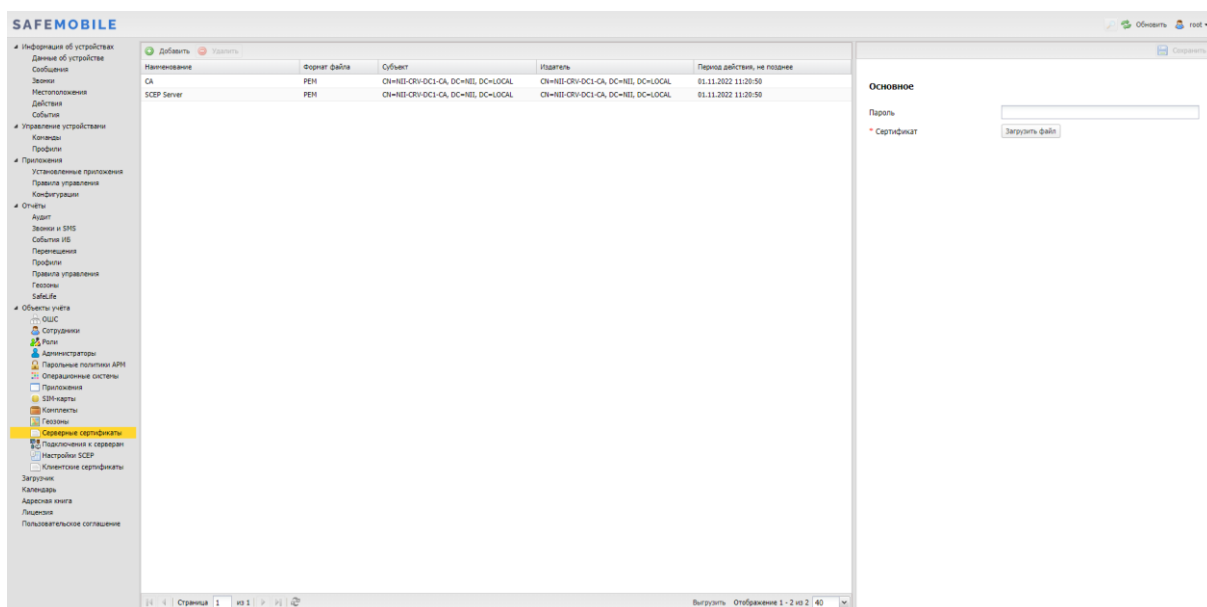


Рисунок 2.114 – Окно «Серверные сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- **Наименование** – наименование сертификата (по умолчанию, отображается в таблице);
- **Отпечаток сертификата** – информация о файле сертификата в формате base64 (по умолчанию, отображается в таблице);
- **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;
- **Приватный ключ** – (Да/Нет).
- **Владелец** – подразделение, владеющее сертификатом.

Для **добавления** нового серверного сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна (рисунок 2.114). 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 2.115.

Основное

* Сертификат

* Наименование

Отпечаток сертификата 4c 0e fa c1 ac 38 be 66 54 1b b9 6a 92 44

Формат файла PEM

X.509

Субъект CN=NII-SRV-DC1-CA, DC=NII, DC=LOCAL

Версия 3

Серийный номер 4c ca 6b f7 cb ff 1b 84 48 af 84 5c 2e 27 8

Период действия, не ранее

Период действия, не позднее

Издатель CN=NII-SRV-DC1-CA, DC=NII, DC=LOCAL

Пароль

Приватный ключ

Рисунок 2.115 – 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 2.116) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждения выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

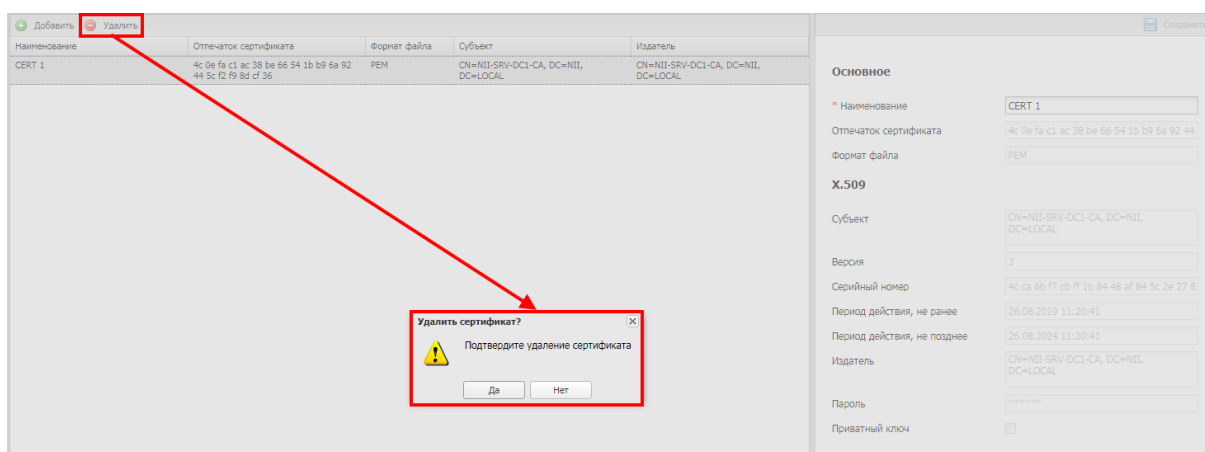


Рисунок 2.116 – Удаление серверного сертификата

2.8.12 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 **SCEP** SafeMobile в соответствии с 2.8.13 необходима при использовании доменной авторизации по клиентским сертификатам. Данная настройка применима только для MCK на платформах Android и iOS.

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

В разделе отображается таблица с перечнем серверов и подключенных к ним серверных сертификатов в соответствии с рисунком 2.117.

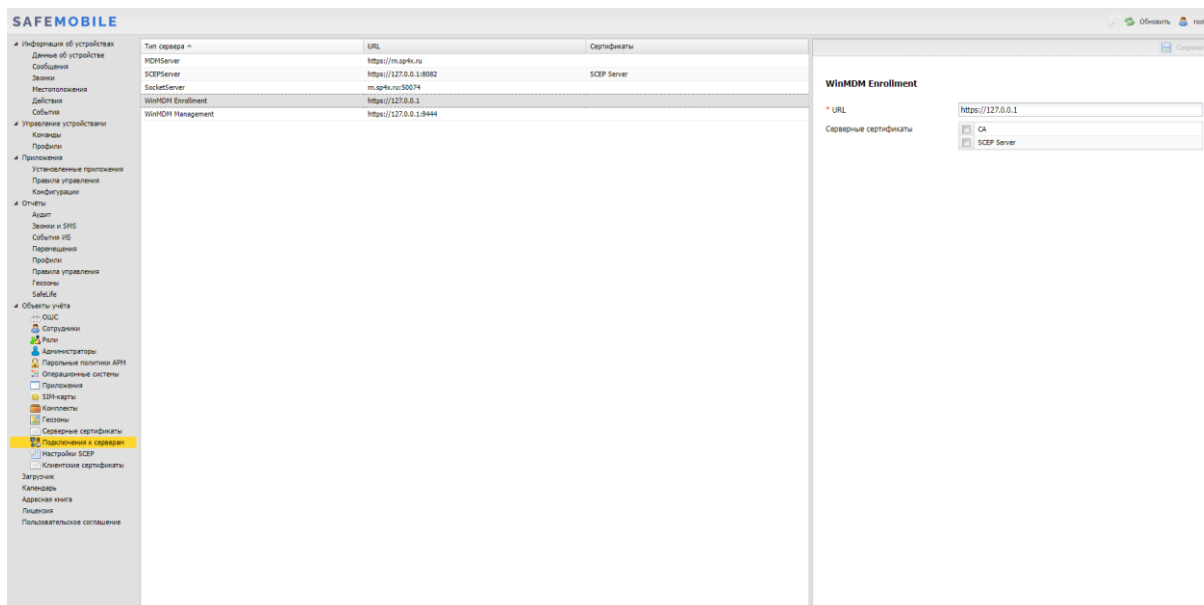


Рисунок 2.117 – Окно «Подключение к серверам»

Таблица подключения к серверам, по умолчанию, содержит столбцы:

- **Тип сервера** – наименование сервера системы);
- **URL** – электронный адрес;
- **Сертификат** – наименование серверного сертификата.

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
				WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.2	enterpriseenrollment.example.com:443
			example.com [x.x.x.2]	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
				WinMDM Enrollment		example1.com:443
			example1.com [x.x.x.2]	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 следует в списке серверов выбрать сервер (рисунок 2.117), а затем в форме правой части окна: ввести URL и установить флажок у тех серверных сертификатов, по которым МСК сможет аутентифицировать данный сервер (рисунок 2.118). В любой момент времени сервер использует только один сертификат. До того момента как истечет время действия текущего сертификата, необходимо выпустить 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.

Рисунок 2.118 – Форма «Подключения к серверу»

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

2.8.13 Настройки SCEP

Пункт меню **«Настройки SCEP»** предназначен для учёта и распространения клиентских сертификатов с настраиваемыми параметрами посредством SCEP в соответствии с рисунком 2.114.

Рисунок 2.119 – 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);

Для *добавления* нового клиентского сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна (рисунок 2.114). Затем заполнить форму в правой части окна 2.115.

The screenshot shows a configuration window titled "Настройки SCEP". It includes the following fields and sections:

- Настройки SCEP:**
 - * Наименование: Text input field.
 - Имя субъекта: Text input field.
 - * Шаблон сертификата: Text input field.
 - * Число попыток поллинга: Spin button.
 - * Время между попытками поллинга (мин): Spin button.
 - Алгоритм шифрования: Dropdown menu (selected: RSA).
 - Challenge: Text input field.
 - Назначение ключа: Dropdown menu (selected: Шифрование).
 - Размер ключа: Dropdown menu (selected: 1024).
- Подключение к серверу SCEP:**
 - * Подключения к серверам: Dropdown menu (selected: Выберите соединение с сервером...).
- Подключение к серверу Удостоверяющего Центра AD:**
 - * URL корпоративного CA: Text input field (placeholder: домен\название удостоверяющего центра).
 - * Период запросов к CA (мин): Spin button.

Рисунок 2.120 – Форма сертификата с настройками SCEP

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

Для *удаления* серверного сертификата необходимо выбрать в таблице (рисунок 2.116) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждения выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

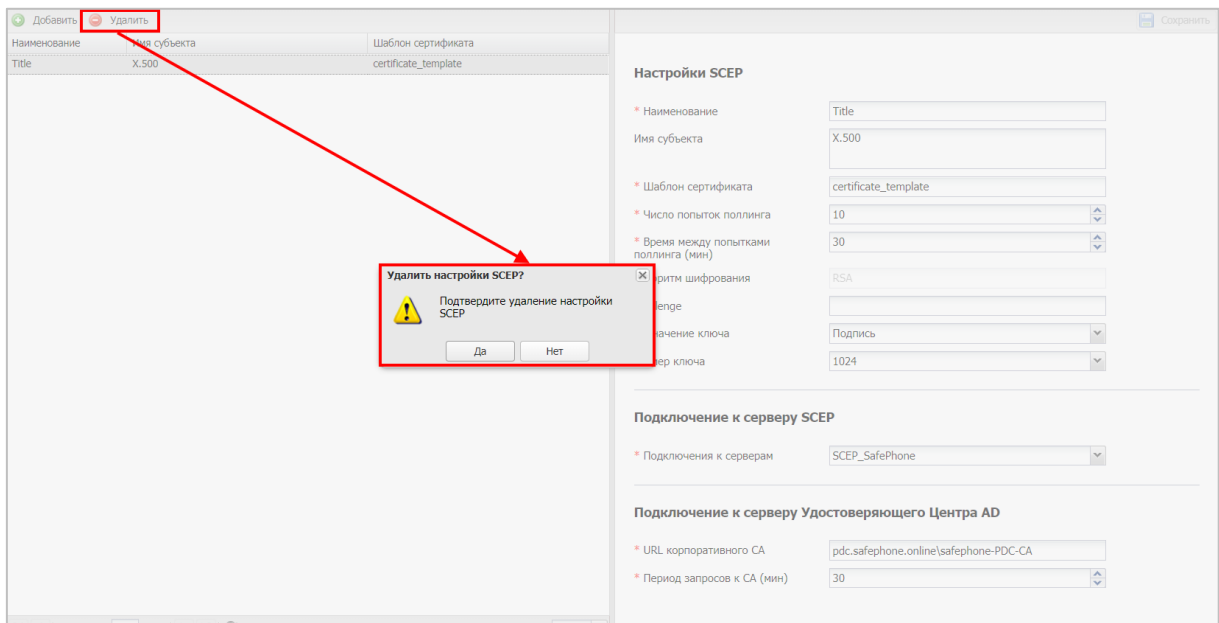


Рисунок 2.121 – Удаление сертификата с настройками SCEP

2.8.14 Клиентские сертификаты

Пункт меню «Клиентские сертификаты» предназначен для учёта и распространения клиентских сертификатов, которые используются для аутентификации пользователя при подключении к корпоративной сети WiFi. В верхней части окна раздела в соответствии с рисунком 2.122 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.

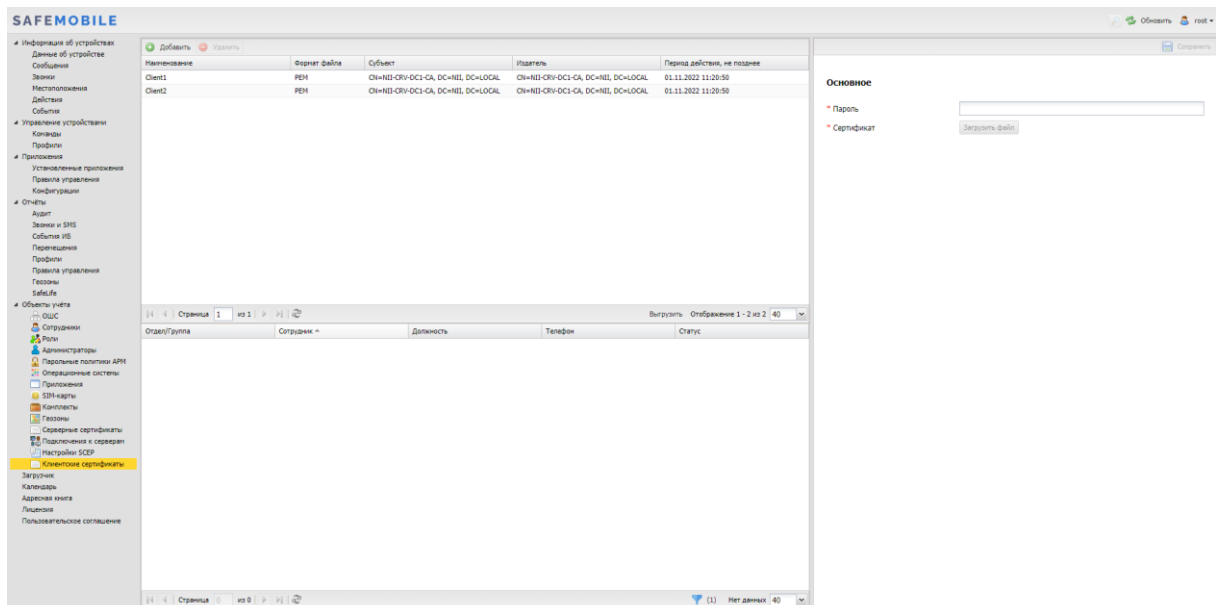


Рисунок 2.122 – Окно «Клиентские сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- **Наименование** – наименование сертификата (по умолчанию, отображается в таблице);
- **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 2.122). 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 2.123.

Основное	
* Сертификат	Загрузить файл
* Наименование	
Отпечаток сертификата	c2 09 62 6e 74 95 3d b3 e0 81 91 ef 6e 0c
Формат файла	PKCS12
x.509	
Субъект	CN=user01, CN=Users, DC=NIL, DC=LOCAL
Версия	3
Серийный номер	51 00 00 00 05 4f 19 5e be 01 e8 85 ab 0c

Рисунок 2.123 – 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 (рисунок 2.124) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

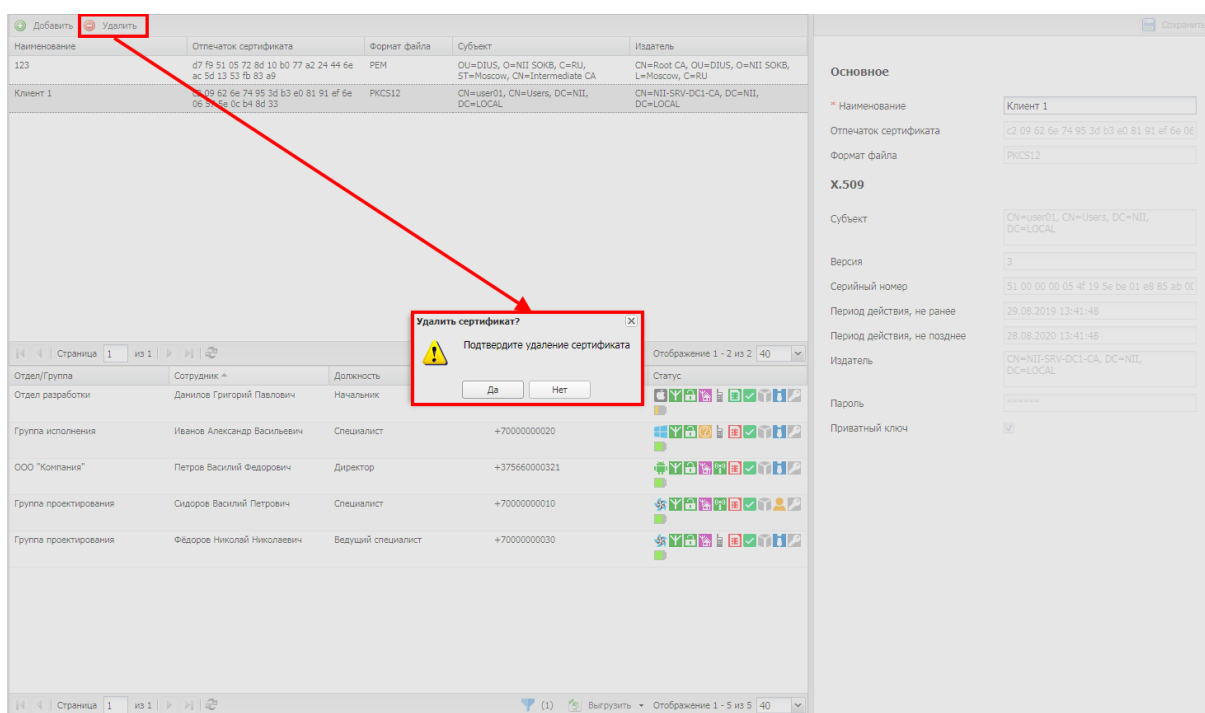


Рисунок 2.124 – Удаление клиентского сертификата

2.9 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»**.

Дата создания	Код	Статус	Действителен до	ФИО	Принадлежность	Стратегия
11.02.2022	251349811	-	24.02.2022	Иванов Иван Иванович	Корпоративная	Автоматический выбор управления
11.02.2022	920404291	-	11.02.2022	Васильев Петр Викторович	Личная	Персональный рабочий профиль (Samsung 5.1+)
11.02.2022	413662392	-	11.02.2022	-	Личная	Персональный рабочий профиль (Samsung 5.1+)

Рисунок 2.125 – Окно «Загрузчик»

В окне отображается таблица кодов приглашений в соответствии с рисунком 2.125, которая состоит из следующих столбцов:

- **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 4.4 - 9)** – требует наличия у монитора привилегий KNOX и администратора устройства (Device Admin). Применима для МСК Samsung с версией Android начиная с 4.4 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.

- **Персональный рабочий профиль (Android 7.0+)** – требует наличия у монитора привилегий владельца профиля (Profile Owner). Применяется 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.

В таблице имеется возможность отображения кодов приглашений в зависимости от статуса. Для этого следует нажать кнопку «Отображать со статусом», после чего раскрывается меню со следующими пунктами (рисунок 2.126):

- **Новый код** – созданный Администратором код, который пока не был использован сотрудником-абонентом МСК;
- **Ожидаются данные** – система ожидает ввода данных сотрудником-абонентом на МСК;
- **Ожидается подтверждение ввода** – на МСК введены данные сотрудником-абонентом или Администратором, и система ожидает их проверки и подтверждения Администратором;
- **Подготовка к установке** – выполняется подготовка к установке мобильного клиента SafeMobile на МСК;
- **Произошла ошибка, необходимо подтверждение** – произошла ошибка при установке мобильного клиента SafeMobile на МСК. Администратор при этом должен разрешить повторную установку монитора, выбрав действие «**Одобрить повторную установку**»;
- **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 раскрываемом меню «**Отображать со статусом**» сняты).

Дата создания	Код	Статус	Действителен до	ФИО	Принадлежность	Стратегия
21.06.2022	584615259	Деактивирован	28.06.2022	Федоров Николай Николаевич	Корпоративная	Автоматический выбор управления
21.06.2022	473857031	Деактивирован	28.06.2022	Васечкин Петр Викторович	Корпоративная	Автоматический выбор управления
21.06.2022	600263389	Деактивирован	28.06.2022	Федоров Николай Николаевич	Корпоративная	Только устройство (Android)
21.06.2022	380288885	Деактивирован	28.06.2022	Васечкин Петр Викторович	Корпоративная	Автоматический выбор управления
20.06.2022	287547635	Деактивирован	27.06.2022	Федоров Николай Николаевич	Корпоративная	Автоматический выбор управления
17.06.2022	575648377	Деактивирован	17.06.2022	Васечкин Петр Викторович	Личная	Личный рабочий профиль (Android 7.0+)
17.06.2022	834476550	Деактивирован	17.06.2022	-	Личная	Личный рабочий профиль (Android 7.0+)

Новый код
 Ожидаются данные
 Ожидается подтверждение ввода
 Подготовка к установке
 Произошла ошибка, необходимо подтверждение
 Деактивирован
 Клиент успешно установлен

Страница 2 из 2 | Выгрузить | Отображать со статусом | Отображение 21 - 27 из 27 | 40

Рисунок 2.126 – Фильтрация по статусам кода приглашения

В верхней части окна расположена кнопка «Создать коды», при нажатии которой открывается окно для создания кодов приглашений (рисунок 2.127).

Дата создания	Код	Статус	Действителен до	ФИО	Принадлежность	Стратегия
17.02.2022	251343811	-	24.02.2022	test@ovpn1.test	Корпоративная	Автоматический выбор управления
11.02.2022	932414251	-	11.02.2022	Васечкин Петр Викторович	Личная	Персональный рабочий профиль (Samsung 5.1+)
11.02.2022	412862992	-	11.02.2022	-	Личная	Персональный рабочий профиль (Samsung 5.1+)

Создание кодов с привязкой к подразделению/сотруднику

Функция: Имя: Отчество: Должность:

Привязать к подразделению Все сотрудники

Срок действия до: 27.02.2022 | Принадлежность: Корпоративная | Стратегия:

Создать коды

Рисунок 2.127 – Окно «Создание кодов»

Для создания кода приглашения для зарегистрированного сотрудника необходимо выбрать подразделение и сотрудника, для которого создается приглашение, указать в календаре дату, после которой действие кода будет прекращено (в поле «Срок действия, до»), выбрать принадлежность и стратегию. Стратегия будет применяться только для МСК Android. Затем следует нажать кнопку «Создать коды», расположенную в нижней части окна «Создание кодов» в соответствии с рисунком 2.128. После подтверждения действия будет создан новый код приглашения, и запись о нем добавится в таблицу кодов со статусом «Новый код».

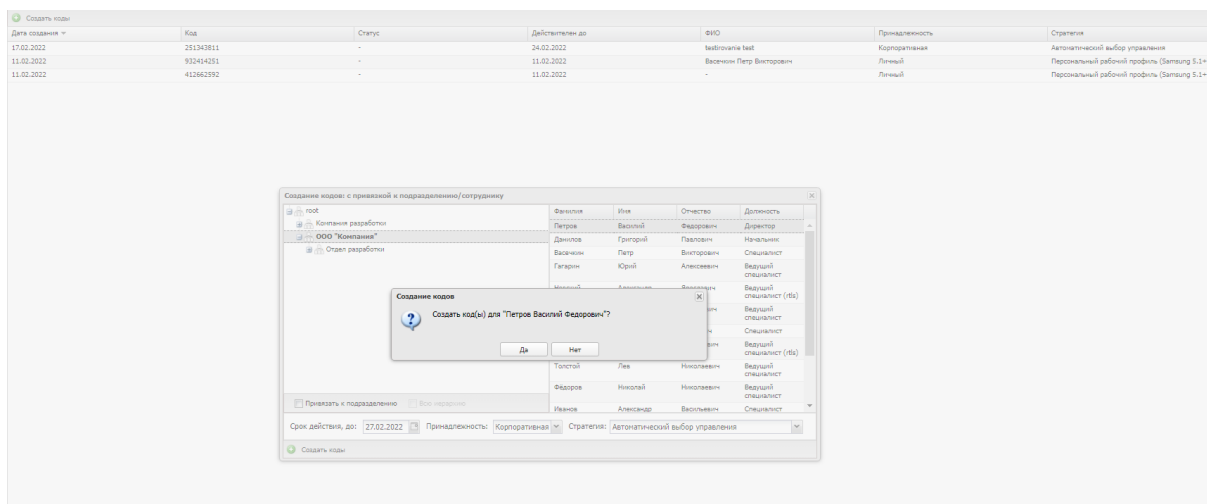


Рисунок 2.128 – Создание кодов с привязкой к сотруднику

«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 **«Всю иерархию»**, если требуется для всех подчиненных сотрудников (рисунок 2.129).

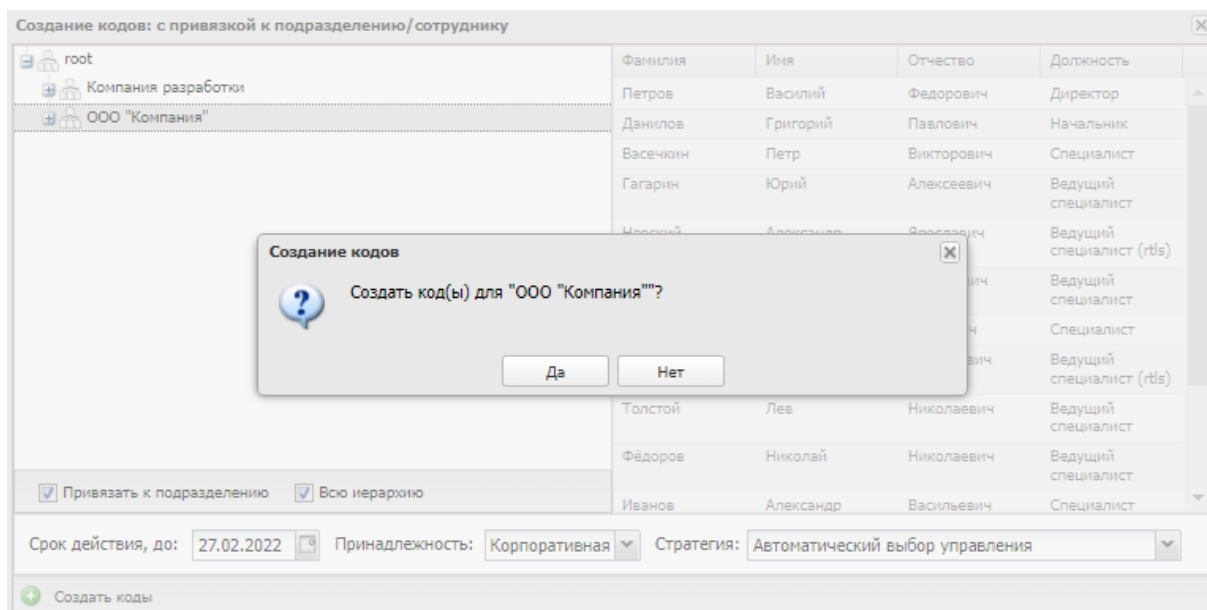


Рисунок 2.129 – Создание кодов с привязкой к подразделению

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 2.130, 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.

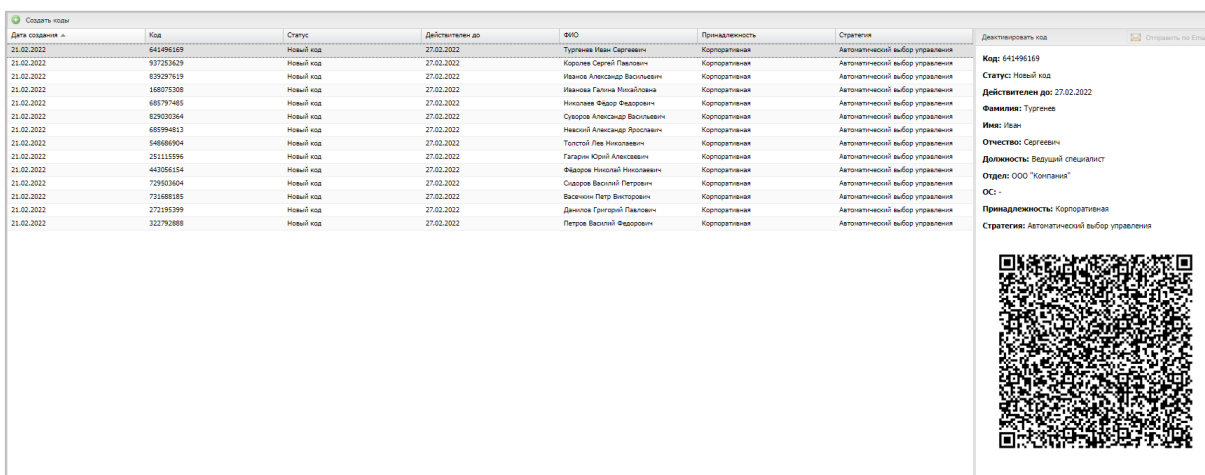


Рисунок 2.130 – Выбор записи с новым кодом

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 2.131):

- Деактивировать код;
- Отправить по Email. Только для кодов в статусе «Новый код» и при наличии у сотрудника заполненного Email.

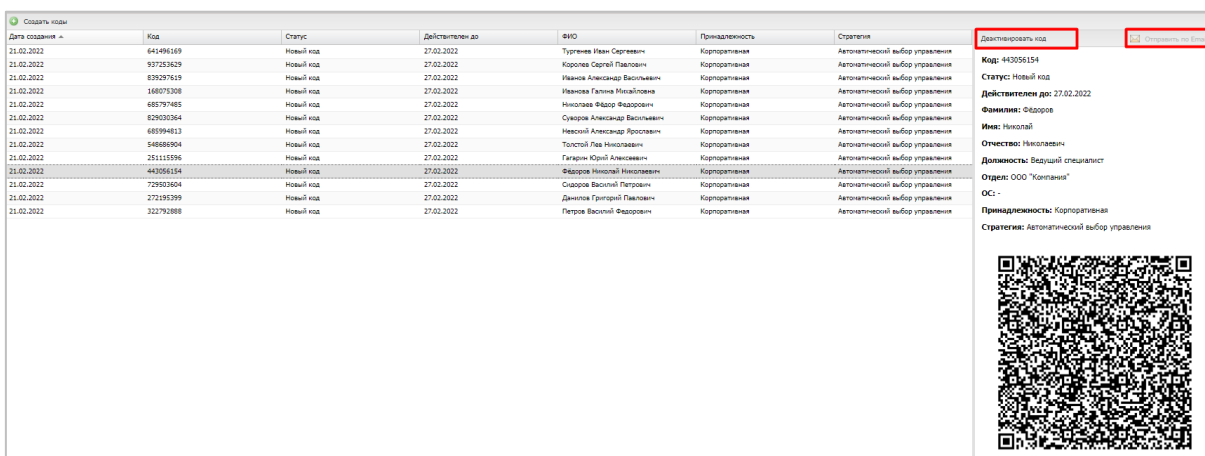


Рисунок 2.131 – Меню «Выбрать действие»

2.10 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 2.132.

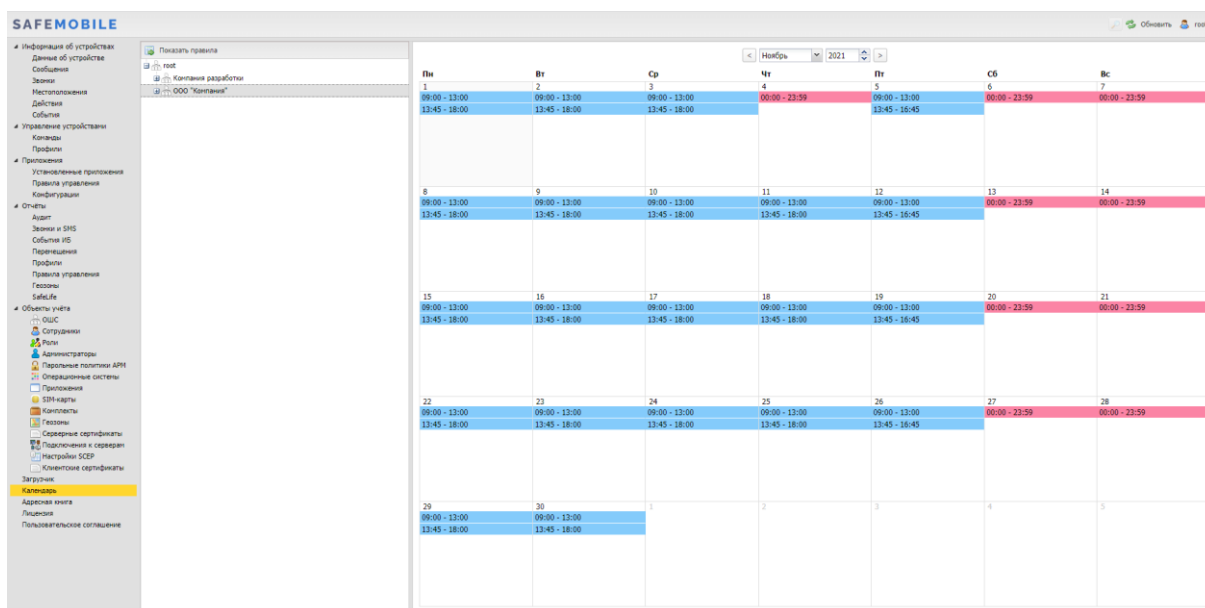



Рисунок 2.132 – Календарь рабочего времени

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 2.133.

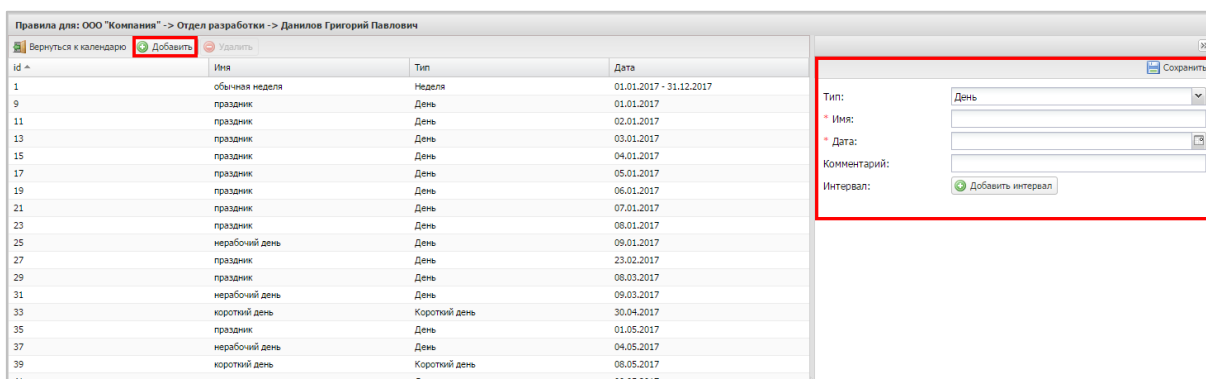


Рисунок 2.133 – Окно создания правил календаря рабочего времени

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 2.134).

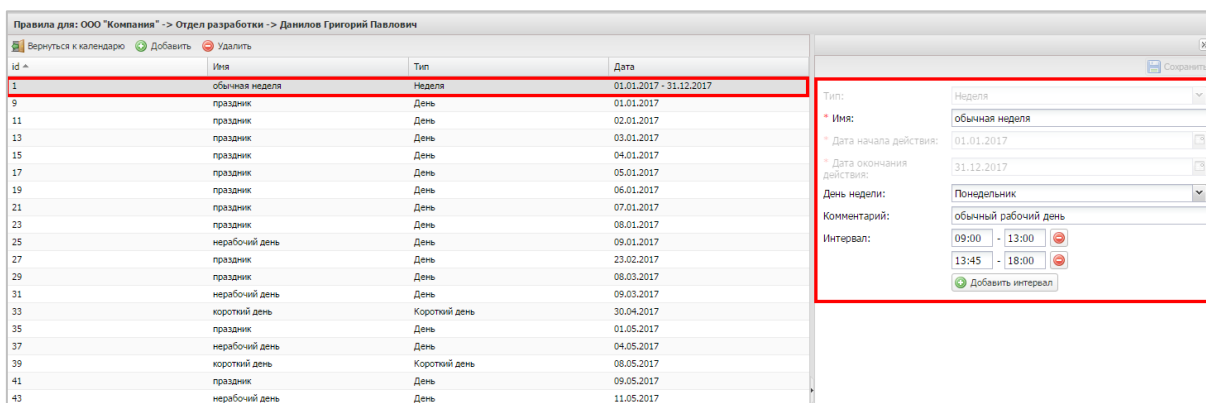


Рисунок 2.134 – Просмотр правила календаря рабочего времени

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.

2.10.1 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 2.135. 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.

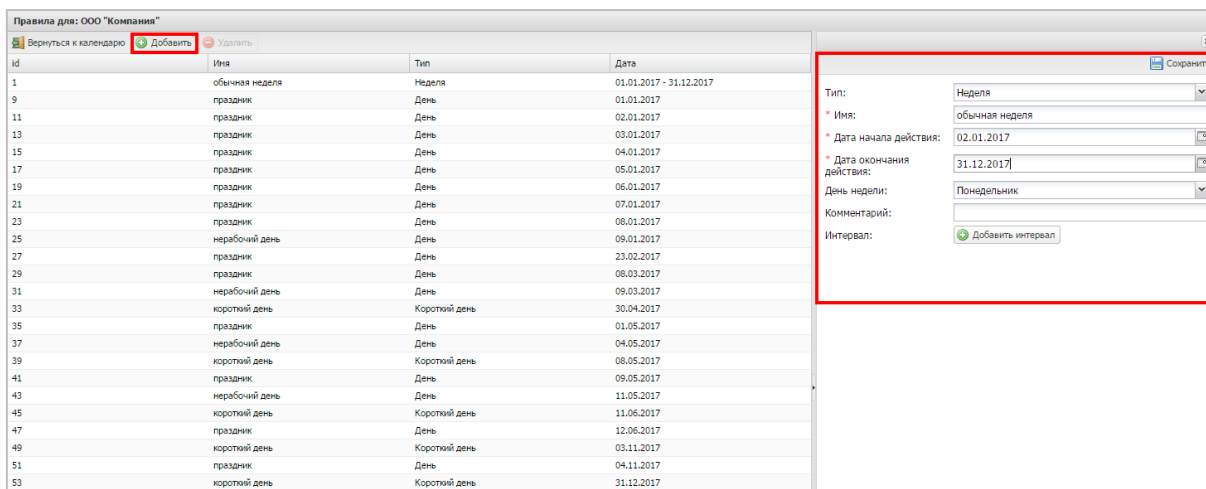



Рисунок 2.135 – Создание правила календаря рабочего времени типа «Неделя»

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 промежутки 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 2.136) необходимо указать следующие обязательные параметры:

- **Имя** – наименование правила;
- **Дата** – дата, к которой будет привязано правило.

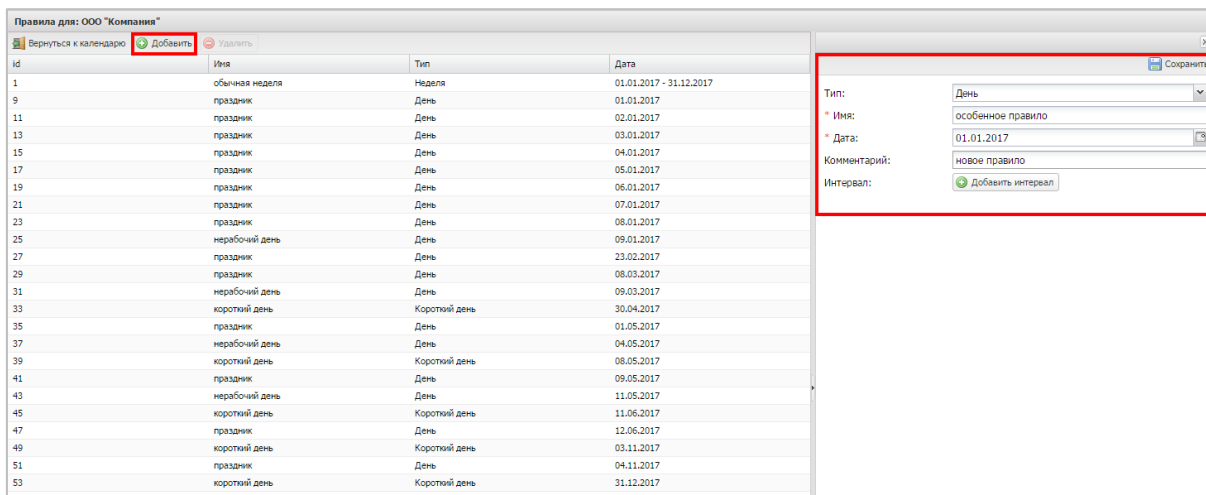


Рисунок 2.136 – Создание правила календаря рабочего времени типа «День»

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 2.137) необходимо указать следующие обязательные параметры:

- **Имя** – название создаваемого правила;
- **Дата** – дата, к которой будет привязано правило.

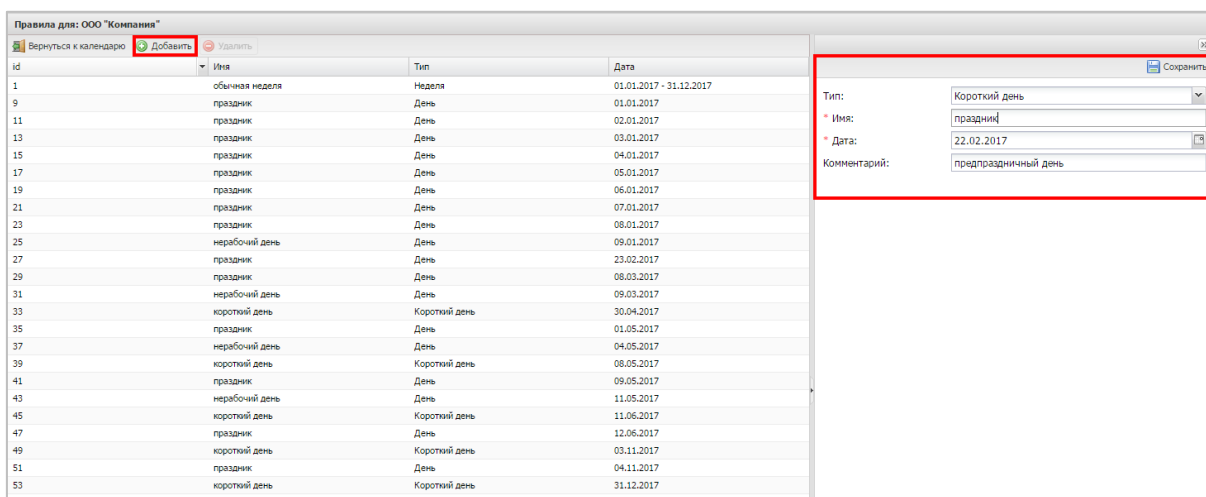


Рисунок 2.137 – Создание правила календаря рабочего времени типа «Короткий день»

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».

2.10.2 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.

2.10.3 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 2.138.

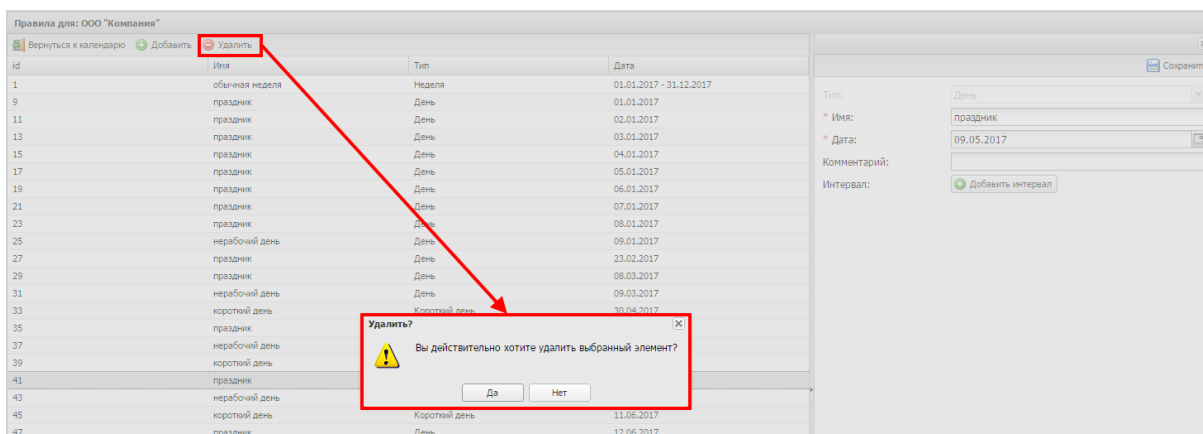


Рисунок 2.138 – Удаление правила календаря рабочего времени

После этого подтвердите действие, нажав «**Да**» в появившемся окне.

2.11 Управление адресной книгой (пункт меню «Адресная книга»)

«UEM SafeMobile» предоставляет возможность использования адресной книги, содержащей список контактов сотрудников организации.

Чтобы открыть окно адресной книги, выберите соответствующий пункт главного меню.

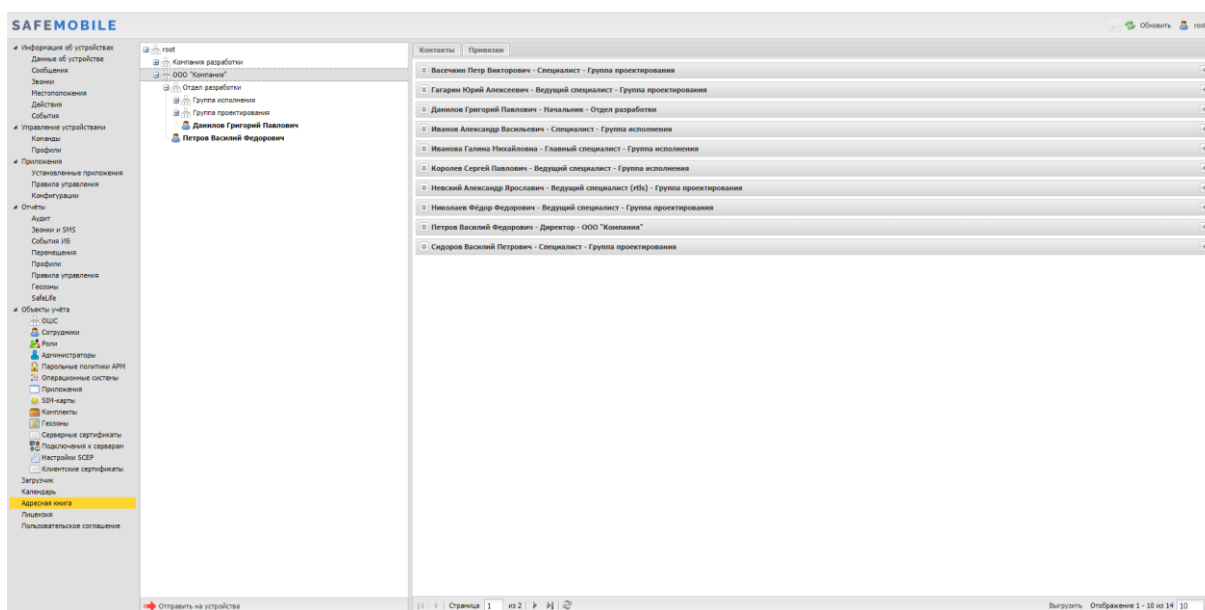


Рисунок 2.139 – Окно адресной книги

Окно адресной книги (рисунок 2.139) состоит из двух частей. В левой части отображается ОШС организации и предназначена для выбора подразделений и сотрудников, которым планируется отправить сформированную адресную книгу. Адресную книгу можно отправить как отдельному сотруднику (или нескольким выбранным сотрудникам),

так и подразделению (нескольким подразделениям) или организации в целом. А в правой расположены две вкладки, предназначенные для управления контактами сотрудников организации, а именно:

- Контакты;
- Привязки.

2.11.1 Вкладка «Контакты»

Во вкладке отображается список абонентов подразделения, выбранного в ОШС.

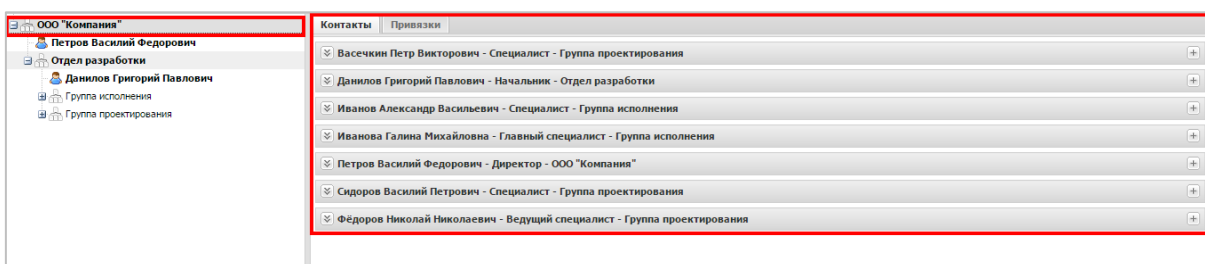


Рисунок 2.140 – Вкладка «Контакты»

ФИО сотрудников, не имеющих привязанного комплекта, отображаются в левой части окна серым шрифтом, в отличие от черного шрифта ФИО сотрудников, обладающих комплектами (рисунок 2.141).

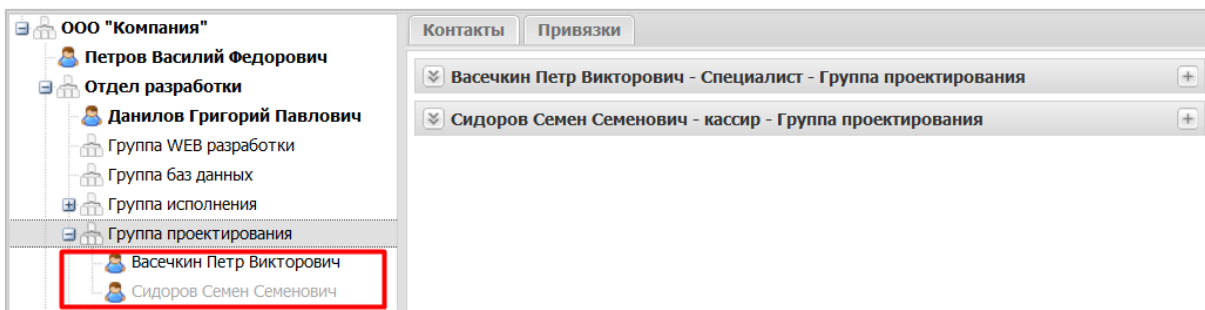


Рисунок 2.141 – Отображение сотрудников с комплектами и без них

Строка записи содержит ФИО абонента, его должность и подразделение, в котором он работает.

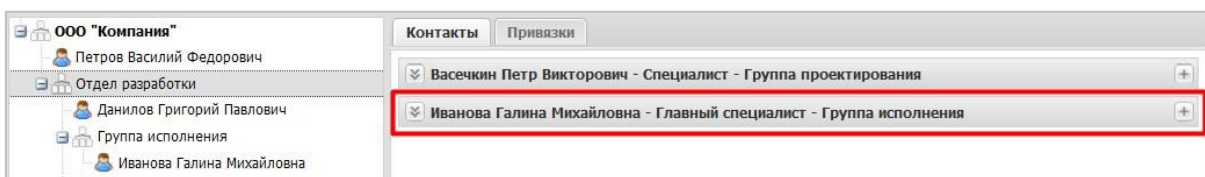




Рисунок 2.142 – Строка записи об абоненте

Чтобы развернуть запись об абоненте, в строке нажмите кнопку , расположенную слева от ФИО.

Запись содержит список контактов абонента следующих типов:

- **Защищенные сообщения** – номера телефонов абонента, используемые для отправки внутренних сообщений с использованием соответствующего клиентского приложения SafeMobile (ЗАС-Сообщения) на устройстве. В качестве номера используется идентификатор МСК, который отображается в столбце **«id»** главной таблицы АРМ;
- **Телефон** – номера телефонов абонента, которые предназначены для выполнения звонков по сети GSM;
- **Защищенные SIP вызовы** – номера телефонов абонента, относящиеся к SIP-аккаунтам, зарегистрированным за МСК абонента;
- **Внутренние номера** – номера телефонов абонента, добавленные в систему Администратором.

Чтобы добавить новый контакт (*внутренний или SIP номер*) в запись об абоненте, нажмите кнопку , расположенную справа от записи абонента.

Откроется окно **«Новый контакт»** в соответствии с рисунком 2.143, в котором необходимо выбрать в раскрывающемся списке **«Тип»** (**«Рабочий мобильный»** или **«Рабочий стационарный»**), а также ввести сам номер в соответствующее поле.

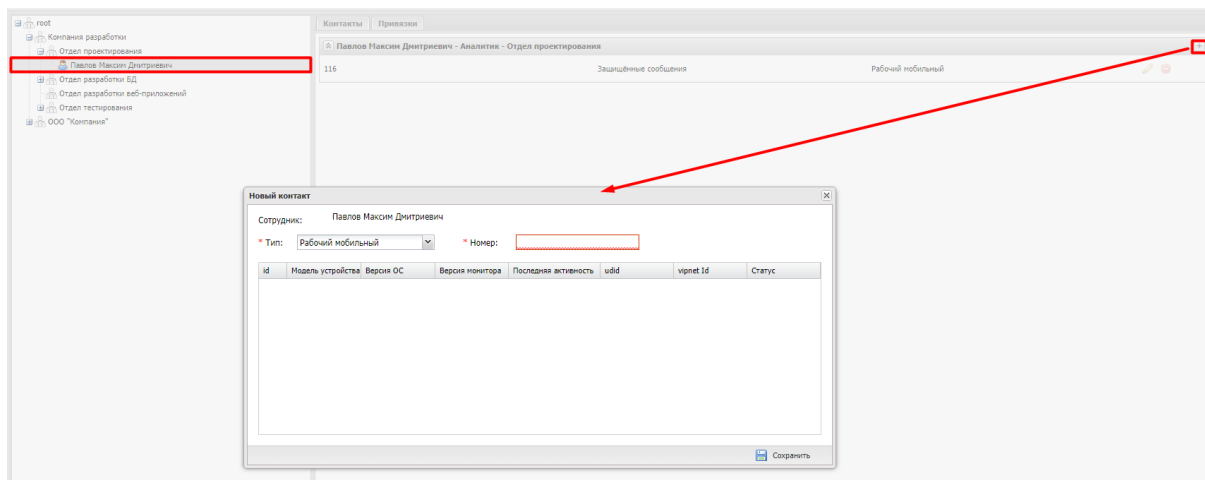


Рисунок 2.143 – Вкладка «Контакты», добавление нового контакта абоненту

В таблице, расположенной в этом окне, отображается список комплектов, относящихся к сотруднику и доступных для привязки к новому номеру телефона. Таблица содержит следующие столбцы:

- **id** – номер комплекта в системе;
- **Модель устройства** – модель устройства, для которой создан комплект;
- **Версия ОС** – версия операционной системы, на которой работает устройство;
- **Версия монитора** – версия приложения SafeMobile, установленного на устройстве;

- **Последняя активность** – время и дата последней активности устройства;
- **udid** – уникальный идентификатор устройства;
- **vipnet Id** – идентификатор vipnet;
- **Статус** – состояние комплекта.

В этой таблице необходимо выбрать комплект, который будет привязан к введенному номеру телефона сотрудника и сохранить созданный контакт, нажав кнопку «**Сохранить**». После этого запись о созданном контакте отобразится в списке контактов абонента.

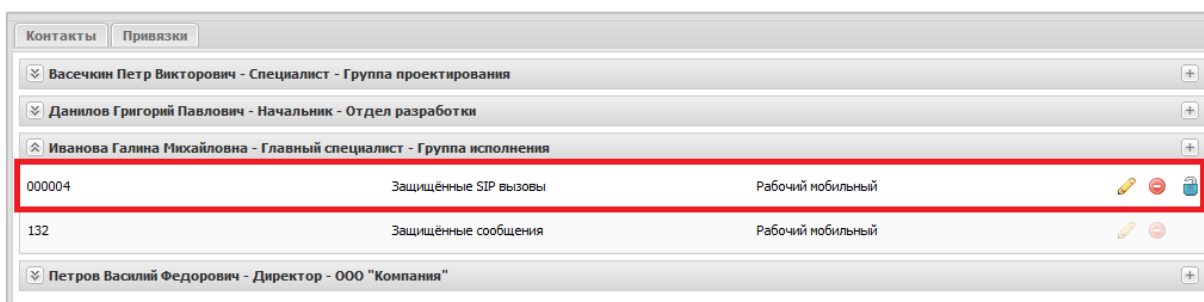





Рисунок 2.144 – Вкладка «Контакты», добавленный новый контакт абонента

Для редактирования записи о контакте следует нажать кнопку , расположенную справа от номера телефона, и после внесения изменений нажать «**Сохранить**». Для удаления номера необходимо нажать кнопку  и подтвердить удаление в окне предупреждения.

Для блокировки SIP-номера следует нажать кнопку  и подтвердить блокировку в появившемся окне предупреждения. После блокировки номера содержащий его контакт будет отображаться в АРМ Администратора со специальным статусом, но не будет отображаться в списке контактов абонента в адресной книге на МСК.

Примечание – Если Администратор удалил SIP-номер и не добавил его вручную заново, то при синхронизации системы номер будет создан автоматически.

2.11.2 Вкладка «Привязки»

Вкладка «**Привязки**» (рисунок 2.145) предназначена для формирования набора абонентов, контактные данные которых будут отправлены выбранным подразделениям (или сотрудникам) в составе адресной книги.

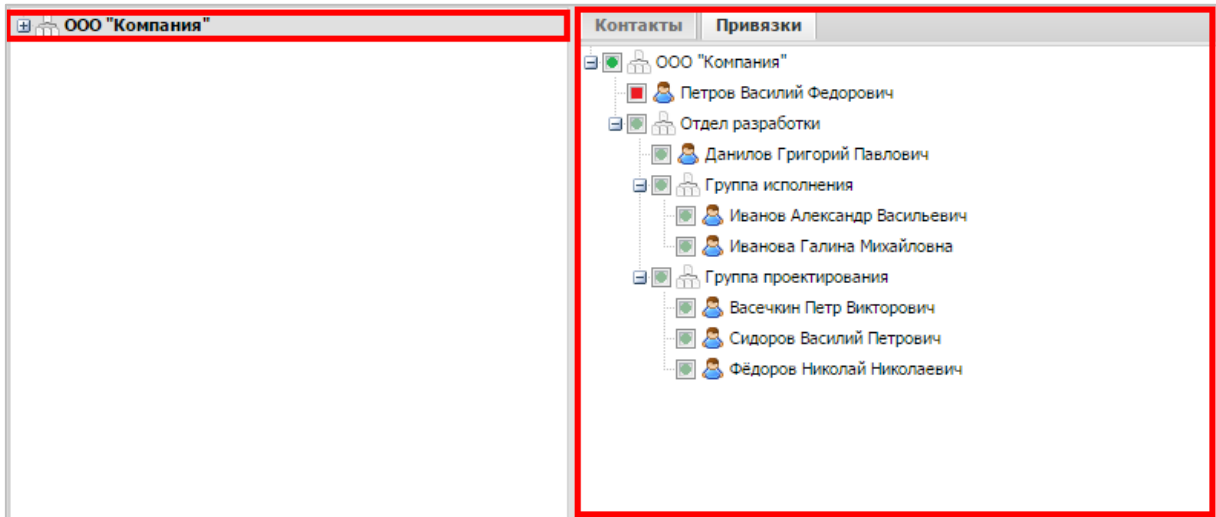


Рисунок 2.145 – Вкладка «Привязки»

Таким образом, система предоставляет возможность гибкого формирования адресной книги и отправки требуемого набора контактных данных только выбранным подразделениям (сотрудникам).

Для указания правил привязки адресной книги к выбранному подразделению в системе предусмотрено следующее акцентирование.

Жирным шрифтом в дереве ОШС отображается подразделение или сотрудник, имеющий собственную адресную книгу. При этом адресная книга, назначенная вышестоящему подразделению, не действует для выделенного жирным подразделения. Дочерние подразделения (сотрудники), не выделенные жирным шрифтом, получают адресную книгу выделенного жирным вышестоящего подразделения.

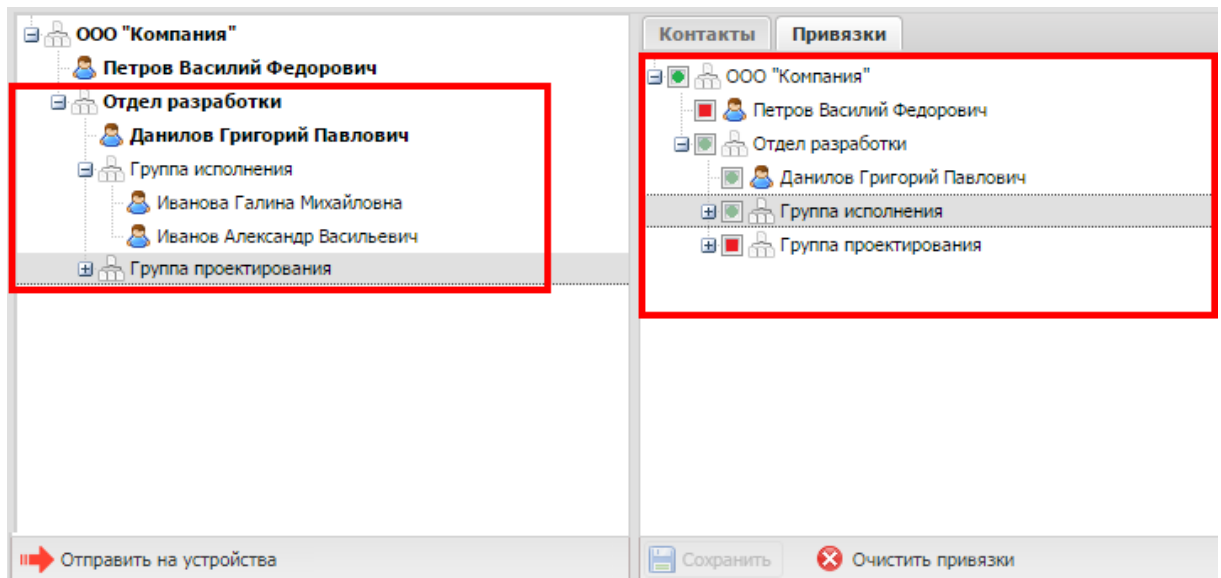







Рисунок 2.146 – Привязка набора контактов выбранному подразделению

Если название узла отображается обычным (нежирным) шрифтом, для него действуют правила формирования адресной книги, назначенные вышестоящему подразделению (обозначенному жирным).


Для сохранения привязки адресной книги необходимо нажать кнопку **«Сохранить»**. Для удаления изменений при редактировании следует нажать кнопку **«Сбросить»**. При нажатии на кнопку **«Очистить привязки»** удаляются все привязки выбранного подразделения, после сохранения для этого подразделения будут действовать правила вышестоящего подразделения.

Примечание – На все МСК сотрудника устанавливается одна и та же корпоративная адресная книга.

На вкладке **«Привязки»** слева от имени сотрудника или названия подразделения расположены цветные значки, показывающие следующие состояния включения в адресную книгу элемента, которому они принадлежат:

-  – элемент и все его вложенные элементы вручную включены в адресную книгу;
-  – элемент и все его вложенные элементы включены в адресную книгу автоматически, после включения вышестоящего элемента;
-  – элемент и все его вложенные элементы исключены из адресной книги вручную;
-  – элемент и все его вложенные элементы исключены из адресной книги автоматически, после исключения вышестоящего элемента;
-  – элемент не включен в адресную книгу.

Для формирования правил адресной книги необходимо выполнить следующие действия:

1. Выберите в ОШС объект, например, головную организацию. Затем выберите во вкладке **«Привязки»** корневой элемент адресной книги (чтобы отобразился значок ) и нажмите кнопку **«Сохранить»**. После этого всем сотрудникам организации будет назначена полная адресная книга со всеми имеющимися абонентами и их контактами.

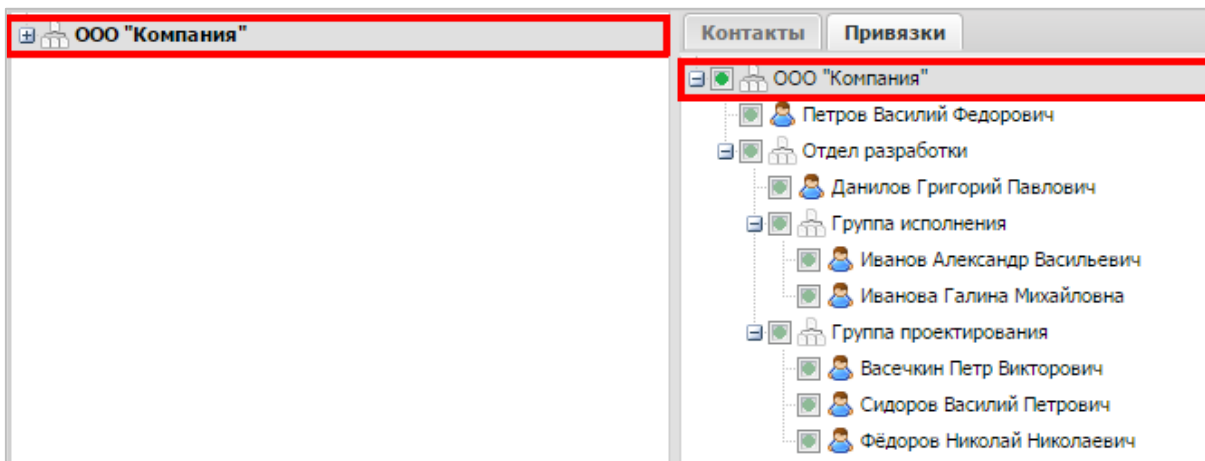



Рисунок 2.147 – Привязка полной адресной книги ко всей организации

2. Если необходимо для конкретного подразделения организации исключить из адресной книги контакты сотрудников определенных подразделений. Для этого в ОШС выберите подразделение, для которого будет сформирована индивидуальная адресная книга. Затем во вкладке «Привязки» выберите подразделение или сотрудника, чьи контакты требуется исключить из формируемой адресной книги. При этом слева от имени сотрудника или названия подразделения отобразится значок . Нажмите кнопку «Сохранить», после чего название подразделения отобразится **жирным** шрифтом.

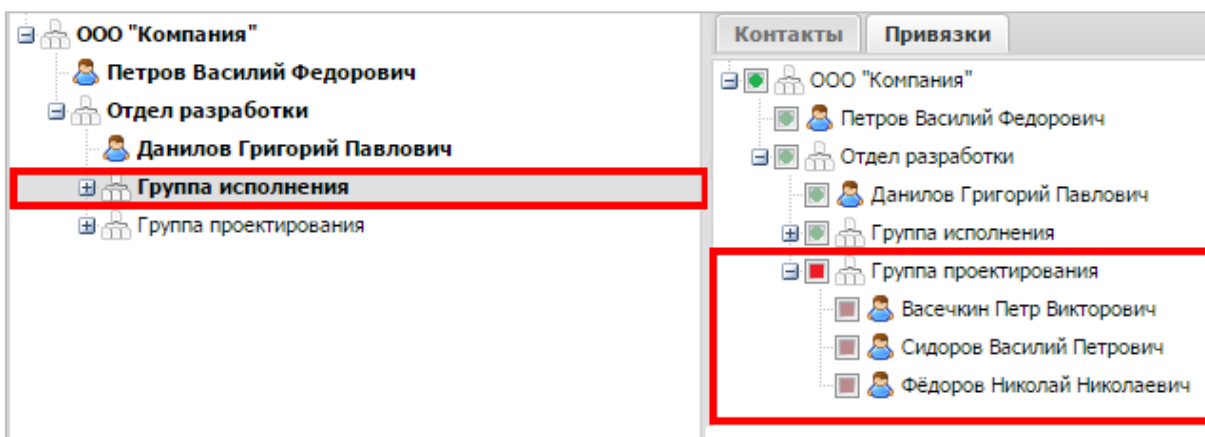


Рисунок 2.148 – Исключение абонентов подразделения из индивидуальной адресной книги

3. Если необходимо одного из сотрудников исключенного подразделения включить в индивидуальную адресную книгу, измените цвет красного значка на зеленый и снова нажмите кнопку «Сохранить».

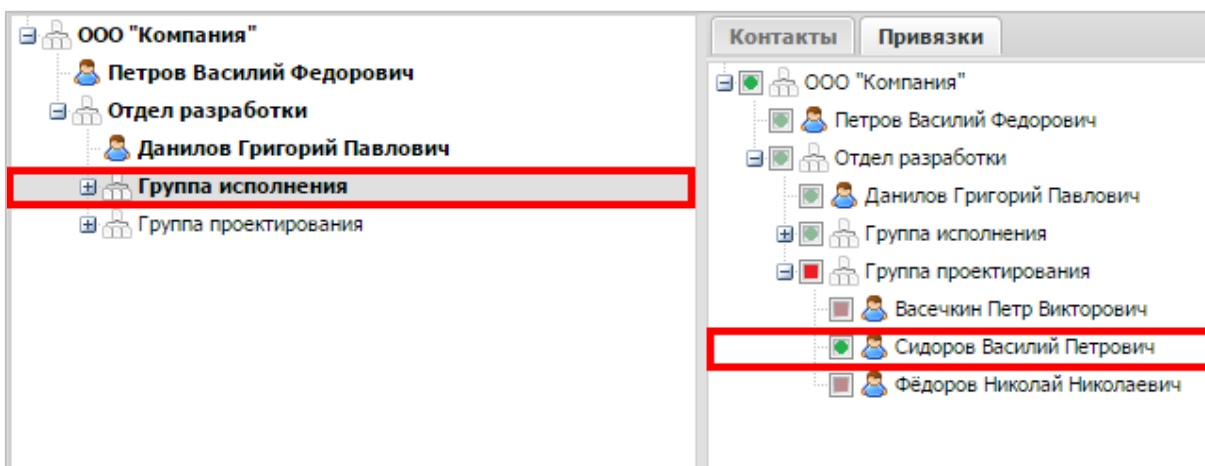


Рисунок 2.149 – Включение сотрудника исключенного подразделения в адресную книгу

4. После завершения формирования адресной книги и привязки ее к требуемым подразделениям или сотрудникам необходимо отправить ее на корпоративные МСК, нажав кнопку «Отправить на устройства», расположенную под ОШС.

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

Пункт главного меню «Лицензия» предназначен для активации лицензии на использование системы. Для этого необходимо информацию из полученного лицензионного файла поместить в поле окна «Лицензия» (рисунок 2.150), которое является обязательным для заполнения. Затем нажать кнопку «Сохранить».

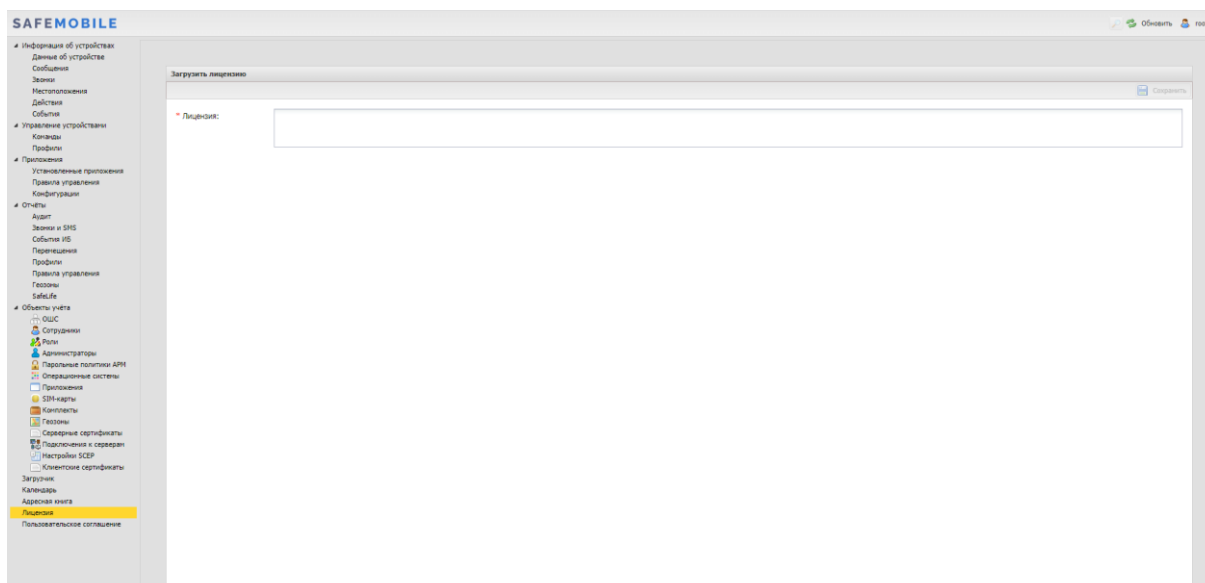


Рисунок 2.150 – Окно «Лицензия»

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.

2.13 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 2.151), 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»**.

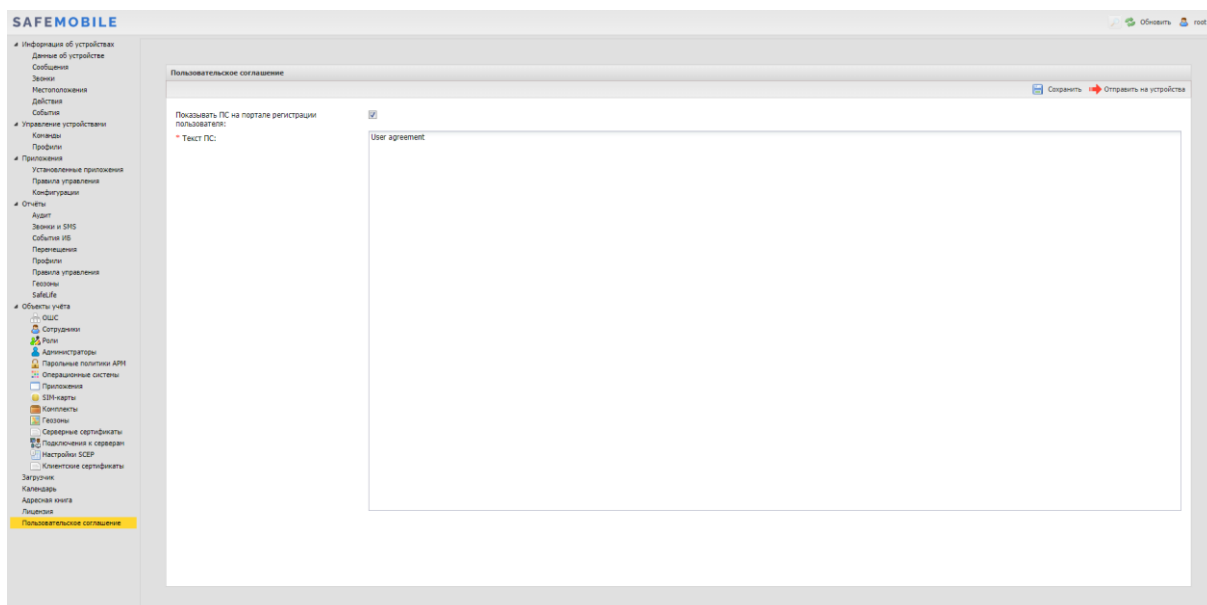


Рисунок 2.151 – Окно «Пользовательское соглашение»

2.14 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.

2.15 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 APM 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:

1. В адресной строке наберите **about:config** и нажмите клавишу **Enter**.
2. Может появиться страница предупреждения **about:config** «**Будьте осторожны, а то лишитесь гарантии!**». Щелкните кнопку «**Я обещаю, что буду осторожен!**», чтобы перейти на страницу **about:config**.
3. На странице **about:config** найдите настройку **dom.max_script_run_time** и дважды щёлкните по ней.
4. Увеличьте исходное значение.
5. Нажмите ОК.

Вопрос 2: что делать, если при смене пароля после успешной аутентификации появляется окно **Подтверждение смены пароля с выбором пользователя**.

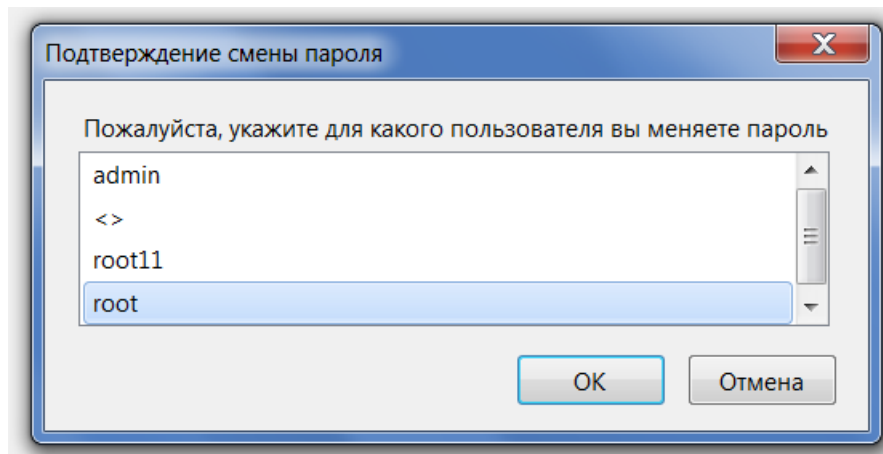


Рисунок 3.1 – Окно подтверждения смены пароля

Ответ: отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox.

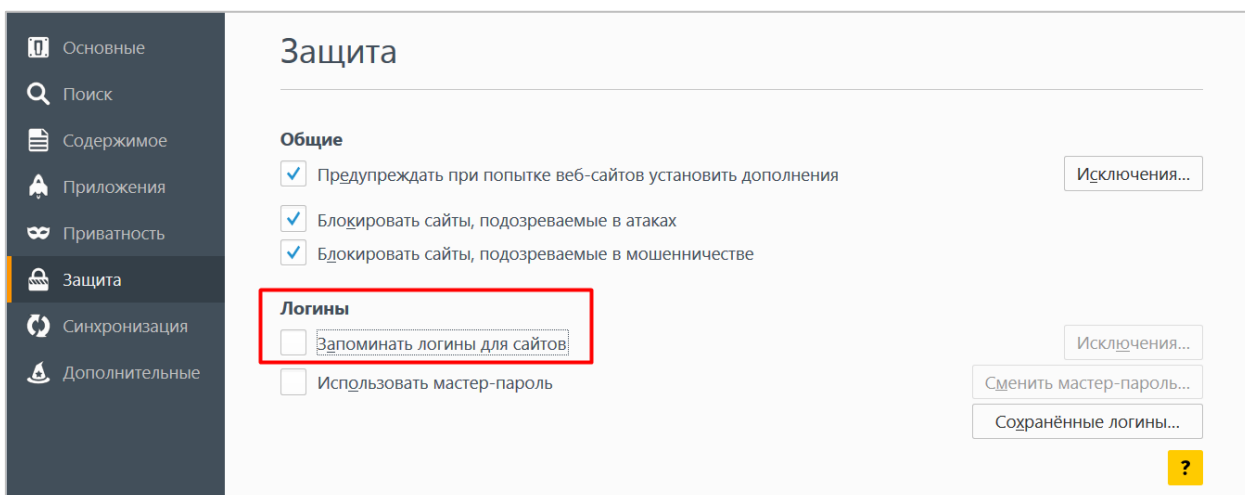


Рисунок 3.2 – Настройка отмены автозаполнения логина и пароля в браузере Firefox

Вопрос 3: что делать, если при открытии раздела главного меню «Администраторы» поле логин и пароль заполнено логином и паролем, сохраненным в окне аутентификации?

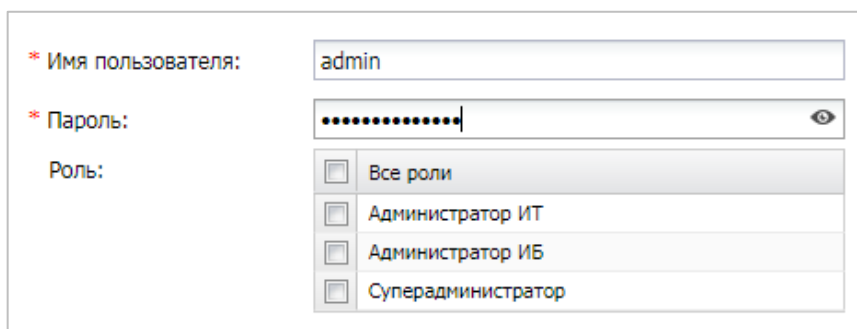


Рисунок 3.3 – Автозаполнение пароля и логина в окне управления Администраторами

Ответ: отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox.

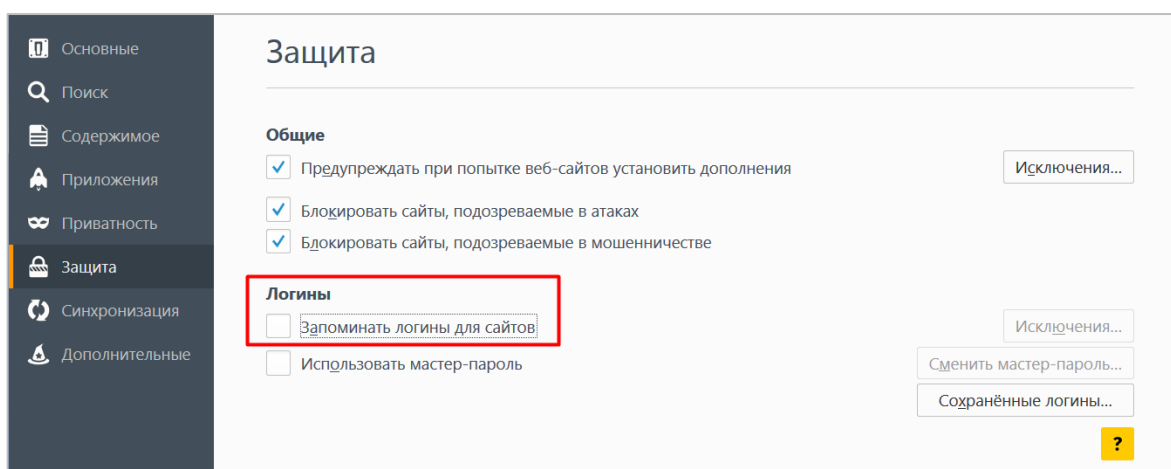


Рисунок 3.4 – Настройка отмены автозаполнения логина и пароля в браузере Firefox

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:

- A.1 Скачать и запустить ПО Apple Configurator 2.
- A.2 Подключить iPhone (iPad) к ПК Mac.
- A.3 Выбрать подключенное МСК и нажать кнопку **«Prepare»** (подготовить) в соответствии с рисунком А.1.

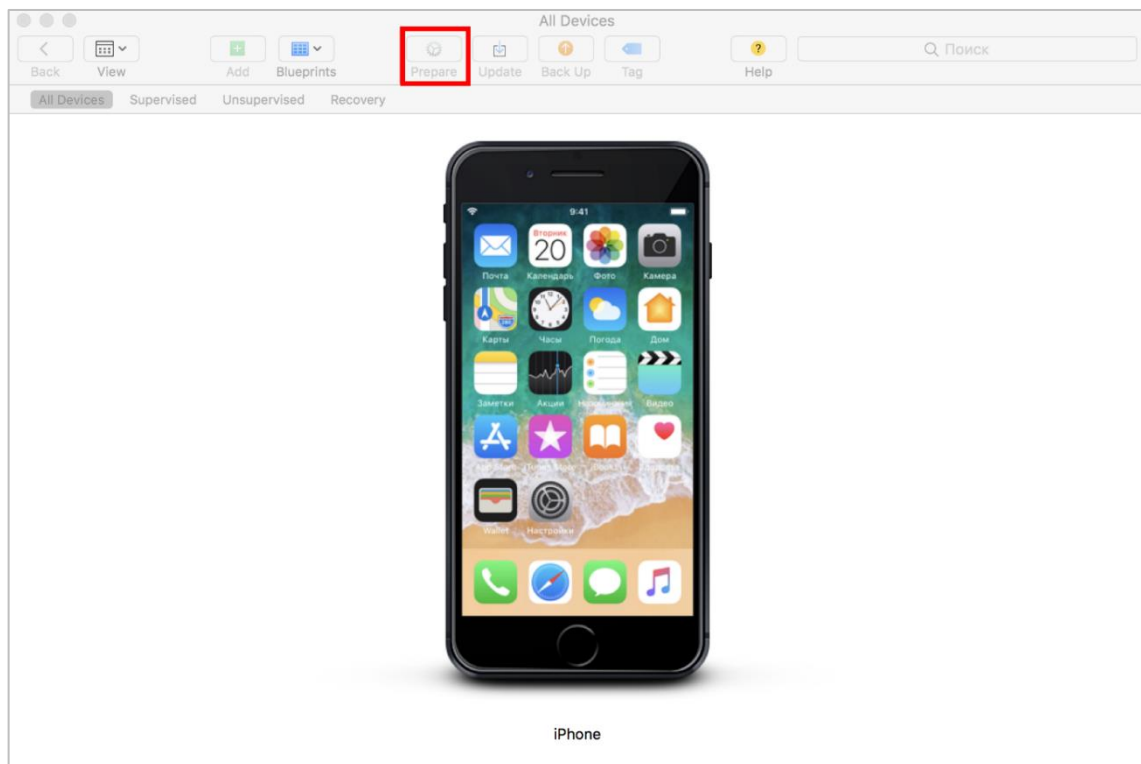


Рисунок А.1 – Окно подключенных устройств

A.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

А.5 В поле «**Server**» (рисунок А.3) выбрать значение «**Do not enroll in MDM**» (не регистрироваться в MDM) и нажать кнопку «**Next**».

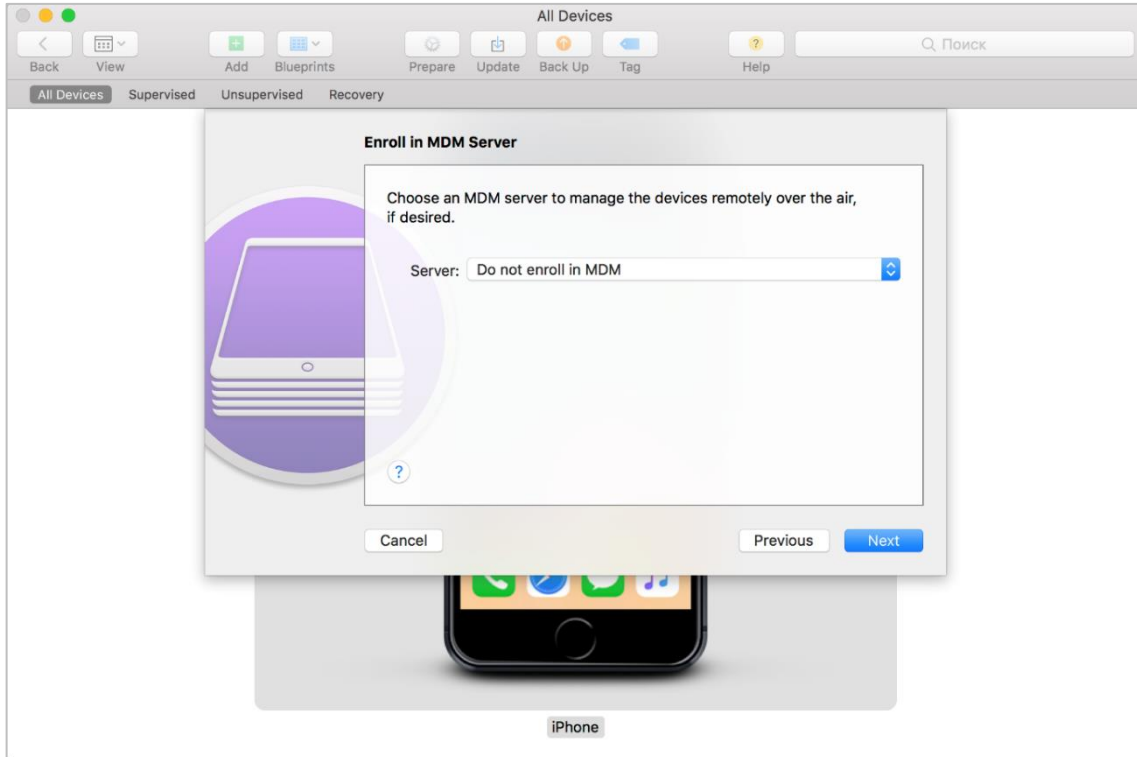


Рисунок А.3 – Выбор MDM сервера

А.6 Ввести значения своей учетной записи (Apple ID/Пароль), зарегистрированной в ADEP, в соответствии с рисунком А.4. Если учетной записи нет, то следует

нажать кнопку «Skip» и перейти к форме на рисунке A.5.

Примечание – Учетная запись должна быть корпоративной для администратора системы, а не персональной.

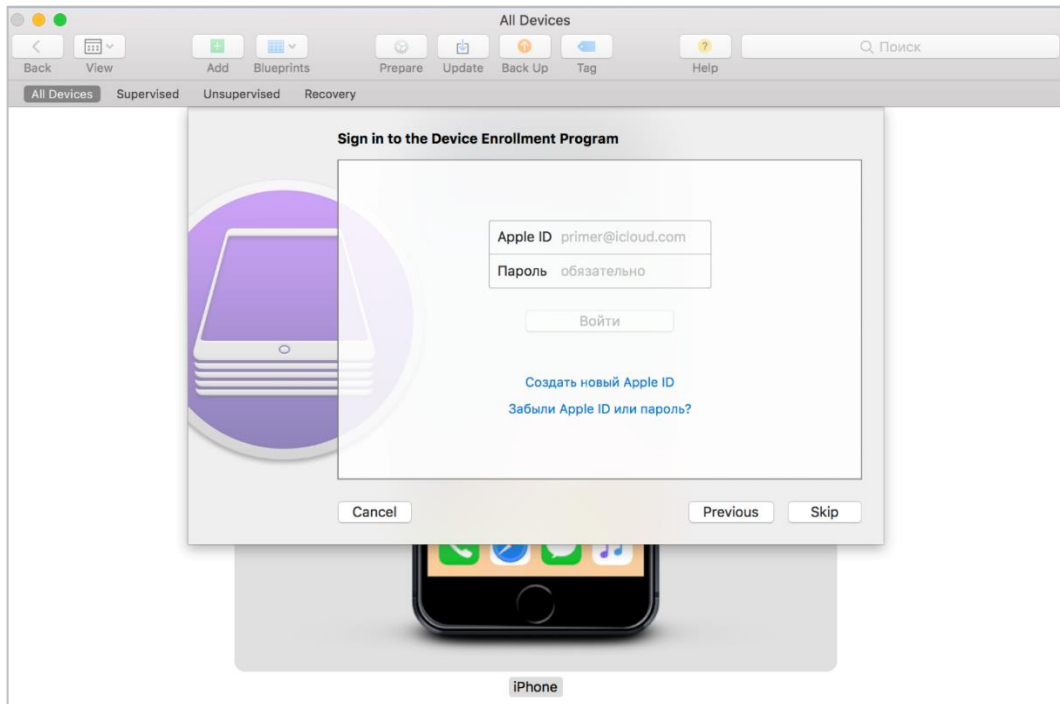


Рисунок A.4 – Аутентификация в ADEP

A.7 В поле «Name» (рисунок A.5) следует указать название организации, остальные поля можно оставить пустыми и нажать «Next».



Рисунок A.5 – Создание записи о контролирующей организации

A.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

А.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).

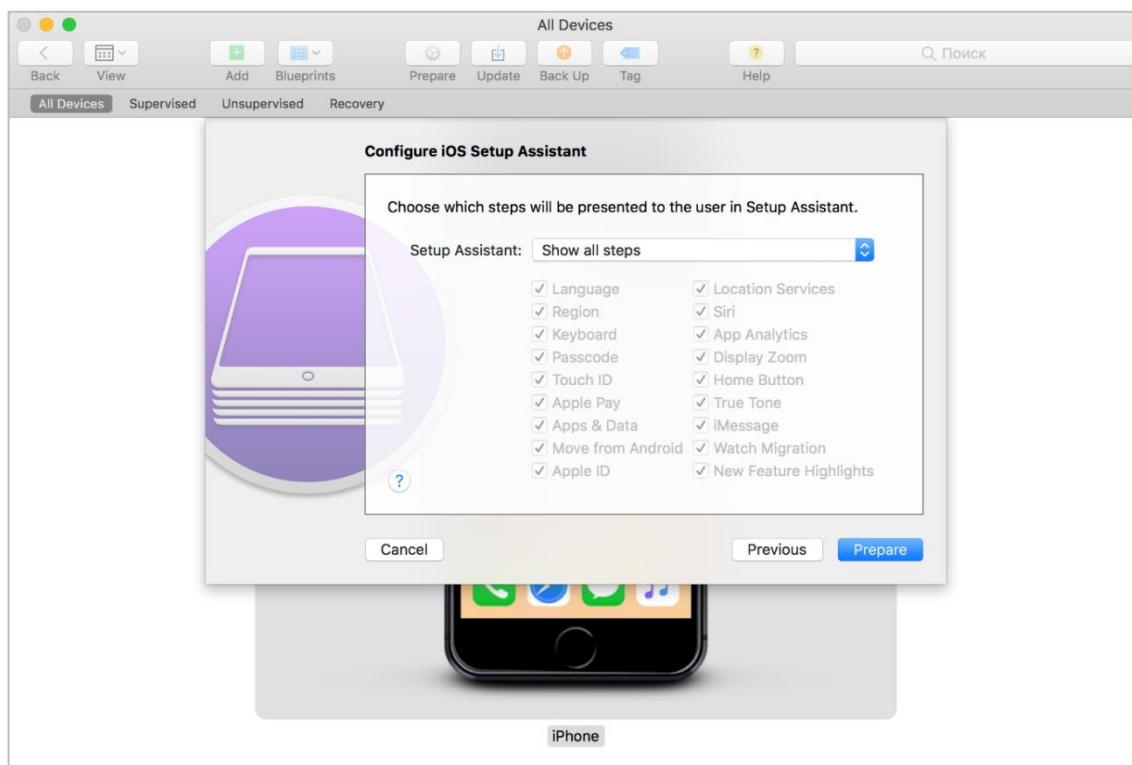


Рисунок А.7 – Выбор параметров первоначальной конфигурации МСК

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»**.

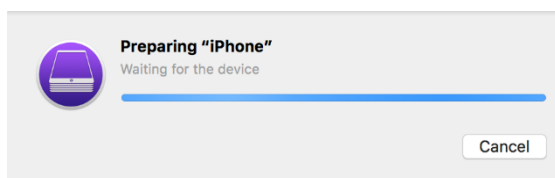


Рисунок А.8 – Индикация процесса подготовки устройства

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.

А.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.

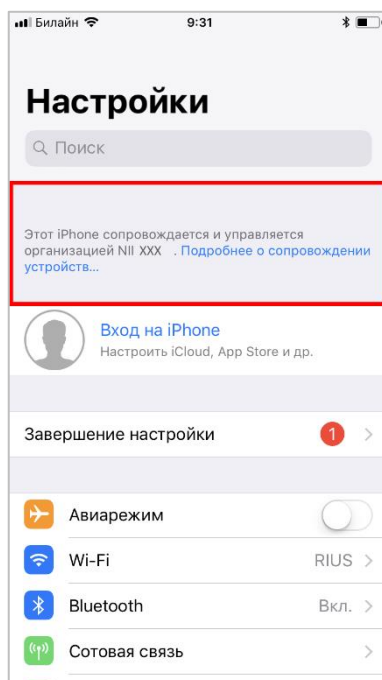


Рисунок А.9 – Сообщение о контроле над устройством в приложении «Настройки»

А.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 OS	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 MCK iOS	Изменить параметр команды и отправить команду повторно. Параметры команд приведены в 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.mobletimer
 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», «Адресная книга», «Пользовательское соглашение»
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 выполняться 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.