



ФЛАТ

ФЛАТ SoftSwitch

Программный коммутатор корпоративных
сетей IP-телефонии

Руководство по установке и
администрированию

для версии 4.1

Версия документа: 3.39

Оглавление

Уведомление	6
Рассматриваемое ПО.....	6
Связанные документы.....	6
История изменений документа.....	6
1. Краткое описание и назначение продукта	8
Поддерживаются следующие стандарты:.....	8
2. Аппаратные и программные требования	10
Технические требования к платформе ядра SIP SoftSwitch	10
Технические требования к платформе Медиасервер в режиме записи	10
Поддерживаемые решения, протоколы и кодеки:	11
Требования к платформам виртуализации	11
3. Архитектура решения	12
3.1. Компоненты системы ФЛАТ SoftSwitch	12
3.2. Отказоустойчивость.....	13
3.3. Логическое деление.....	14
4. Описание сценариев отказоустойчивости	16
4.1. Сценарий 1	16
4.2. Сценарий 2	19
5. Стоимость программного обеспечения	23
6. Активация лицензий	24
7. Установка на Debian и Astra Linux	25
7.1. Предустановочные действия.....	25
7.2. Отключение SELinux	25
7.3. Настройки сети, даты и времени	26
7.4. Доступ к репозиторию	28
7.5. Установка системы ФЛАТ SoftSwitch.....	29
7.5.1. Установка сервиса FlatFileManager	31
7.5.2. Установка фронтенда и бэкенда SoftSwitch, ЛК пользователя	33
7.6. Выключение и перезапуск системы.....	43
7.7. Обновление системы	43
7.8. Удаление системы.....	43
7.9. Откат на предыдущую версию	44
7.10. Обновление лицензионных ключей.....	44
7.11. Настройка SIP-TLS	44
8. Ротация логов	45
8.1. Ротация логов с помощью Logrotate.....	45
8.2. Ротация логов сервиса FlatFileManager, бэкенда SoftSwitch и ЛК	46

9.	Доступность WEB-интерфейса и проверка работоспособности	48
9.1.	Настройки для формы авторизации	48
9.2.	Вход в WEB-интерфейс.....	48
9.3.	Проверка работоспособности	49
10.	Настройка системы.....	51
10.1.	Этапы настройки системы	51
10.2.	Подключение к WEB-интерфейсу	51
10.3.	Параметры системы	52
10.3.1.	Администраторы	52
10.3.2.	Тарификация	60
10.3.3.	Логирование.....	62
10.3.4.	Диагностика.....	65
10.3.5.	Фильтры	66
10.4.	Зона.....	67
10.4.1.	Создание зон	67
10.4.2.	Создание локаций.....	67
10.4.3.	Абоненты	71
10.4.4.	Группы.....	81
10.4.5.	Транки	85
10.4.6.	Маршрутизация	90
10.4.7.	Сервисные коды.....	108
10.4.8.	Классификация	110
10.4.9.	АОН.....	114
10.4.10.	Черные/Белые списки на уровне зон.....	118
10.4.11.	Маршруты в аварийном режиме	120
10.5.	Глобальная маршрутизация	120
10.5.1.	Зоны	120
10.5.2.	Глобальные области	121
10.5.3.	Маршрутизация глобальная	122
10.5.4.	Все абоненты.....	128
10.5.5.	Контроль вызовов.....	129
10.6.	Оборудование	130
10.6.1.	Кластер.....	130
10.6.2.	Медиасерверы	131
10.6.3.	Живучий Офис	132
10.7.	Резервные копии	137
10.7.1.	Цели	137
10.7.2.	Задания	140

10.8. Задачи.....	142
Приложения.....	143
Изменение наименований пакетов	143
Лицензионное соглашение.....	144
Предоставление лицензии	144
Сохранение права собственности и прочих прав.....	144
Ограничение на вскрытие технологии, декомпиляцию и деасемблирование.....	145
Запрет на передачу во временное пользование и коммерческое использование	145
Дополнительное программное обеспечение и службы.....	145
Программное обеспечение, не предназначенное для перепродажи.....	145
Прекращение действия соглашения.....	145
Полнота соглашения и ограничение недействительности	145
Взаимодействие с пользовательским интерфейсом.....	146
Лицензирование	149
Список администрируемых систем в форме авторизации	150
Матрица портов и разрешённых соединений	151
Аутентификация пользователей с использованием AD и SSO.....	154
Настройка бэкенда ФЛАТ SoftSwitch.....	155
Настройка фронтенда ФЛАТ SoftSwitch	157
Регулярные выражения в правилах маршрутизации	158
Регулярные выражения при проверке номера	158
Регулярные выражения при модификации номера	159
Сценарии использования.....	160
Применение ролей пользователей	160
Применение профиля абонента.....	161
Применение групп перехвата.....	162
Применение классов сервиса и ограничений.....	166
Настройка отправки уведомлений о пропущенных вызовах	174
Функции и возможности системы ФЛАТ SoftSwitch	175
Интервал проверки состояния транка	175
Таймаут ожидания ответа на вызов.....	175
Индикация статусов BLF	175
Дополнительные виды обслуживания	176
Функция «Обратный вызов».....	176
Функция «Перехват вызова в группе»	176
Множественная регистрация	176
Функция «Shared line»	176
SNMP мониторинг.....	178

SNMP мониторинг ядра ФЛАТ SoftSwitch	178
SNMP мониторинг Медиасервера	178
Формат аудиофайлов пользовательских звуковых оповещений.....	179
Конвертация аудиофайла (Linux)	179
Конвертация аудиофайла на примере приложения Audacity (Windows).....	179
Описание конфигурационных файлов	182
Ядро системы	182
Бэкенд WEB-интерфейса ФЛАТ SoftSwitch	184
Фронтенд WEB-интерфейса ФЛАТ SoftSwitch	189
FlatFileManager.....	189
Сервис Mediasrv.....	191
Сервис SRClient.....	191
Словарь аббревиатур и сокращенных слов.....	192
Таблица маршрутизации.....	193
Общая схема маршрутизации	193
Внутрizonовая маршрутизация	194
Глобальная маршрутизация	195
Модификация АОН	196

Уведомление

Информация, содержащаяся в этом документе, считается точной и надежной на момент печати. Однако из-за постоянных улучшений и изменений продуктов ООО «ФЛАТ» не может гарантировать точность печатных материалов после даты публикации и не может принять ответственность за ошибки или упущения.

Обновление этого документа доступно по адресу <https://partnerportal.flat-soft.ru/pages/viewpage.action?pageId=2031707>.

Этот документ может быть изменен без предварительного уведомления.

Информация о выходе обновлений рассматриваемого в этом документе программного обеспечения размещается:

- на партнерском портале <https://partnerportal.flat-soft.ru>
- на портале поддержки <https://portal.flat-soft.ru>

Рассматриваемое ПО

Наименование	Номер релиза
Ядро ФЛАТ SoftSwitch	v.4.2
Бэкенд ФЛАТ SoftSwitch	v.4.2
Фронтенд ФЛАТ SoftSwitch	v.4.2
Бэкенд ЛК пользователя	v.4.2
Фронтенд ЛК пользователя	v.4.2
Менеджер файлов	v.1.0
Сервис Mediasrv	v.4.2
Сервис SRClient	v.4.2

Связанные документы

Наименование документа
ФЛАТ Software. Технические требования
ФЛАТ Software. Матрица портов и разрешённых соединений
ФЛАТ SoftSwitch. Руководство по установке

История изменений документа

Дата	Изменения
17.05.2023	Первоначальный выпуск документа для версии 2.5
02.11.2023	Обновлено для версии 3.0
13.02.2024	Дополнено главой Живучий Офис.
28.08.2024	Дополнено главой «Аутентификация с Active Directory».
15.11.2024	Обновлено для версии 3.2

Дата	Изменения
03.07.2025	Обновлено для версии 4.1 Изменение наименований пакетов и связанных с ними ресурсов.
29.11.2025	Обновлено для версии 4.2 Изменение наименований пакетов и связанных с ними ресурсов.



При установке и администрировании компонентов системы ФЛАТ SoftSwitch версий v.4.1 – 4.2 следует учитывать происходящую поэтапную замену наименований инсталляционных пакетов, сервисов, каталогов расположения, названий файлов журналов событий (см. [Изменение наименований пакетов](#)).

1. Краткое описание и назначение продукта

ФЛАТ SoftSwitch – программный комплекс, предназначенный для построения сетей IP-телефонии корпоративного уровня. В основе решения лежит взаимодействие по протоколу SIP для передачи голоса и данных. ФЛАТ SoftSwitch обладает законченным, полнофункциональным набором бизнес-функций, может развертываться в дата-центрах компаний в виртуальной среде или на базе стандартного серверного оборудования.

Основные параметры ФЛАТ SoftSwitch:

- Работа с высокой нагрузкой до 25 000 одновременных сессий на один узел в круглосуточном режиме с количеством абонентов до 100 000 на узле кластера, но не более 100 000 абонентов на всех узлах.
- Выдерживает нагрузку до 120 одновременных вызовов в секунду. По результатам нагрузочного теста в дамп сетевого трафика все входящие SIP сообщения получили корректные коды ответов, сессии установлены корректно, после чего корректно завершены.
- Высокая надежность – дублированный кластер с коэффициентом доступности 99,99%.
- Модульная архитектура. Все модули поддерживают виртуализацию.
- Построение распределенных систем с поддержкой георезервирования (размещения узлов на географически разнесенных площадках), дублирование каналов для повышения связности – обеспечивает непрерывную доступность сервисов даже в случае выхода из строя одного из узлов.
- Круглосуточная работа. Не требует перезагрузки при изменениях в конфигурации, кроме процедуры установки обновлений.
- В качестве абонентских устройств могут применяться как физические, так и программные телефонные аппараты, поддерживающие протокол SIP, таких производителей как Cisco, Unify, Avaya, Atcom, Yealink, Fanvil, AudioCodes и др. Таблица поддерживаемых телефонных аппаратов различных производителей доступна в документе «ФЛАТ SoftSwitch. Описание продукта» по адресу <https://partnerportal.flat-soft.ru/pages/viewpage.action?pageId=2031707>.

ФЛАТ SoftSwitch поддерживает виртуализированную архитектуру, в том числе отечественного производства, или может размещаться на независимой серверной платформе, удовлетворяющей требованиям архитектуры и конфигурации системы.

Высокий уровень надежности комплекса ФЛАТ SoftSwitch обеспечивается за счет функционирования на двухкомпонентном резервируемом кластере, работающем в режиме Active-Active. При выходе из строя одной части вторая в горячем режиме продолжит обработку вызовов. Обрыва текущих соединений не происходит, за исключением случаев принудительного проксирования RTP трафика и случае использования методов записи, подразумевающих проксирование.

Для подключения аппаратных интерфейсов, таких как FXS/FXO и E1, могут использоваться шлюзы сторонних производителей.

Поддерживаются следующие стандарты:

SIP

- RFC 3261 “SIP: Session Initiation Protocol”;
- RFC 3326 “The Reason Header Field for the Session Initiation Protocol (SIP)”;
- RFC 2976 “The SIP INFO Method”.

Privacy

- RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”;
- RFC 3324 “Short Term Requirements for Network Asserted Identity”;
- RFC 3325 “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”;
- SIP Extensions for Caller Identity and Privacy (спецификация Cisco по обработке Remote-Party-ID).

Расширения SIP

- RFC 3262 “Reliability of Provisional Responses in Session Initiation Protocol (SIP)”;
- RFC 3265 “Session Initiation Protocol (SIP) – Specific Event Notification”;
- RFC 3311 “The Session Initiation Protocol (SIP) UPDATE Method”;
- RFC 3515 “The Session Initiation Protocol (SIP) Refer Method”;
- RFC 3581 “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”;
- RFC 3891 “The Session Initiation Protocol (SIP) "Replaces" Header”;
- RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”;
- RFC 5806 “Diversion Indication in SIP”;
- The Calling Party's Category tel URI Parameter;

Аутентификация запросов

- RFC 2069 “An Extension to HTTP: Digest Access Authentication”;
- RFC 2617 “HTTP Authentication: Basic and Digest Access Authentication”.

SDP

- RFC 3264 “An Offer/Answer Model with Session Description Protocol (SDP)”;
- RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”;
- RFC 3555 “MIME Type Registration of RTP Payload Formats”;
- RFC 4566 “SDP: Session Description Protocol”;
- RFC 4568 “Session Description Protocol (SDP) Security Descriptions for Media Streams”.

DTMF

- RFC 2833 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”;
- SIP INFO Method for DTMF Tone Generation;
- Inband DTMF. Обработка тональных сигналов в кодеке G.711 (обнаружение и/или прозрачная передача);
- RTP/RTCP и SRTP/SRTPC
- RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”;
- RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”;
- RFC 3711 “The Secure Real-time Transport Protocol (SRTP)”.

2. Аппаратные и программные требования

Прежде чем продолжить, обратитесь к документу «ФЛАТ Software. Технические требования», в котором приведены подробные требования к среде эксплуатации и информация о поддерживаемых платформах виртуализации продуктов семейства ФЛАТ.



При развертывании систем необходимо предусмотреть резервирование ресурсов VM

Технические требования к платформе ядра SIP SoftSwitch

Параметр	Значение
ОС	Linux x64: Debian 11 (core v.5.10.0-23-amd64) РЕД ОС 8 (core v.6.6.6-1.red80.x86_64) Astra Linux SE 1.7.x (core v.6.1.50-1-generic) / 1.8.x (core v.6.1.90-1-generic)
vCPU	<ul style="list-style-type: none"> 4 vCPU (min 2,1 ГГц) до 5 000 абонентов 8 vCPU (min 2,1 ГГц) от 5 000 до 50 000 абонентов
Резервирование частоты	<ul style="list-style-type: none"> 4 vCPU * 2,1 ГГц = 8,4 ГГц до 5 000 абонентов 8 vCPU * 2,1 ГГц = 16,8 ГГц от 5 000 до 50 000 абонентов
Оперативная память	8 Гб
Дисковое пространство	120 Гб
Бэкап	БД на 1000 абонентов ~ 2 Мб

Технические требования к платформе Медиасервер в режиме записи

Параметр	Значение
ОС	Linux x64: Debian 11 (core v.5.10.0-23-amd64) РЕД ОС 8 (core v.6.6.6-1.red80.x86_64) Astra Linux SE 1.7.x (core v.6.1.50-1-generic) / 1.8.x (core v.6.1.90-1-generic)
vCPU	<ul style="list-style-type: none"> 2 vCPU (min 2,1 ГГц) с поддержкой AVX до 3000 одновременно записываемых абонентов 4 vCPU с поддержкой AVX на 1000 одновременных участников АКС/портов МОН
Резервирование частоты	<ul style="list-style-type: none"> 2 vCPU * 2,1 ГГц = 4,2 ГГц с поддержкой AVX до 3000 одновременно записываемых абонентов 4 vCPU * 2,1 ГГц = 8,4 ГГц с поддержкой AVX на 1000 одновременных участников АКС/портов МОН
Оперативная память	4 Гб в режиме записи, 8 Гб на 1000 портов АКС (ad hoc)
Дисковое пространство	80 Гб

Поддерживаемые решения, протоколы и кодеки:

- Поддерживается 64-битная версия процессоров архитектуры x86.
- G.711a, G.711u, G.722, G.729.
- SDP (Session Description Protocol) – протокол согласования общего набора параметров обмена, в т.ч. методы обмена сообщениями SDP Offer/Answer: Early Offer, Delayed Offer.
- Поддержка протокола SIP.
- Поддерживается предответное состояние линии после прихода входящего звонка, но до ответа на него.
- Используется режим набора номера полным цифровым блоком.
- Поддерживается совместная работа с антивирусным программным обеспечением, в том числе с антивирусным ПО Kaspersky.

Требования к платформам виртуализации

Продукты семейства ФЛАТ протестированы и полностью совместимы со следующими платформами виртуализации:

- Платформа zVirt (Россия)
- Платформа Брест (Россия)
- Платформа VMware
- Платформа KVM
- Платформа Microsoft Hyper-V

Ограничений на работу со SPAN трафиком, реализованную посредством гипервизора, система ФЛАТ SoftSwitch не накладывает.

3. Архитектура решения

3.1. Компоненты системы ФЛАТ SoftSwitch

ФЛАТ SoftSwitch состоит из следующих компонентов (см. [Рисунок 1](#)):

- **SIP SoftSwitch** – ядро системы, обрабатывающее вызовы (сигнализацию SIP) и ДВО (дополнительные виды обслуживания – перевод и переадресация вызова, команда на сбор конференции и т.д.).
- **Медиа сервер** – отвечает за обработку медиа потоков, музыки на удержании, уведомлений голосом, создание конференций, проксирование медиатрафика.

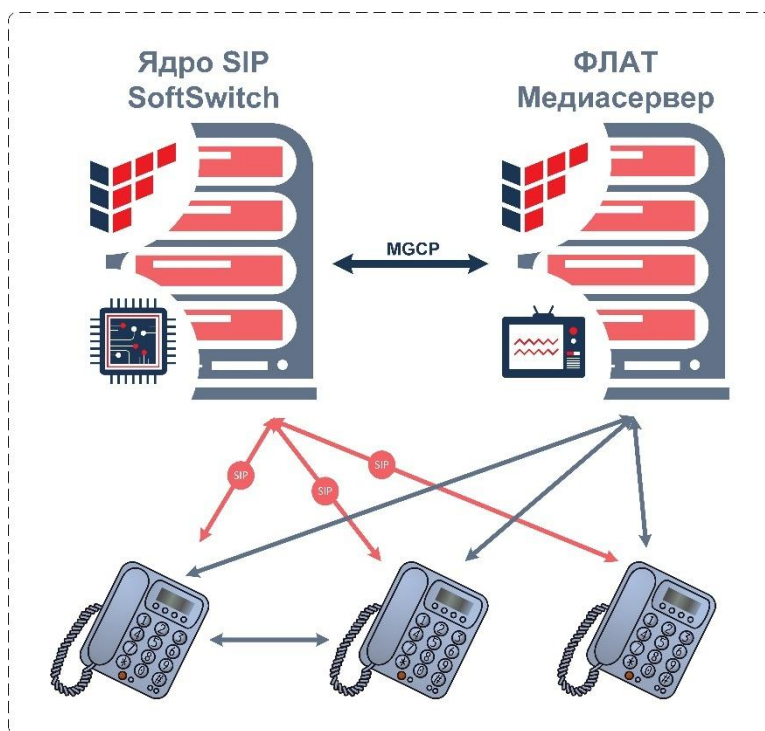


Рисунок 1. Компоненты ФЛАТ SoftSwitch и их взаимодействие

В сценарии установления соединения между двумя пользователями участвует ядро SIP SoftSwitch, выполняя задачу поиска и вызова абонента. Для этого вызывающему пользователю необходимо знать только постоянный номер вызываемого абонента. При этом SIP SoftSwitch не участвует в непосредственной передаче голоса, а лишь предоставляет условия и способы согласования открытия каналов обмена на основе других протоколов, в данном случае – RTP. После установления соединения передача голосового трафика происходит напрямую между абонентами с использованием протокола RTP (Real-Time Transfer Protocol).

В случае необходимости сбора конференции или добавления к разговору нового абонента к указанной схеме подключается Медиа сервер, который берет на себя функцию обработки медиа потока. При необходимости Медиа сервер может выполнять проксирование медиатрафика и пропускать через себя все сессии RTP.

Функционально Медиа сервер представляет собой два отдельных сервиса, отвечающих за разные направления обработки:

- **Mediasrv** – за обработку медиа потока, музыки на удержании, уведомлений голосом и создание конференций;
- **SRClient** – за проксирование RTP и запись SIPREC.

В рамках концепции построения системы ФЛАТ SoftSwitch рассматриваем Медиа сервер как единый модуль, лишь по мере необходимости отмечаем разделение на отдельные сервисы.

Ядро SIP SoftSwitch и модуль Медиа сервер могут быть установлены на одном физическом или виртуальном сервере. Количество модулей Медиа сервера определяется нагрузкой, целесообразностью и топологией сети. Горизонтальная масштабируемость обеспечивается установкой дополнительных Медиа серверов. При этом возможна установка отдельных сервисов **Mediasrv** и **SRClient**.

Система ФЛАТ SoftSwitch всегда работает в режиме B2BUA-сервера, разделяя транзитные вызовы на разные диалоги. Для взаимодействия с каждым отдельным пользователем в рамках сеанса связи используются уникальные идентификаторы.

3.2. Отказоустойчивость

Отказоустойчивость системы ФЛАТ SoftSwitch может быть реализована как резервированием управляющих серверов – **Кластер SIP SoftSwitch**, так и локальным выносом системы (branch office) – **Живучий Офис**.

- **Кластер SIP SoftSwitch** – объединение двух узлов, работающих в режиме Active-Active, устанавливаемых на различные серверы, часто разнесенные территориально (см. [Рисунок 2](#)), с поддержкой уровня L3. Один кластер серверов на систему. В случае выхода из строя одного из серверов, нарушения сетевой связности, отказа системы хранения и базы данных система ФЛАТ SoftSwitch продолжит работу за счет переключения на резервное ядро.

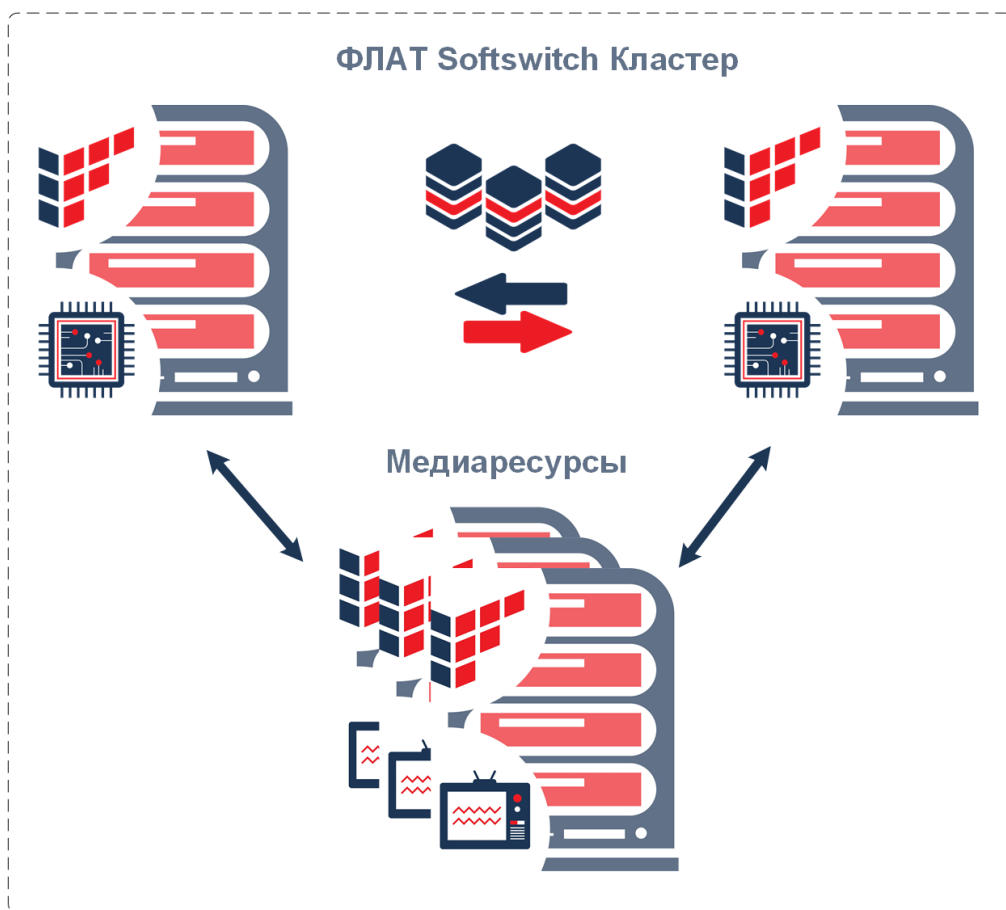


Рисунок 2. Резервирование управляющих серверов – кластер ФЛАТ SoftSwitch

- **Живучий Офис** – специально сконфигурированное ядро SIP SoftSwitch с функционалом локальной выживаемости и дополнительным медиа сервером для работы с RTP локально на площадке (см. [Рисунок 3](#)). В случае разрыва связи с центральным ядром телефоны переключаются на Живучий Офис, который берет на себя обработку правил маршрутизации вызовов, и вынос продолжает работать в автономном режиме. Для автономного режима работы может быть настроена специальная схема маршрутизации вызовов. Живучий Офис управляется через настройки Локации на основном или резервном сервере. В настройках Локации задается аварийный режим работы узла Живучего Офиса.

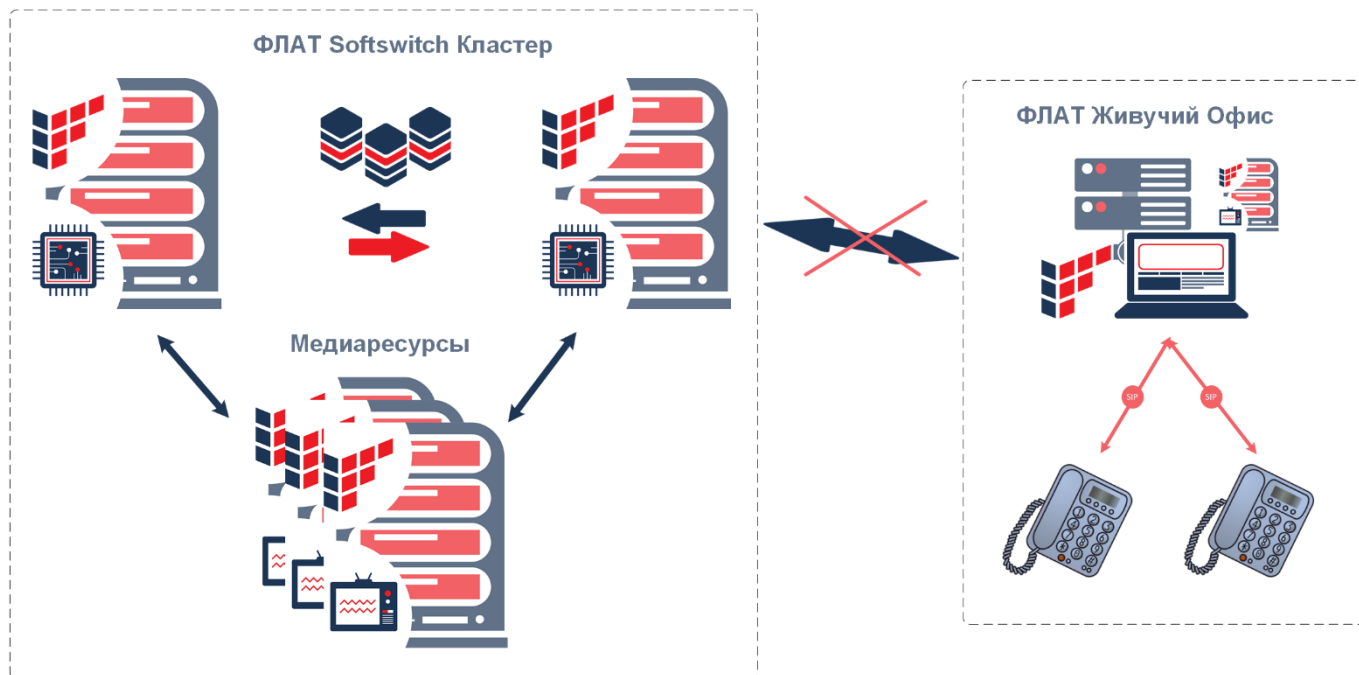


Рисунок 3. Общая схема резервирования ФЛАТ SoftSwitch

3.3. Логическое деление

Система ФЛАТ SoftSwitch поддерживает разграничение корпоративной телефонной сети на отдельно управляемые Зоны, деление на которые может определяться структурой подразделений заказчика, территориальным расположением или разделением процессов маршрутизации.

Деление на Зоны удобно, когда необходимо выделить независимые инстансы – отдельные виртуальные АТС для разных компаний со своим локальным администрированием и своими правилами маршрутизации.

Внутри зон происходит деление на Локации, между которыми распределяется абонентская емкость и к которым привязываются различные устройства (шлюзы для выхода в сеть общего пользования, медиасерверы). С помощью Локаций удобно выделять небольшие структурные подразделения, отделы, офисы.

Локации можно рассматривать и как распределенные удаленные площадки с локальными медиаресурсами, маршрутизацией по признаку источника, управлением медиатрафиком и резервированием ресурсов (Живучий Офис).

Обязательно должна быть хотя бы одна Зона и одна Локация.

Схема деления на Зоны и Локации (см. [Рисунок 4](#)):

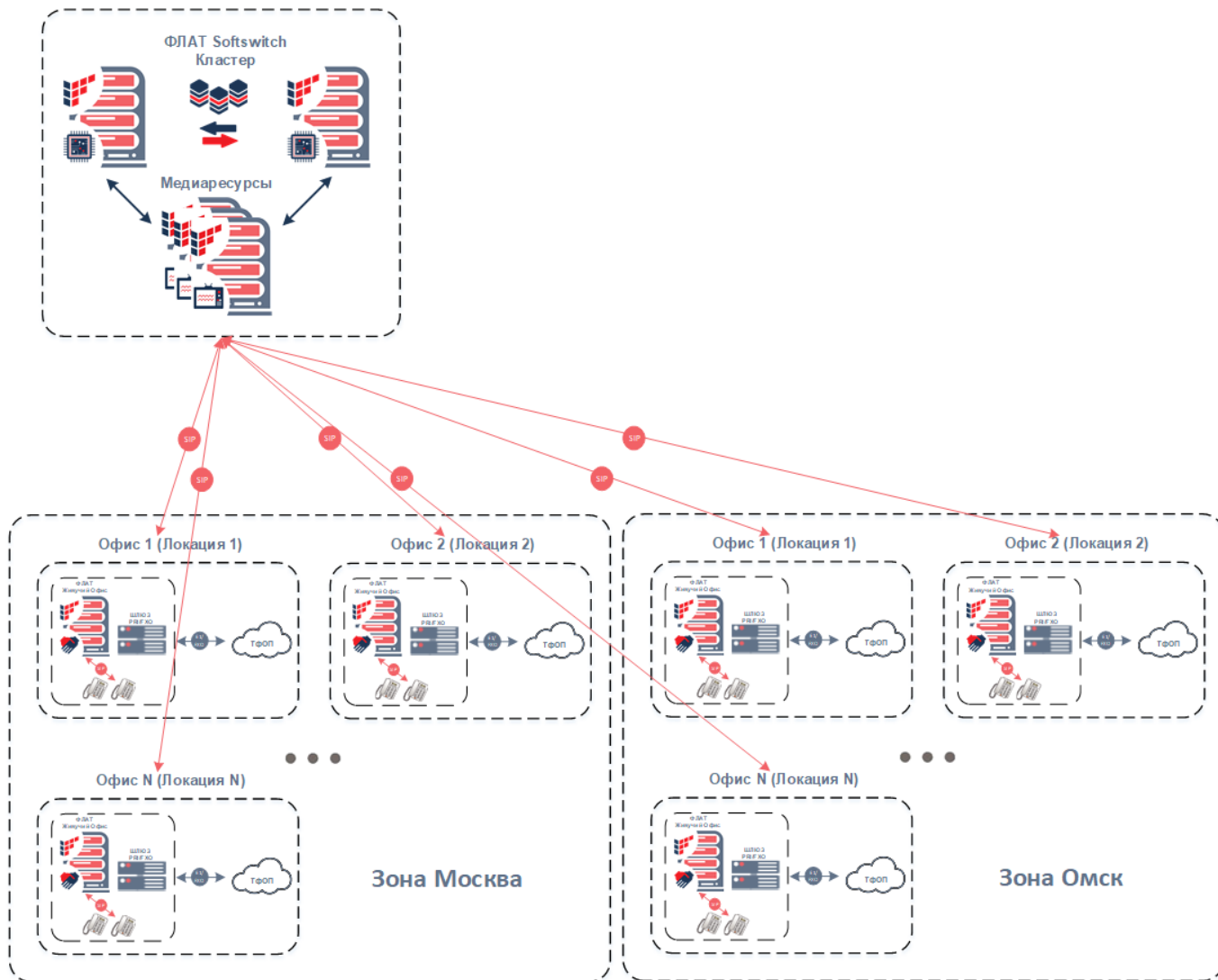

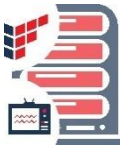






Рисунок 4. Деление на Зоны и Локации

4. Описание сценариев отказоустойчивости

Рассмотрим несколько сценариев отказоустойчивости ФЛАТ SoftSwitch.

В описании использованы следующие обозначения:

Обозначение	Описание
	ФЛАТ SIP SoftSwitch – ядро системы. Основной компонент, отвечает за обработку SIP-сигнализации и дополнительных видов обслуживания (переводы, переадресацию, команды на сбор конференции, и т.д.).
	ФЛАТ Медиа сервер. Основной компонент, отвечает за обработку медиа потока, музыки на удержании, уведомлений голосом, создание конференций. Так же используется в различных сценариях для передачи RTP трафика в систему записи и т.д.
	ФЛАТ Device Manager – модуль управления телефонами. Позволяет автоматизировать процесс администрирования и обслуживания телефонных аппаратов.
	ФЛАТ Запись - модуль записи разговоров. Позволяет организовать запись телефонных переговоров, запись экранов на рабочих местах.
	ФЛАТ Живучий Офис – специально сконфигурированное ядро ФЛАТ SoftSwitch, настроенное для поддержания работоспособности определенной Локации при разрыве связи с центральным ядром.
	ФЛАТ SBC – пограничный контроллер сессий для безопасного функционирования корпоративной сети телефонии на стыке с сетью оператора связи.

4.1. Сценарий 1

Конфигурация ФЛАТ SoftSwitch: площадка Основная, отказоустойчивый вынос на Площадке 2. На каждой площадке расположены SIP-абоненты, обеспечивается свой выход на ТФОП, и активированы отдельные системы записи телефонных переговоров.

Рассматривается сценарий разрыва канала между площадками.

Примечание: В рассматриваемых примерах Host-1, Host-2 – гипервизоры.

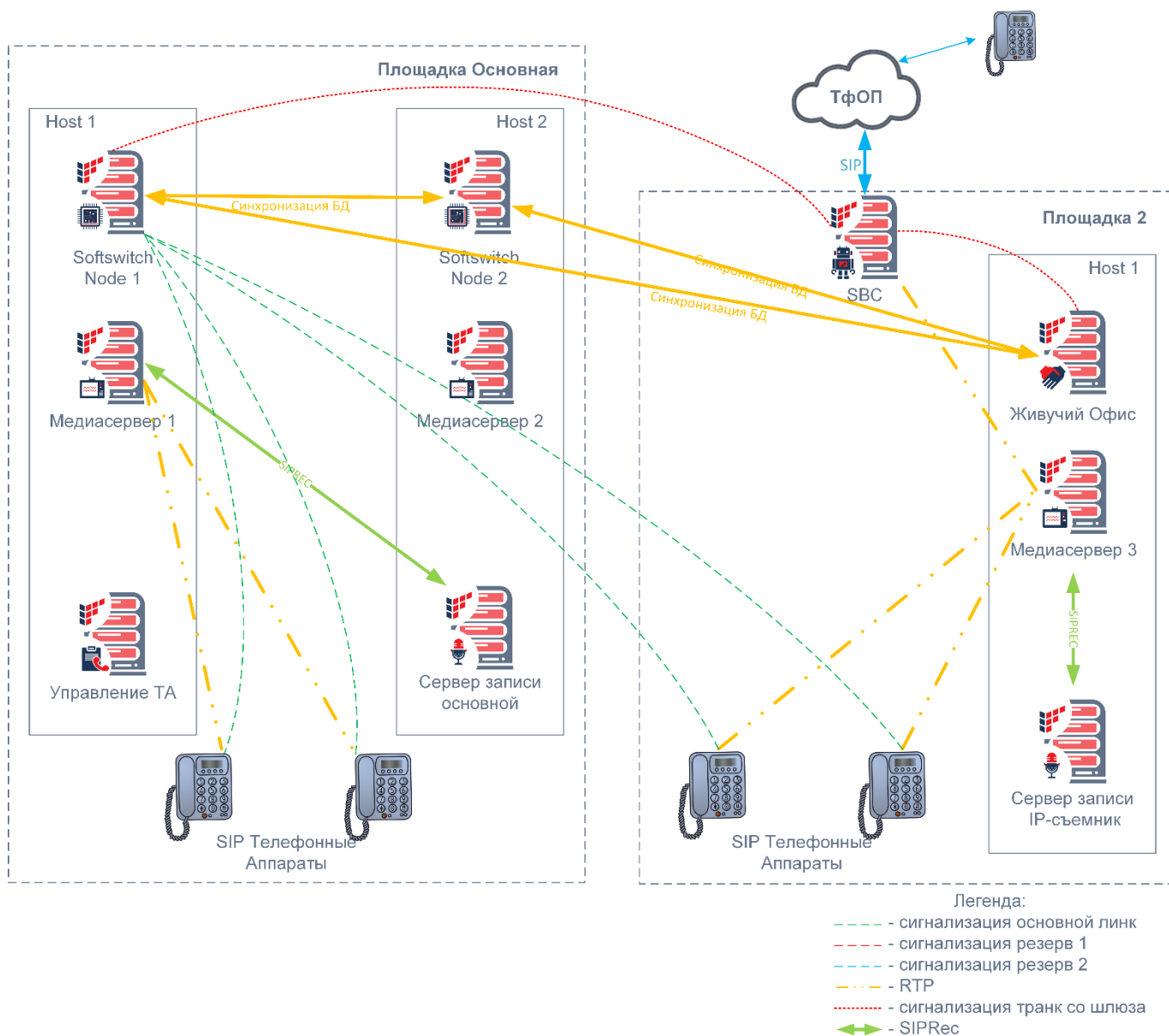


Рисунок 5. Штатный режим работы

Описание механизма: Механизм резервирования на Основной площадке **SoftSwitch** реализован методом дублирования узлов, работающих в режиме Активный-Активный. Между узлами происходит синхронизация данных, хранимых в БД, а также отслеживание состояния каждого узла.

На Площадке 2 установлен резервный узел **Живучий Офис** с функционалом локальной выживаемости и дополнительный медиа сервер для работы с RTP локально на площадке.

Для всех абонентов включена функция записи телефонных переговоров.

В штатном режиме работы все телефонные аппараты на обеих площадках регистрируются на первом узле **Node 1**.

При установлении соединения между абонентами в рамках одной локации RTP трафик проходит через **Медиа сервер**. **Медиа сервер** транслирует RTP потоки каждого абонента в сторону сервера записи (центрального или локального IP съемника).

В случае установления соединения между абонентами разных локаций, RTP трафик каждой стороны проходит через локальные медиа шлюзы.

При недоступности основного узла **Node 1**, телефонные аппараты на Площадках по истечении тайм-аута регистрации перерегистрируются на узел **Node 2** (см. [Рисунок 6](#)). Переключение происходит без разрыва уже

установленных сессий, если не используется принудительное проксирование RTP трафика (в случае использования записи методом SIPREC).



Таймер регистрации настраивается на каждом телефонном аппарате.

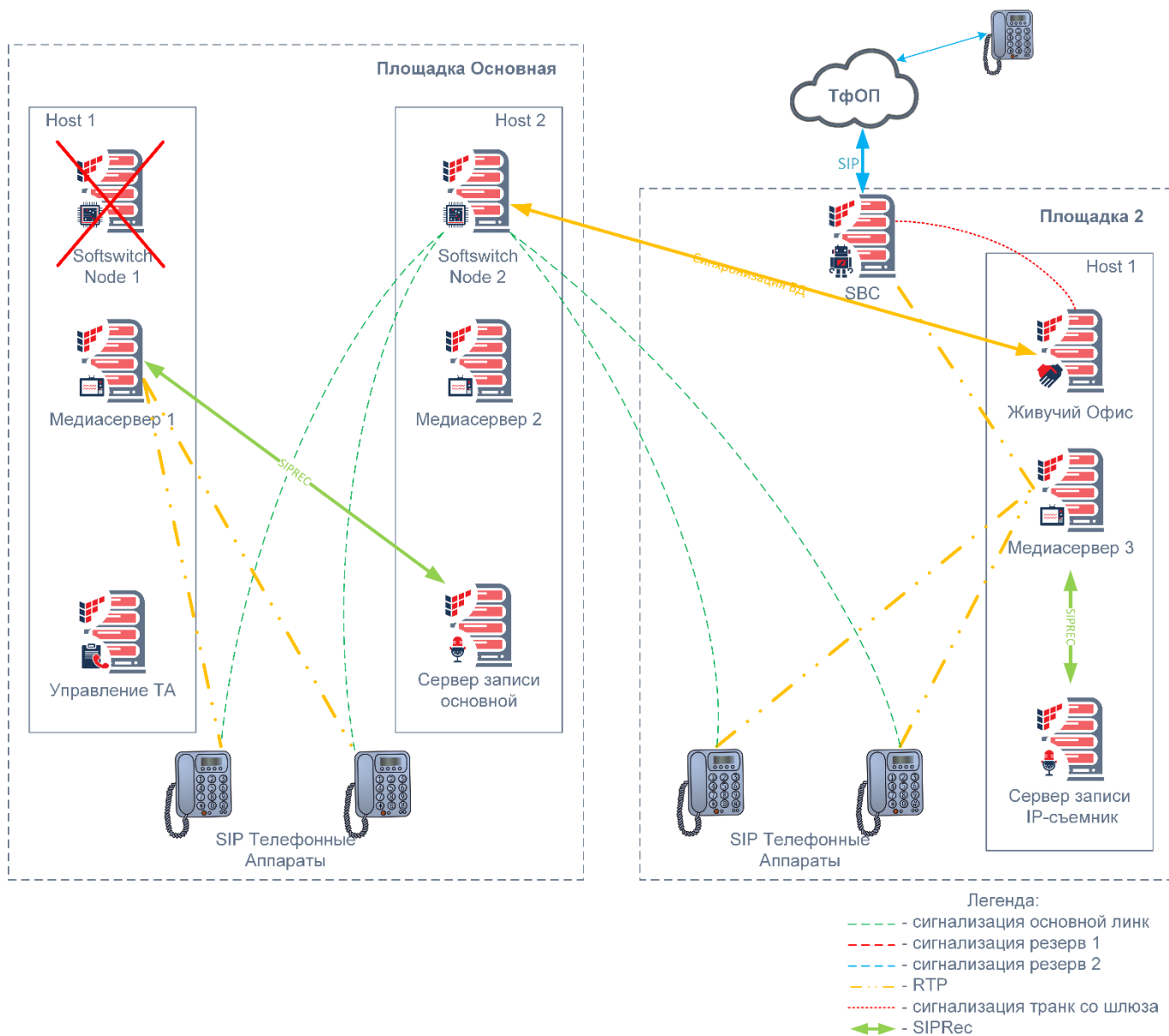


Рисунок 6. Отказ узла SoftSwitch (Node 1)

После восстановления работоспособности первого узла произойдет повторная (обратная) перерегистрация телефонных аппаратов.

При обрыве канала между площадками телефонные аппараты на Площадке 2 по истечении таймаута регистрации перерегистрируются на узел **Живучий Офис** (см. [Рисунок 7](#)).

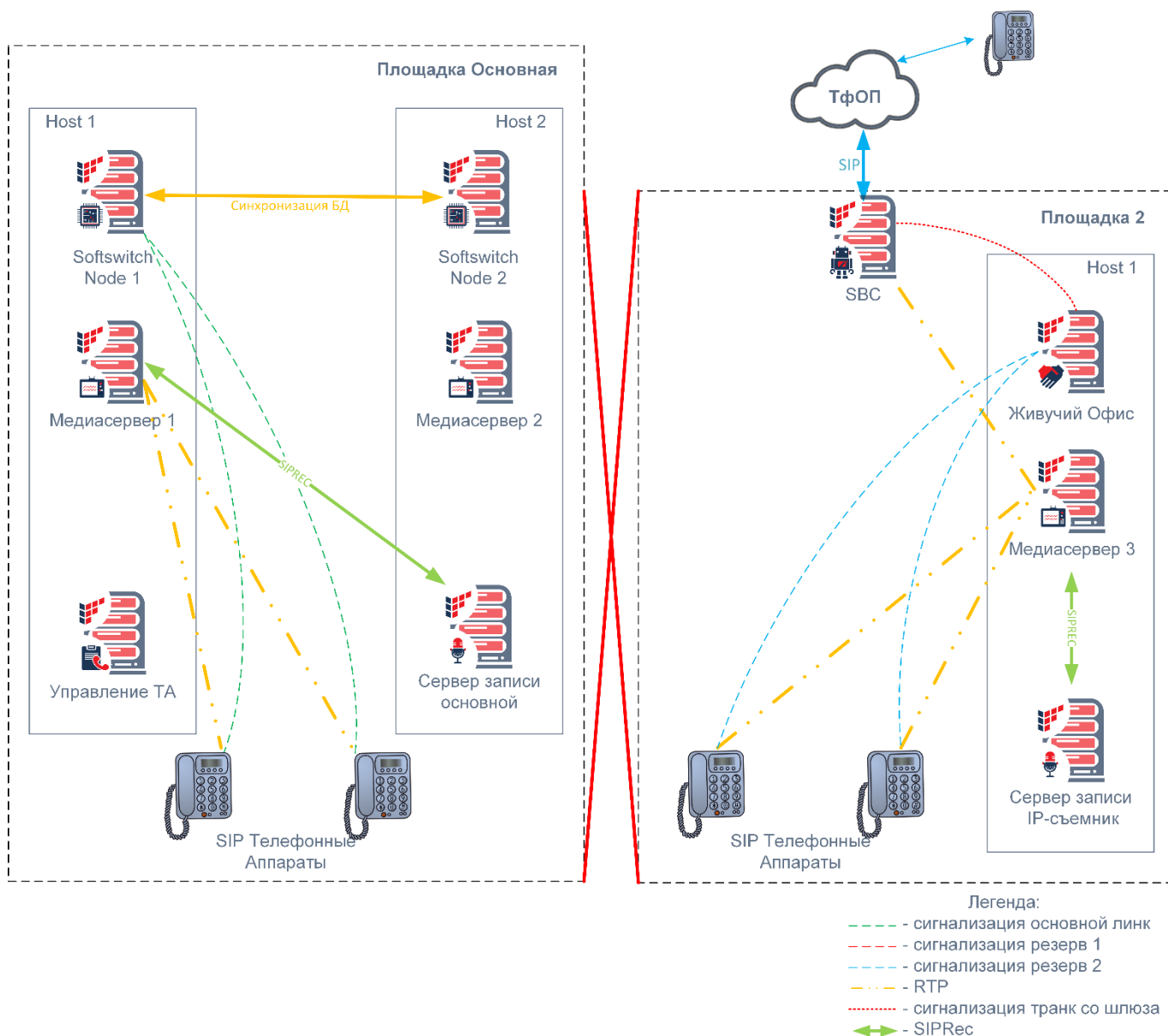


Рисунок 7. Переключение на Живучий Офис

Живучий Офис синхронизирует необходимые параметры абонентов, групп и транков. Дополнительно для него настраиваются маршруты аварийной маршрутизации.

Переключение происходит без разрыва уже установленных разговорных сессий в пределах Площадки 2.

Соединения с основной площадкой разорвутся.

После восстановления канала между площадками, в автоматическом режиме произойдет обратная перерегистрация на основной узел **Node 1**.

4.2. Сценарий 2

Конфигурация ФЛАТ SoftSwitch: Две площадки с соединением по L3. Абоненты расположены на обеих площадках. Выход на ТФОП реализован на обеих площадках. Активирована система записи телефонных переговоров.

Рассматривается сценарий разрыва канала между площадками.

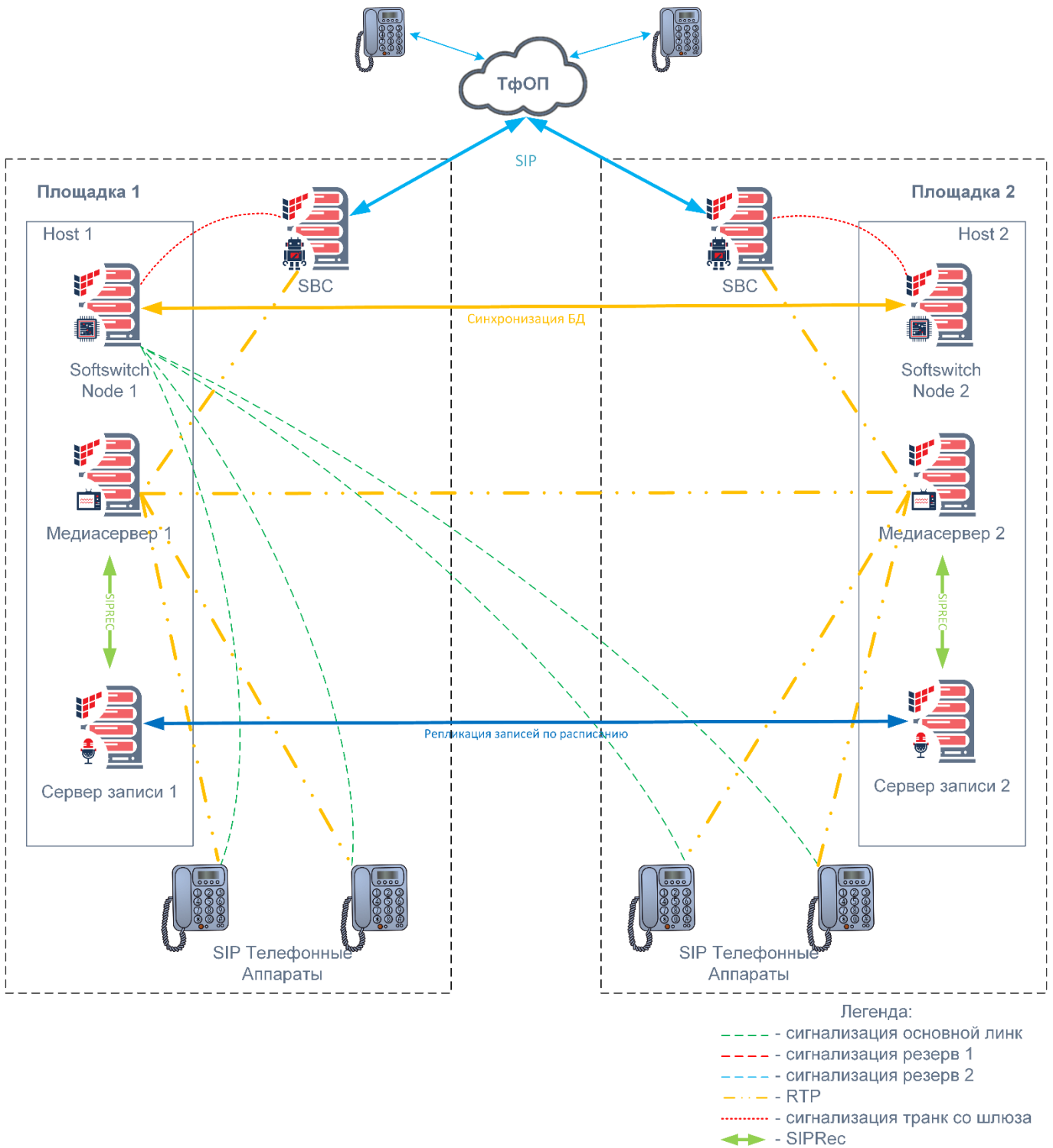


Рисунок 8. Штатный режим работы

В штатном режиме работы все телефонные аппараты на обеих площадках регистрируются на первом узле **SoftSwitch Node 1**.

При установлении соединения между абонентами в рамках одной локации RTP трафик проходит через локальный **Медиа сервер**. **Медиа сервер** транслирует RTP потоки каждого абонента в сторону сервера записи.

В случае установления соединения между абонентами разных локаций, RTP трафик каждой стороны проходит через локальные медиа шлюзы.

При выходе из строя основного узла **Node 1**, телефонные аппараты на Площадках по истечении тайм-аута регистрации перерегистрируются на узел **Node 2** (см. *Рисунок 9*).

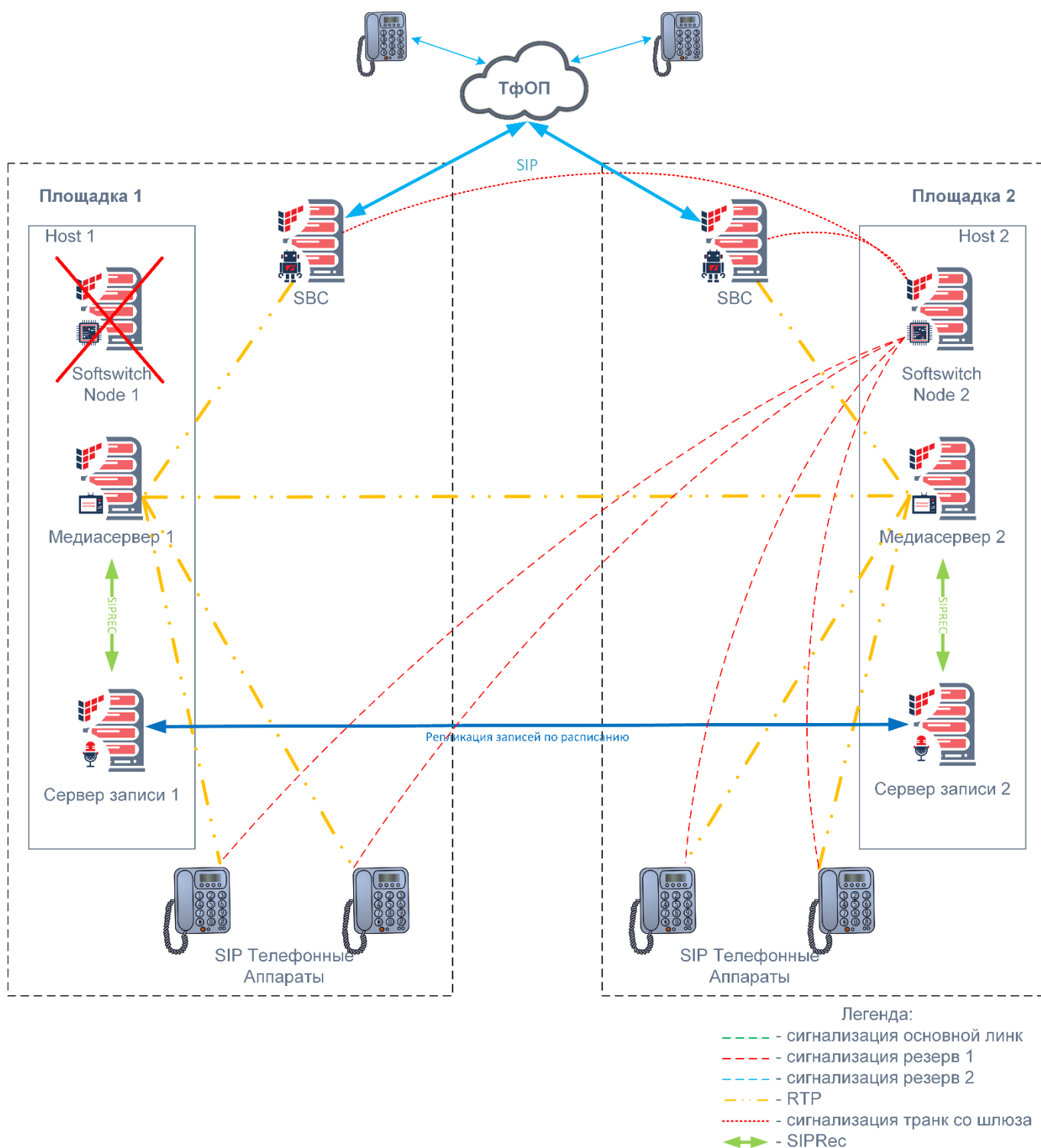


Рисунок 9. Отказ узла SoftSwitch Node 1 на Площадке 1

Переключение происходит без разрыва уже установленных сессий.

После восстановления работоспособности первого узла произойдет повторная (обратная) перерегистрация телефонных аппаратов. Тайм-аут регистрации выставляется в настройках самого телефонного аппарата.

Записи продолжают проксироваться на локальные сервера записи.

При выходе из строя **Медиа сервера 1** разорвутся активные RTP сессии, проходящие через данный **Медиа сервер**. При установке нового соединения RTP пойдет через следующий в цепочке **Медиа сервер**¹ (см. *Рисунок 10*).

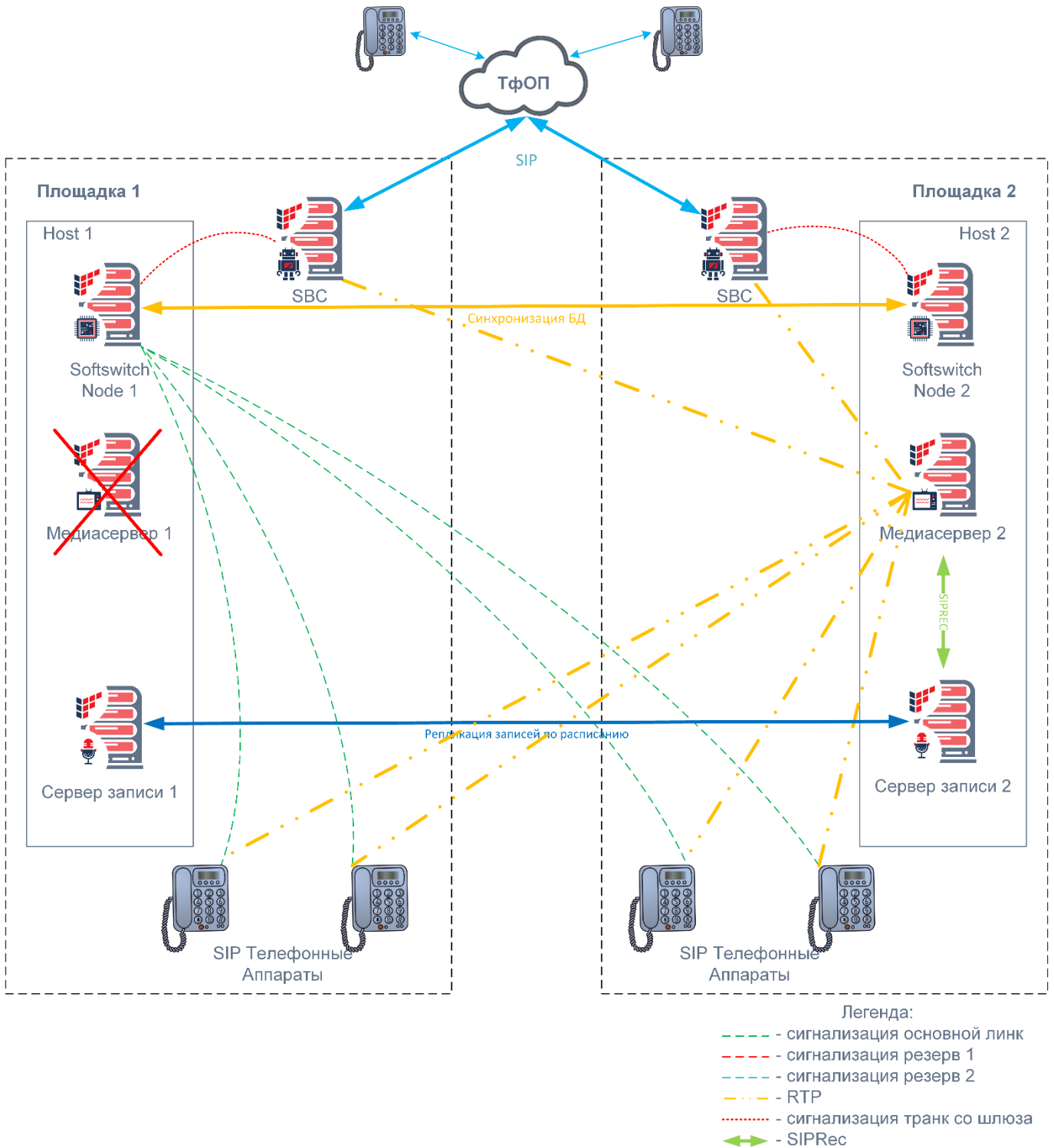


Рисунок 10. Отказ Медиа сервера на Площадке 1

¹ Функционал синхронизации сессий между Медиа серверами находится в стадии разработки

5. Стоимость программного обеспечения

В связи со спецификой лицензирования, стоимость программного обеспечения ФЛАТ рассчитывается индивидуально. Информацию о лицензировании можно получить по электронной почте: info@flat-soft.ru. После обработки запроса, наши сотрудники свяжутся с Вами для консультации и предоставления расчёта в соответствии с техническими характеристиками вашего проекта.

6. Активация лицензий

Система ФЛАТ SoftSwitch лицензируется на временной или постоянной основе только по количеству абонентов и варианту развертывания (дублирование, Живучий Офис). Абонентские лицензии расходуются при регистрации абонентского устройства и высвобождаются при его отключении. Множественная регистрация нескольких абонентских устройств на один номер (до 5 устройств) не требует дополнительной лицензии.

Лицензия предоставляется в цифровом виде, наличие физического носителя не требуется.

Запрос на ввод лицензионного ключа для ядра системы ФЛАТ SoftSwitch (или для каждого узла при организации кластера), а также для отказоустойчивого выноса (Живучего Офиса), выводится на стадии установки системы.

7. Установка на Debian и Astra Linux



При установке компонентов системы ФЛАТ SoftSwitch версий v.4.1 – 4.2 следует учитывать поэтапную замену наименований инсталляционных пакетов, сервисов, каталогов расположения, названий файлов журналов событий (см. [Изменение наименований пакетов](#)).



В приведенных в руководстве примерах конфигурационных файлов указан **условный** IP-адрес хоста установки системы. При необходимости копирования настроек из примеров изменяйте адрес на реальный.

7.1. Предустановочные действия

В данном разделе рассматривается установка ФЛАТ SoftSwitch в объеме, достаточном для запуска WEB-интерфейса системы. Полное описание настроек устанавливаемых подсистем приведено в документе «ФЛАТ SoftSwitch. Руководство администратора» (ссылку на документ см. в разделе [Связанные документы](#)).

Установка выполняется на операционных системах Debian и Astra Linux. В качестве сервера используется виртуальная машина VMWare.

1. С официального сайта производителя ([Debian.org](#), [Astralinux.ru](#)) скачайте актуальную версию ОС (см. [Аппаратные и программные требования](#)). Поддерживаемая архитектура amd64.
2. Создайте виртуальную машину и подключите к ней образ ОС. Назначьте параметры виртуальной машины с учетом планируемой нагрузки (см. [Аппаратные и программные требования](#)). Выполните установку операционной системы.
3. Получите от вендора лицензионный ключ вида:

```
m7it95xd7UYNPMT/3jbybPeL25/0GTKA15RLYx3ZVXa/RGqB7zbpBpt5
```

7.2. Отключение SELinux

Если вы используете SELinux, либо он установлен и включен в системе по умолчанию, при обновлении и установке программных продуктов ФЛАТ рекомендуем его отключить.

Проверьте параметры запуска SELinux при загрузке системы:

```
cat /etc/selinux/config
```

Если параметр **SELINUX** имеет значение enforcing, отключите запуск SELinux при загрузке системы. Для этого в файле **/etc/selinux/config** измените значение параметра **SELINUX**:

```
/etc/selinux/config
```

```
SELINUX=disabled
```

Выполните перезапуск системы:

```
reboot
```

Проверьте текущее состояние SELinux командой:

```
sestatus
```

7.3. Настройки сети, даты и времени

После установки ОС выполните настройки сети. MAC-адресам VM назначьте IP-адреса согласно плану статической адресации. При использовании DHCP-сервера зарезервируйте используемые IP-адреса за конкретными VM.

Для просмотра состояния сетевых интерфейсов используйте команду `ip addr`:

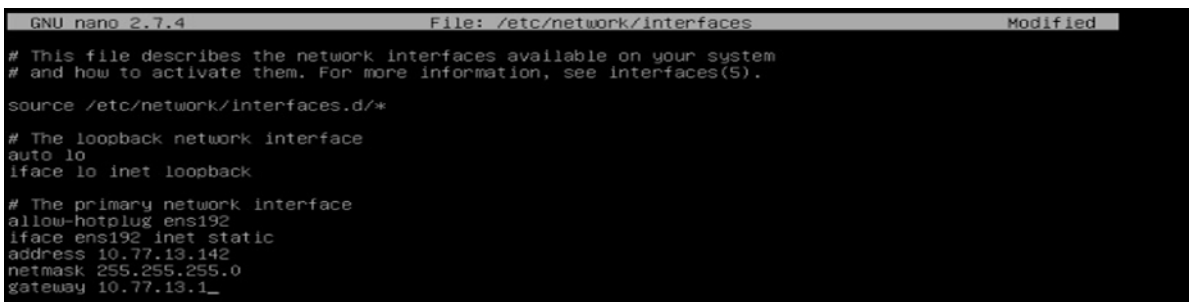
```
flat@flat-ss-main:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:be:fb:7b brd ff:ff:ff:ff:ff:ff
    inet 10.77.13.142/24 brd 10.77.13.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:febe:fb7b/64 scope link
        valid_lft forever preferred_lft forever
flat@flat-ss-main:~$ _
```

Рисунок 11. Состояние сетевых интерфейсов

Как видно, интерфейс **ens192** включился и получил адрес в автоматическом режиме DHCP. Перенастройте интерфейс на статическую IP-адресацию, отредактировав файл `/etc/network/interfaces`.

1. Перейдите в режим суперпользователя командой `su` - и введите пароль пользователя **root**.
2. Откройте на редактирование `nano /etc/network/interfaces` и укажите данные вашей сети, например:

```
allow-hotplug ens192
iface ens192 inet static
address 10.77.13.142
netmask 255.255.255.0
gateway 10.77.13.1
```



```
GNU nano 2.7.4 File: /etc/network/interfaces Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug ens192
iface ens192 inet static
address 10.77.13.142
netmask 255.255.255.0
gateway 10.77.13.1_
```

Рисунок 12. Изменение `/etc/network/interfaces`

3. Сохраните изменения сочетанием клавиш `Ctrl+X -> Y -> Enter`.
4. Перезагрузите сетевой интерфейс командой `service networking restart`, запустите сетевой интерфейс командой `ifup ens192`.
5. Используя программу PuTTY или любой другой SSH-клиент, подключитесь к серверу по SSH:

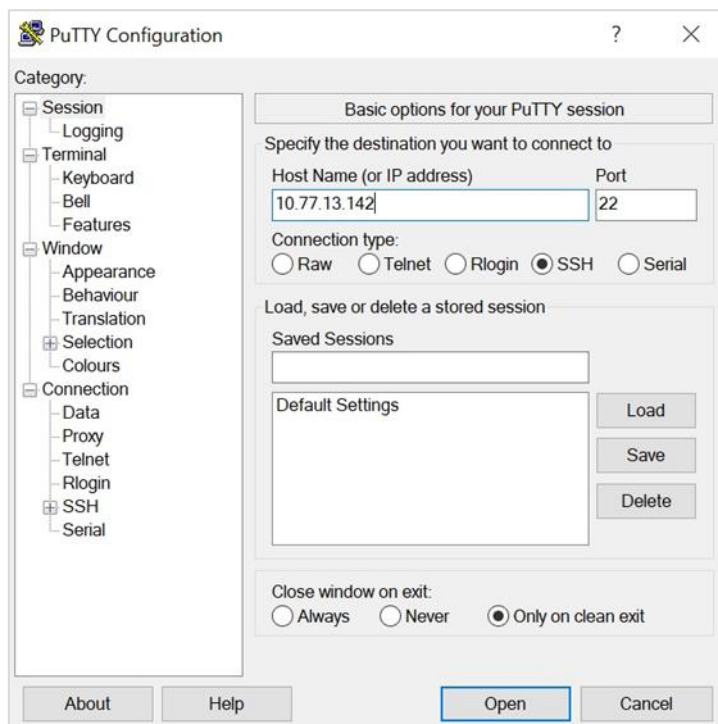


Рисунок 13. Настройки подключения

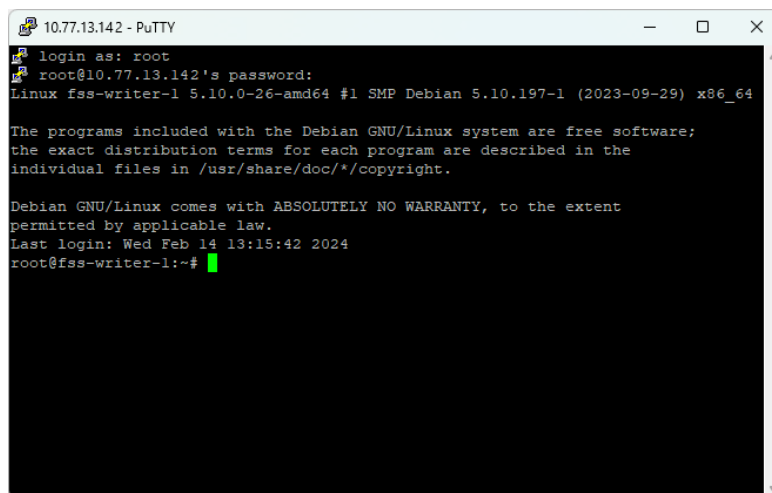


Рисунок 14. Подключение по SSH

Проверьте дату и время командой **timedatectl**. При необходимости выставьте корректные значения.

6. Выставьте дату и время командой **date 08211545**

Где 08 — месяц, 21 — число, 15 — час, 45 — минуты. Формат команды имеет вид **date MMDDhhmm**.

7. Выставьте часовой пояс командой **timedatectl set-timezone Europe/Moscow**

7.4. Доступ к репозиторию

Для доступа к репозиторию программных продуктов семейства ФЛАТ авторизуйтесь на сайте <https://partnerportal.flat-soft.ru> под учетной записью, полученной от вендора. После авторизации выберите пункт меню **Руководства к продуктам ФЛАТ** (см. *Рисунок 15*) и раздел **Репозиторий** (см. *Рисунок 16*):

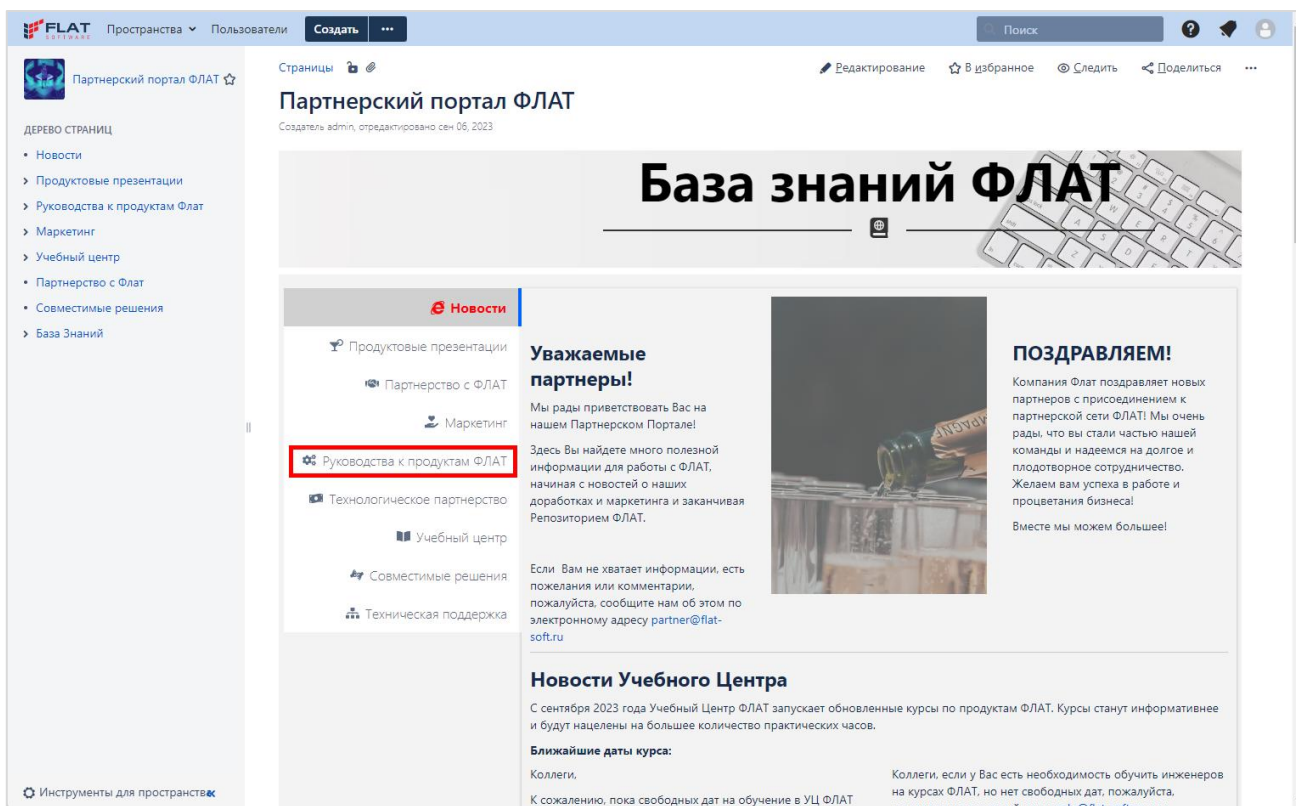


Рисунок 15. Партнерский портал ФЛАТ

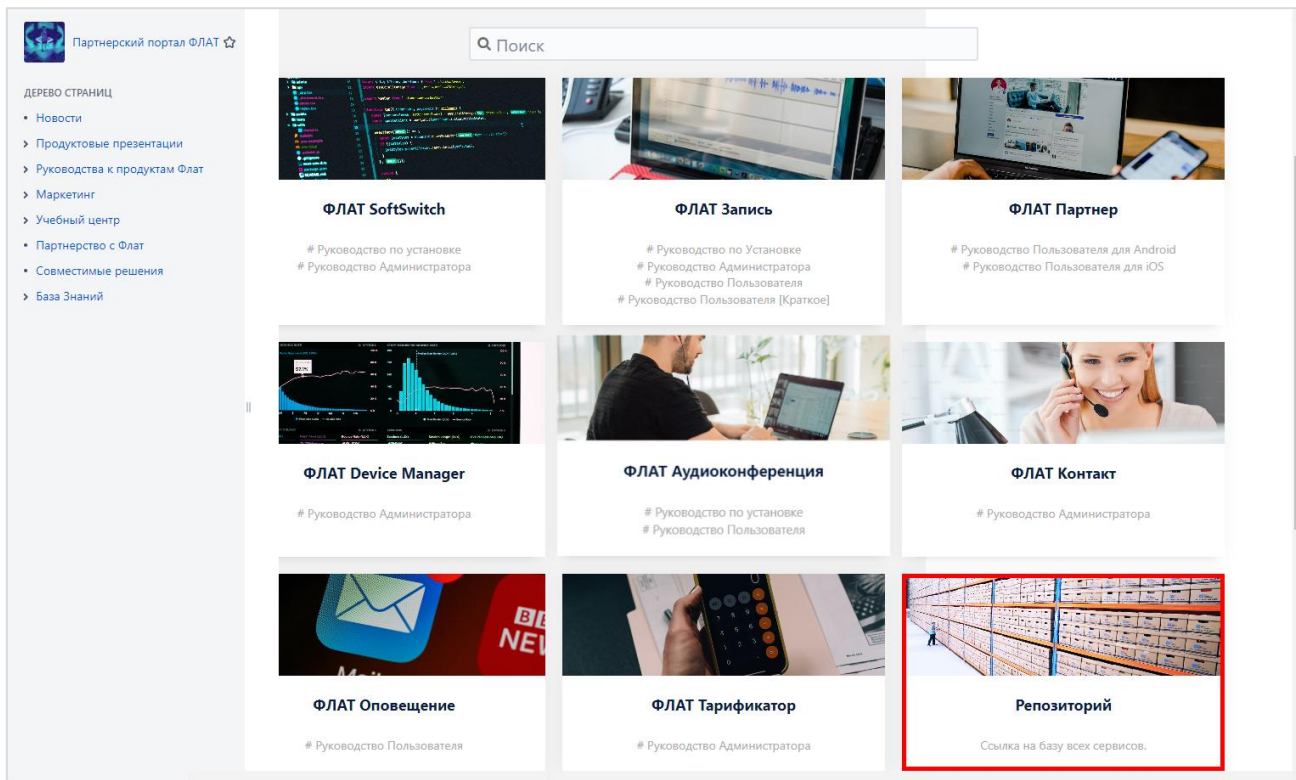


Рисунок 16. Раздел «Репозиторий»

В открывшемся окне репозитория программных продуктов ФЛАТ повторите авторизацию.

Для этого нажмите кнопку  в правом верхнем углу и снова введите полученные логин и пароль.

Далее нажмите Browse, в окне справа раскройте раздел **flat-local-repository/flat-softswitch-repository**, выберите и скачайте репозиторий нужной версии (см. [Рисунок 17](#)):

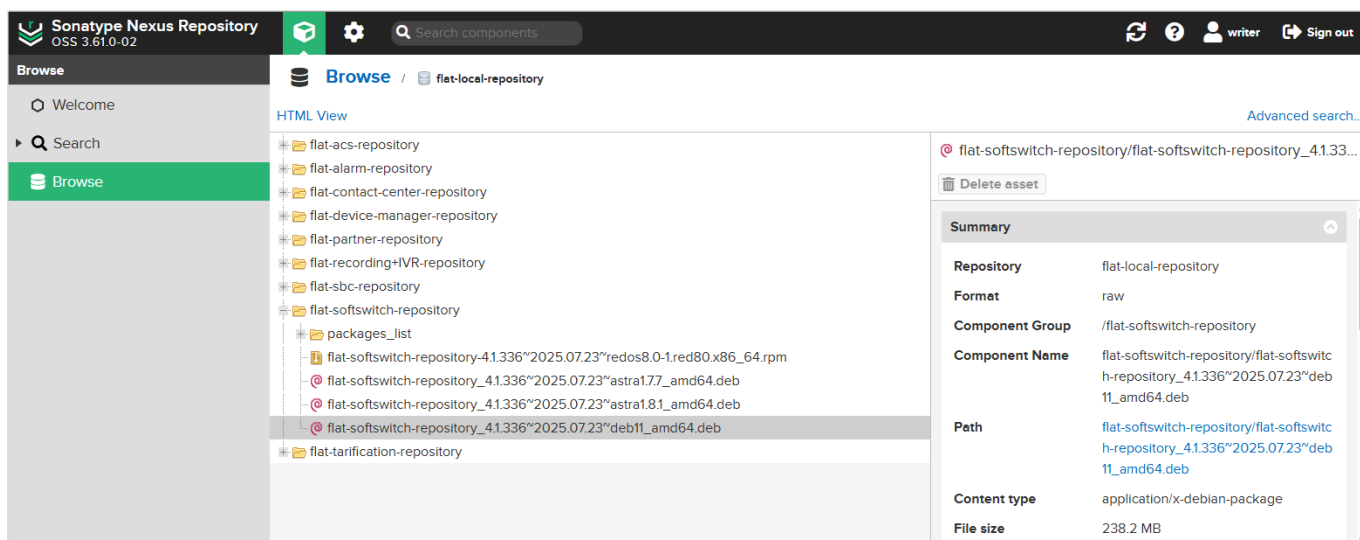


Рисунок 17. Репозиторий Nexus

После загрузки проверьте целостность полученного пакета, чтобы убедиться, что загруженный файл не был подделан или поврежден. Проверку выполните путем сравнения контрольных сумм (sha1 или md5) с эталонными значениями, указанными на странице загрузки (см. [Рисунок 18](#)):

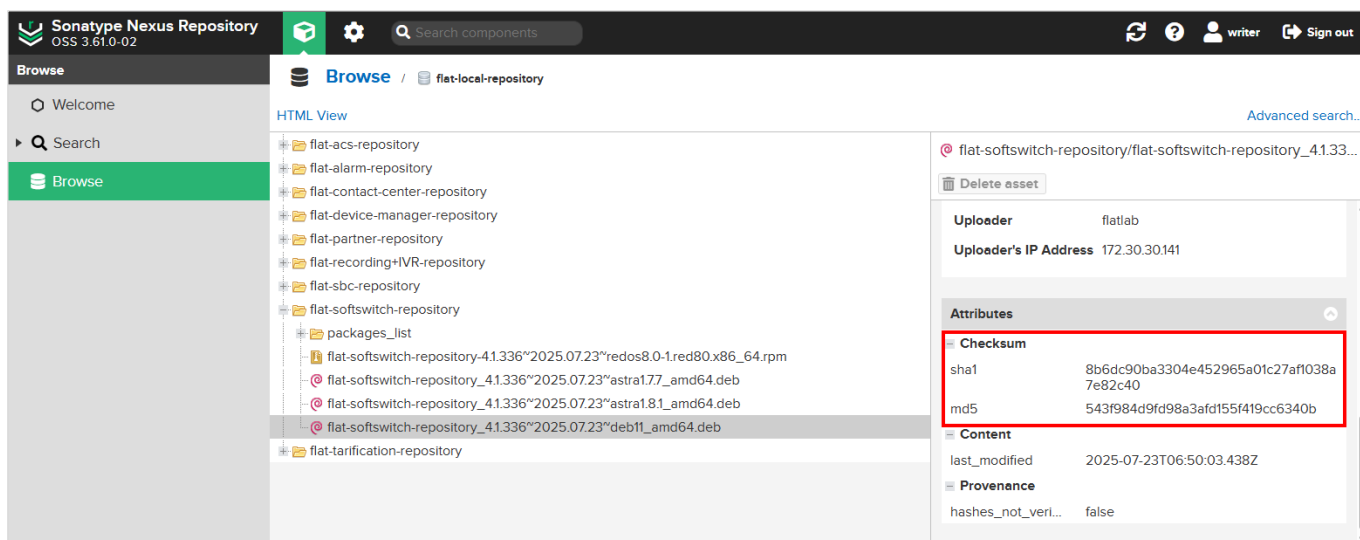


Рисунок 18. Контрольные суммы

7.5. Установка системы ФЛАТ SoftSwitch

Скачайте репозиторий ФЛАТ SoftSwitch, в состав которого входят следующие пакеты:

Описание	Название пакета	Имя пакета	Компонент
Ядро SIP SoftSwitch	fss-server	fss-server_<версия пакета>_amd64.deb	backend
Сервис Mediasrv	fss-mediasrv	fss-mediasrv_<версия пакета>_amd64.deb	backend
Сервис SRClient	fss-srclient	fss-srclient_<версия пакета>_amd64.deb	backend

Описание	Название пакета	Имя пакета	Компонент
Сервис FlatFileManager	flat-file	flat-file_<версия пакета>_amd64.deb	backend
Библиотеки libssl и libcrypto	libssl1.0.2	libssl1.0.2_1.0.2u-1~deb9u7_amd64.deb	library
Бэкенд WEB-интерфейса ФЛАТ SoftSwitch	flatsoftswitchbackend	flatsoftswitchbackend_<версия пакета>_amd64.deb	backend
Фронтенд WEB-интерфейса ФЛАТ SoftSwitch	fss-frontend	fss-frontend_<версия пакета>_amd64.deb	frontend
Бэкенд WEB-интерфейса ЛК пользователя	lc-backend	lc-backend_<версия пакета>_amd64.deb	backend
Фронтенд WEB-интерфейса ЛК пользователя	lc-frontend	lc-frontend_<версия пакета>_amd64.deb	frontend

Где <версия пакета> – номер версии пакета.



Текущая версия руководства основана на репозитории:
flat-softswitch-repository_4.1.481~2025.08.13~deb11_amd64.deb

Перенесите репозиторий на подготовленный сервер, используя клиент SCP, или любым другим способом.

1. Отправьте запрос на получение лицензии по MAC адресу сетевой карты. MAC адрес можно узнать средствами гипервизора или используя команду Linux:

```
ip a | grep ether
```

2. Подготовьте полученный от вендора лицензионный ключ вида:

```
m7it95xd7UYNPMT/3jbybPeL25/0GTKA15RLYx3ZVXa/RGqB7zbpBpt5
```

3. Перейдите в каталог с репозиторием (в примере **home**) и повысьте привилегии до суперпользователя:

```
cd /home/*  
su -
```

4. Закомментируйте существующие репозитории в `/etc/apt/sources.list` и выполните команду установки:

```
apt install ./flat-softswitch-repository_<версия репозитория>_amd64.deb
```

5. Убедитесь в наличии нужных для установки пакетов (команда одной строкой):

```
apt list | grep -e nodejs -e redis -e nginx -e fss-server -e fss-mediasrv -e fss-srclient -e flatsoftswitchbackend -e fss-frontend -e lc-backend -e lc-frontend -e flat-file
```

6. Для Astra Linux версии 1.8.X установите следующие библиотеки:

```
apt install /opt/flat/local/repo/fss-local-repo/libxml2_2.9.10_<версия_пакета>_amd64.deb
```

Где <версия пакета> – номер версии пакета.

7. Установите следующие пакеты:

```
apt install redis  
apt install nginx  
apt install fss-server  
apt install fss-mediasrv  
apt install fss-srclient
```

В ходе установки в ответ на запрос введите полученный ключ активации.

8. Проверьте успешность запуска сервисов:

```
systemctl status redis.service
systemctl status nginx.service
systemctl status flat_ss.service
systemctl status fss-mediasrv.service
systemctl status fss-srclient.service
```

Статус каждого сервиса должен быть: **active (running)**.

7.5.1. Установка сервиса FlatFileManager

1. Установите сервис:

```
apt install flat-file
```

2. В конфигурационном файле `/opt/flat/flat-file/config.yml` измените значение параметров:

http: host – укажите FQDN или IP-адрес хоста установки ядра ФЛАТ SoftSwitch, если значение не будет присвоено автоматически.

fss-backup: enable – укажите значение **true**.

fss-logs: enable – укажите значение **true**.

Пример конфигурационного файла:

```
/opt/flat/flat-file/config.yml
```

```
force: false

# Настройка сети
http:

  # Адрес
  # localhost - при настройке nginx (http/https или домен)
  # ip адрес - доступ по IP адресу, настройка nginx не требуется
  host: 10.77.13.34

  # Порт
  # Укажите любой свободный порт или оставьте по умолчанию
  # При настройке nginx укажите этот порт в проху настройках
  port: 8053

# Настройка логирования
log:

  # Архивация файлов -> max_backups.
  # Каждый файл архивируется отдельно
  compress: false

  # production или development
  debug: development

  # Путь к папке с логами
  # Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
  dir: /var/log/flat/flat-file

  # Максимальное время хранения
  max_age: 28

  # Максимальное количество файлов
  max_backups: 10

  # Максимальный размер файла
```

```
max_size: 20
```

```
services:
```

```
contact-scripts:
```

```
# Укажите true для включения
```

```
enable: false
```

```
# Разрешения
```

```
rules:
```

```
# Разрешение создавать каталоги
```

```
create_dir: true
```

```
# Разрешение создавать файлы
```

```
create_file: true
```

```
# Разрешение скачивать
```

```
download: true
```

```
# Разрешение удалять каталоги
```

```
remove_dir: true
```

```
# Разрешение удалять файлы
```

```
remove_file: true
```

```
# Путь хранения скриптов для ФЛАТ Контакт
```

```
workdir: /opt/flat/scripts
```

```
# Резервное копирование для ФЛАТ SoftSwitch
```

```
fss-backup:
```

```
# Укажите true для включения
```

```
enable: true
```

```
# Разрешения
```

```
rules:
```

```
# Разрешение создавать каталоги
```

```
create_dir: true
```

```
# Разрешение создавать файлы
```

```
create_file: true
```

```
# Разрешение скачивать
```

```
download: true
```

```
# Разрешение удалять каталоги
```

```
remove_dir: true
```

```
# Разрешение удалять файлы
```

```
remove_file: true
```

```
# Путь хранения резервных копий ФЛАТ SoftSwitch
```

```
workdir: /opt/flat/switchserver/backup
```

```
# Логирование для ФЛАТ SoftSwitch
```

```
fss-logs:
```

```
# Укажите true для включения
```

```
enable: true
```

```
# Разрешения
```

```
rules:
```

```
# Разрешение создавать каталоги
```

```
create_dir: true
```

```
# Разрешение создавать файлы
```

```
create_file: true
```

```
# Разрешение скачивать
```

```
download: true
```

```
# Разрешение удалять каталоги
```

```
remove_dir: true
```

```
# Разрешение удалять файлы
```

```
remove_file: true
```

```
# Путь хранения логов для ФЛАТ SoftSwitch
```

```
workdir: /var/log/switchserver
```

```
# НЕ РЕДАКТИРОВАТЬ. Версия конфига.
```

```
version: 4
```

После изменения конфигурационных файлов перезапустите сервис:

```
service flat-file restart
```

Проверьте успешность запуска сервиса:

```
systemctl status flat-file.service
```

Статус сервиса должен быть: **active (running)**.

7.5.2. Установка фронтенда и бэкенда SoftSwitch, ЛК пользователя

7.5.2.1. Установка бэкенда ФЛАТ SoftSwitch

1. Установите модуль:

```
apt install flatswitchbackend
```

2. В конфигурационном файле `/usr/lib/flatSoftSwitchBackend/config.yml` измените значение параметров:

soft_switch: url – укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch.

db: dsn – в строке параметра укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch, например:

```
db:
  dsn: rapid:QwSDv@tcp(10.77.13.34:3306)/rapidcall?charset=utf8mb4&parseTime=True&loc=Local
```

3. При необходимости скрыть в конфигурационном файле IP-адрес подключения, порт взаимодействия и пароль доступа к БД зашифруйте указанное на предыдущем шаге значение параметра:

db: dsn – присвойте параметру зашифрованное значение строки, в которой укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch. Перейдите в каталог с сервисом и выполните команду шифрования одной строкой:

```
cd /usr/lib/flatSoftSwitchBackend/
./flatsoftswitchbackend_<версия_сервиса> encrypt --
text='rapid:QwSDv@tcp(10.77.13.34:3306)/rapidcall?charset=utf8mb4&parseTime=True&loc=Local'
```

Где `<версия_сервиса>` – номер версии сервиса.

4. При необходимости скрыть в конфигурационном файле назначенный при установке ключ шифрования access-токена зашифруйте значение параметра:

auth: key – присвойте параметру зашифрованное значение этого же параметра, сформированное при установке системы. Перейдите в каталог с сервисом и выполните команду шифрования:

```
cd /usr/lib/flatSoftSwitchBackend/
./flatsoftswitchbackend_<версия_сервиса> encrypt --text='jNsywRxzywlkXTICaarqZlucCjzdvPngeSQCAvCcl'
```

Где в строке команды:

версия_сервиса – номер версии сервиса.

jNsywRxzywlkXTICaarqZlucCjzdvPngeSQCAvCcl – назначенный при установке ключ шифрования access-токена.

В результате выполнения команды шифрования будет получено значение, которое необходимо присвоить параметру **key**: `e519925533aa70b2ec1fff24f19854729eb3e319972aa43ee0901982741e0fe5be8c365934bf9ad2`.

Пример конфигурационного файла с уже зашифрованными параметрами:

```
/usr/lib/flatSoftSwitchBackend/config.yml
# Настройки аутентификации
auth:
  # Время жизни access токена в минутах. По умолчанию 15 минут.
```

```
# Для SSO время жизни токена согласно настройкам IDP
access_token_ttl: 30

# Ключ шифрования access токена.
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
# ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
key: e519925533aa70b2ec1fff24f19854729eb3e319972aa43ee0901982741e0fe5be8c365934bf9ad2

# Настройки аутентификации через Active Directory.
ldap:

    # Адрес AD
    # ldap://example.com:389
    # ldaps://example.com:636
    addr: ldap://10.77.13.11:389

    # BaseDN пользователей
    # Если включена синхронизация через LDAPsynchronizer, рекомендуется скопировать
    # base_dn из config.json.
    base_dn: OU=OrganizationalUnit,DC=example,DC=com

    # Фильтрация пользователей.
    # Если нужно разрешить доступ только пользователям из определенной группы или
    # по другому признаку.
    # Оставьте пустым, если хотите разрешить доступ всем пользователям из BaseDN.
    base_filter: (objectClass=Person)

    # Домен AD.
    # Требуется для авторизации пользователей - login_attr + @ + example.com
    domain: example.com

    # Укажите true для включения
    enabled: false

    # Из какого параметра извлекать Логин. Принимает одно значение.
    # Если включена синхронизация через LDAPsynchronizer, рекомендуется скопировать
    # data.login из config.json.
    # Обычно sAMAccountName или cn
    login_attr: sAMAccountName

# Время жизни refresh токена в минутах. По умолчанию 540 минут - 8 часов.
refresh_token_ttl: 540

# Настройки SSO
sso:

    # Настройки OIDC
    oidc:

        # ID клиента
        client_id:

        # Секретный ключ
        # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
        # ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
        client_secret:

        # Укажите адрес для извлечения конфигурации провайдера
        # Отправится запрос по адресу config_url + /.well-known/openid-configuration
        config_url: http://10.77.13.11/oauth2/token

        # Укажите true для включения
        enabled: false
```

```

# Из какого параметра извлекать Логин
# По умолчанию sub
login_attr: sub

# Адрес данного сервиса.
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
root_url: https://10.77.13.11:443

# Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
# Принимает массив (несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:
  - http://10.77.13.11:3000

# Настройки SAML
saml:

# Самоподписанный сертификат
# openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
# -days 365 -nodes -subj "/CN=myservice.example.com"
cert_file:

# Укажите true для включения
enabled: false

# Самоподписанный ключ
# openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
# -days 365 -nodes -subj "/CN=myservice.example.com"
key_file:

# Из какого параметра извлекать Логин
# По умолчанию http://wso2.org/claims/username
login_attr: http://wso2.org/claims/username

# Если файл xml расположен на сервере, укажите полный путь к нему
# У текущего пользователя должны быть права на чтение
meta_data_path: /etc/metadata.xml

# Если xml расположен на сервере IDP, укажите его адрес
# https://example.com:8443/realms/master/protocol/saml/descriptor
meta_data_url:

# Адрес данного сервиса.
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
root_url: https://10.77.13.11:443

# Адреса админ сервисов (frontend), которым разрешена OIDC аутентификация
# Принимает массив (несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:
  - http://10.77.13.11:3000

# Настройки БД.
db:

# Настройка подключения к MariaDB.
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
# ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
dsn: fd36914520c259bfc62cc00fddaf6d19cee5a346fe76ff7b93d454d3387d52b2edf6486814b9b0d5

# Максимальное количество неактивных подключений к базе данных
max_idle_conn: 10

```

```
# Максимальное количество открытых подключений к базе данных
max_open_conn: 100

# Настройки Device Manager
device_manager:
  # Укажите true для включения
  enabled: false

  # Логин
  # Нужно создать пользователя на DM с логином API
  login: API

  # Пароль
  # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
  # ./flatsoftswitchbackend_1.0.0 encrypt --text=...
  password:

  # Адрес DM
  url: https://10.77.13.20

# Настройки файлового менеджера FFM
ffm:

  # Установите FFM на сервере SoftSwitch
  # Добавьте сервис fss-backup в config.yml
  # В настройках укажите папку с бэкапами софт-свитча
  # (/opt/flat/fss-server/backup) и перезапустите сервис
  # Параметр принимает адрес FFM
  fss-backup: http://localhost:8053

  # Установите FFM на сервере SoftSwitch
  # Добавьте сервис fss-logs в config.yml
  # В настройках укажите папку с логами софт-свитча
  # (/var/log/fss-server) и перезапустите сервис
  # Параметр принимает адрес FFM
  fss-logs: http://localhost:8053

# НЕ РЕДАКТИРОВАТЬ. Всегда должен быть false.
force: false

# Настройки FPS
fps:
  # Укажите true для включения
  enabled: false
  # Адрес
  url: 10.77.13.15:5081

# Настройка сети
http:

  # Адрес
  # localhost - при настройке nginx(http/https или домен)
  # ip адрес - доступ по IP адресу, настройка nginx не требуется
  host: localhost

  # Порт
  # Укажите любой свободный порт
  # При настройке nginx укажите этот порт в проху настройках
  port: 8051

# Настройка логирования
log:
```

```
# Архивация файлов -> max_backups.
# Каждый файл архивируется отдельно
compress: true

# production или development
debug: production

# Путь к папке с логами
# Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
folder: /var/log/flatSoftSwitchBackend

# Максимальное время хранения
max_age: 28

# Максимальное количество файлов
max_backups: 4

# Максимальный размер файла
max_size: 10

# Настройка подключения к REDIS
redis:

  # Адреса
  address:
    - localhost:6379

  # Включить кластер
  cluster_mode: false

  # Номер БД
  db: 0

  # Максимальное количество попыток подключения
  max_retry: 10

  # Пароль. По умолчанию пусто
  # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
  # ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
  password:

  # Логин. По умолчанию пусто
  username:

# Настройки подключения к SoftSwitch
soft_switch:

  # Путь хранения бэкапов на сервере софт-свитча
  # По умолчанию /opt/flat/fss-server/backup
  backup_dir: /opt/flat/fss-server/backup

  # Адрес
  url: 10.77.13.34:1540

# НЕ РЕДАКТИРОВАТЬ. Версия конфига.
version: 7
```

5. После изменения конфигурационных файлов перезапустите сервис и проверьте успешность его запуска:

```
service flatsoftswitchbackend restart
systemctl status flatsoftswitchbackend.service
```

Статус сервиса должен быть: **active (running)**.

7.5.2.2. Установка бэкенда ЛК пользователя

1. Установите модуль:

```
apt install lc-backend
```

2. В конфигурационном файле `/opt/flat/lc-backend/config.yml` измените значение параметров:

soft_switch: url – укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch.

device_manager: login – укажите логин пользователя DM с ролью API. Не обязательное значение.

device_manager: password – укажите пароль пользователя DM с ролью API. Не обязательное значение.

device_manager: url – укажите адрес DM. Не обязательное значение.

db: dsn – в строке параметра укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch, например:

```
db:
  dsn: rapid:QwSDv@tcp(10.77.13.34:3306)/rapidcall?charset=utf8mb4&parseTime=True&loc=Local
```

3. При необходимости скрыть в конфигурационном файле IP-адрес подключения, порт взаимодействия и пароль доступа к БД зашифруйте указанное на предыдущем шаге значение параметра:

db: dsn – присвойте параметру зашифрованное значение строки, в которой укажите FQDN или IP-адрес хоста ФЛАТ SoftSwitch. Перейдите в каталог с сервисом и выполните команду шифрования одной строкой:

```
cd /opt/flat/lc-backend/
./lc-backend_<версия_сервиса> encrypt --
text='rapid:QwSDv@tcp(10.77.13.34:3306)/rapidcall?charset=utf8mb4&parseTime=True&loc=Local'
```

Где `<версия_сервиса>` – номер версии сервиса.

4. При необходимости скрыть в конфигурационном файле назначенный при установке ключ шифрования access-токена зашифруйте значение параметра:

auth: key – присвойте параметру зашифрованное значение этого же параметра, сформированное при установке системы. Перейдите в каталог с сервисом и выполните команду шифрования:

```
cd /opt/flat/lc-backend/
./lc-backend_<версия_сервиса> encrypt --text='jNsywRxywlkXTICaarqZlucvPngeSQCAvCcl'
```

Где в строке команды:

версия_сервиса – номер версии сервиса.

jNsywRxywlkXTICaarqZlucvPngeSQCAvCcl – назначенный при установке ключ шифрования access-токена.

В результате выполнения команды шифрования будет получено значение, которое необходимо присвоить параметру **key**: `e519925533aa70b2ec1fff24f19854729eb3e319972aa43ee0901982741e0fe5be8c365934bf9ad2`.

Пример конфигурационного файла с уже зашифрованными строками:

```
/opt/flat/lc-backend/config.yml

# Настройки аутентификации
auth:

  # Время жизни access токена в минутах. По умолчанию 15 минут.
  # Для SSO время жизни токена согласно настройкам IDP
  access_token_ttl: 30

  # Ключ шифрования access токена.
  # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
  # ./lc-backend_1.0.0 encrypt --text='....'
  key: e519925533aa70b2ec1fff24f19854729eb3e319972aa43ee0901982741e0fe5be8c365934bf9ad2
```

```
# Настройки аутентификации через Active Directory.
```

```
ldap:
```

```
# Адрес AD
```

```
# ldap://example.com:389
```

```
# ldaps://example.com:636
```

```
addr: ldap://10.77.13.11:389
```

```
# BaseDN пользователей
```

```
# Если включена синхронизация через LDAPSynchronizer, рекомендуется скопировать
```

```
# base_dn из config.json.
```

```
base_dn: OU=OrganizationalUnit,DC=example,DC=com
```

```
# Фильтрация пользователей.
```

```
# Если нужно разрешить доступ только пользователям из определенной группы или
```

```
# по другому признаку.
```

```
# Оставьте пустым, если хотите разрешить доступ всем пользователям из BaseDN.
```

```
base_filter: (objectClass=Person)
```

```
# Домен AD.
```

```
# Требуется для авторизации пользователей - login_attr + @ + example.com
```

```
domain: example.com
```

```
# Укажите true для включения
```

```
enabled: false
```

```
# Из какого параметра извлекать Логин. Принимает одно значение.
```

```
# Если включена синхронизация через LDAPSynchronizer, рекомендуется скопировать
```

```
# data.login из config.json.
```

```
# Обычно sAMAccountName или cn
```

```
login_attr: sAMAccountName
```

```
# Время жизни refresh токена в минутах. По умолчанию 540 минут - 8 часов.
```

```
refresh_token_ttl: 540
```

```
# Настройки SSO
```

```
sso:
```

```
# Настройки OIDC
```

```
oidc:
```

```
# ID клиента
```

```
client_id:
```

```
# Секретный ключ
```

```
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
```

```
# ./lc-backend_1.0.0 encrypt --text='....'
```

```
client_secret:
```

```
# Укажите адрес для извлечения конфигурации провайдера
```

```
# Отправится запрос по адресу config_url + /.well-known/openid-configuration
```

```
config_url: http://10.77.13.11/oauth2/token
```

```
# Укажите true для включения
```

```
enabled: false
```

```
# Из какого параметра извлекать Логин
```

```
# По умолчанию sub
```

```
login_attr: sub
```

```
# Адрес данного сервиса.
```

```
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
```

```

root_url: http://10.77.13.11:8041

# Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
# Принимает массив(несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:
  - http://10.77.13.11:3000

# Настройки SAML
saml:

  # Самоподписанный сертификат
  # openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
  # -days 365 -nodes -subj "/CN=myservice.example.com"
  cert_file:

  # Укажите true для включения
  enabled: false

  # Самоподписанный ключ
  # openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
  # -days 365 -nodes -subj "/CN=myservice.example.com"
  key_file:

  # Из какого параметра извлекать Логин
  # По умолчанию http://wso2.org/claims/username
  login_attr: http://wso2.org/claims/username

  # Если файл xml расположен на сервере, укажите полный путь к нему
  # У текущего пользователя должны быть права на чтение
  meta_data_path: /etc/metadata.xml

  # Если xml расположен на сервере IDP, укажите его адрес
  # https://example.com:8443/realms/master/protocol/saml/descriptor
  meta_data_url:

  # Адрес данного сервиса.
  # Если настроен nginx, домен и порт должны совпадать с настройками nginx
  root_url: http://10.77.13.11:8041

  # Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
  # Принимает массив (несколько адресов)
  # Удалите все адреса, чтобы снять ограничение (не рекомендуется)
  valid_redirect_urls:
    - http://10.77.13.11:3000

# Настройки БД.
db:

  # Настройка подключения к MariaDB.
  # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
  # ./lc-backend_1.0.0 encrypt --text='....'
  dsn: fd36914520c259bfc62cc00fddaf6d19cee5a346fe76ff7b93d454d3387d52b2edf6486814b9b0d5

  # Максимальное количество неактивных подключений к базе данных
  max_idle_conn: 10

  # Максимальное количество открытых подключений к базе данных
  max_open_conn: 100

# Настройки Device Manager
device_manager:

```

```
# Логин
# Нужно создать пользователя на DM с логином API
login: api

# Пароль
password: 12345678

# Адрес DM
url: https://10.77.14.124

# НЕ РЕДАКТИРОВАТЬ. Всегда должен быть false.
force: false

# Настройка сети
http:

# Адрес
# localhost - при настройке nginx (http/https или домен)
# ip адрес - доступ по IP адресу, настройка nginx не требуется
host: localhost

# Порт
# Укажите любой свободный порт
# При настройке nginx укажите этот порт в проху настройках
port: 8041

# Настройка логирования
log:

# Архивация файлов -> max_backups.
# Каждый файл архивируется отдельно
compress: true

# production или development
debug: production

# Путь к папке с логами
# Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
folder: /var/log/flat/lc-backend

# Максимальное время хранения
max_age: 28

# Максимальное количество файлов
max_backups: 4

# Максимальный размер файла
max_size: 10

# Настройка подключения к REDIS
redis:

# Адреса
address:
  - localhost:6379

# Включить кластер
cluster_mode: false

# Номер БД
db: 0

# Максимальное количество попыток подключения
```

```

max_retry: 10

# Пароль. По умолчанию пусто
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
./lc-backend_1.0.0 encrypt --text='....'
password:

# Логин. По умолчанию пусто
username:

# Адрес SoftSwitch
soft_switch_url: 10.77.13.34:1540

# НЕ РЕДАКТИРОВАТЬ. Версия конфига.
version: 5

```

5. После изменения конфигурационных файлов перезапустите сервис и проверьте успешность его запуска:

```

service lc-backend restart
systemctl status lc-backend.service

```

Статус сервиса должен быть: **active (running)**.

7.5.2.3. Установка фронтенда ФЛАТ SoftSwitch и ЛК пользователя

1. Установите сервисы:

```

apt install fss-frontend
apt install lc-frontend

```

Проверьте успешность запуска сервисов:

```

systemctl status fss-frontend.service
systemctl status lc-frontend.service

```

Статус сервиса должен быть: **active (running)**.

2. Проверьте успешность запуска и версию **nodejs** (пакет должен быть не ниже 18 версии):

```
node -v
```

В ответ должна быть выведена версия, например: v18.20.6.

7.5.2.4. Обеспечение безопасности онлайн-транзакций

Для защиты соединения между сервисами ЛК и WEB-браузером пользователя применяется автоматически создаваемый при установке системы самоподписанный SSL-сертификат. Поддерживается TLS v.1.3. Файлы самоподписанного сертификата и приватного ключа располагаются по следующему пути:

```

/opt/flat/cert/rootCA.pem
/opt/flat/cert/rootCA.key

```

При необходимости использования коммерческого сертификата или в случае выпуска самоподписанного сертификата с другими параметрами поместите их в указанный каталог и внесите изменения в конфигурационные файлы системы.

7.5.2.4.1. Создание самоподписанного сертификата

Действия по созданию самоподписанного сертификата можно выполнить на машине с ФЛАТ Личный Кабинет.

Для генерации необходимых файлов перейдите в каталог **/opt/flat/cert/** (при отсутствии каталога **/cert** создайте его) и выполните команду одной строкой, например:

```
openssl req -x509 -newkey rsa:2048 -days 3650 -nodes -out rootCA.crt -keyout rootCA.key -subj
/C=RU/O="Flat Software"/CN="softswitch.ts.lab" -addext "subjectAltName = DNS:softswitch.ts.lab"
```

где:

rootCA.key – имя получаемого приватного ключа

rootCA.crt – имя получаемого SSL-сертификата

Flat Software – название организации (например, Flat Software)

softswitch.ts.lab – доменное имя в корпоративном DNS

После выполнения команды в каталоге **/opt/flat/cert** будут созданы файлы самоподписанного сертификата и приватного ключа.

7.5.2.4.2. Внесение изменений в конфигурационные файлы

Внесите изменения в следующие конфигурационные файлы:

/etc/nginx/sites-available/fss-frontend

/etc/nginx/sites-available/lc-backend

/etc/nginx/sites-available/lc-frontend

В каждом из них в следующих параметрах:

ssl_certificate – укажите путь расположения и имя коммерческого или самоподписанного SSL-сертификата.

ssl_certificate_key – укажите путь расположения и имя приватного ключа.

Пример части конфигурационного файла для самоподписанного сертификата:

```
/etc/nginx/sites-available/fss-frontend
```

```
ssl_certificate /opt/flat/cert/rootCA.crt;
ssl_certificate_key /opt/flat/cert/rootCA.key;
```

7.6. Выключение и перезапуск системы

Корректное выключение системы выполняется командой:

```
shutdown now
```

Перезапуск системы происходит вводом команды:

```
reboot
```

7.7. Обновление системы

Перед обновлением рекомендуется сделать копию БД системы. См. главу «Резервные копии» руководства «ФЛАТ SoftSwitch. Руководство администратора» (ссылку на документ см. в разделе [Связанные документы](#)).

Для обновления системы вначале удалите прежний репозиторий командой:

```
apt purge flat-softswitch-repository*
```

Скачайте и установите новый репозиторий, затем в том же порядке выполните установку всех необходимых пакетов.

Обновление ФЛАТ SoftSwitch не влияет на конфигурацию системы и сохраненные журналы событий.

7.8. Удаление системы

При необходимости удаления всех установленных пакетов выполните команды:

```
/opt/flat/fss-server/tools/.drop-database.sh
```

```
apt purge fss-server*
```

```
apt purge fss-mediasrv*
```

```
apt purge fss-srclient*
```

```
apt purge flat-file*
```

```
apt purge flatsoftswitchbackend*
```

```
apt purge fss-frontend*
```

```
apt purge lc-backend*
```

```
apt purge lc-frontend*
```

7.9. Откат на предыдущую версию

После обновления ФЛАТ SoftSwitch может возникнуть необходимость отката на предыдущую сборку ядра. Для этого выполните следующий скрипт:

```
/opt/flat/switchserver/tools/switch-version.sh
```

7.10. Обновление лицензионных ключей

Для замены временной лицензии на постоянную, либо обновлении лицензионного ключа при расширении системы, отредактируйте конфигурационный файл `/opt/flat/switchserver/settings.ini`, указав новый ключ в параметре License, раздел [General]:

```
[General]
```

```
License= m7it95xd7UYNPMT/3jbybPeL25/0GTKA15RLYx3ZVXa/RGqB7zbpBpt5
```

После обновления ключей необходимо поочередно перезапустить сервисы на основном и дублирующем узле командой:

```
service flat_ss restart
```



Временная лицензия после окончания своего срока продолжает действовать до перезагрузки ядра системы (для версий ФЛАТ SoftSwitch до v.3.4).

7.11. Настройка SIP-TLS



TLS между ядром ФЛАТ SoftSwitch и клиентом работает без проверки валидности сертификатов и без SRTP/SRTCP.

При необходимости шифрования сигнальных сообщений возможно использование коммерческого сертификата организации, либо самоподписанного сертификата, автоматически создаваемого при установке системы ФЛАТ SoftSwitch. В случае необходимости выпуска самоподписанного сертификата с другими параметрами выполните его генерацию.

Описание действий по созданию самоподписанного сертификата см. [Создание самоподписанного сертификата](#).

8. Ротация логов

Для автоматизации обработки журналов событий применяется как встроенный в некоторые модули механизм ротации, так и утилита Logrotate, по умолчанию входящая в большинство дистрибутивов.

При установке подсистем ФЛАТ SoftSwitch механизм запуска Logrotate настраивается автоматически.

8.1. Ротация логов с помощью Logrotate

Правила обработки логов подсистем ФЛАТ SoftSwitch находятся в следующих конфигурационных файлах (при отсутствии создайте их самостоятельно):

Подсистема	Имя конфигурационного файла
Ядро SIP SoftSwitch	/etc/logrotate.d/fss-server.conf
Фронтенд SoftSwitch	Логи ротируются через logrotate nginx. См. /etc/logrotate.d/nginx.conf
Фронтенд ЛК	Логи ротируются через logrotate nginx. См. /etc/logrotate.d/nginx.conf
Сервис Mediasrv	/etc/logrotate.d/fss-mediasrv.conf
Сервис SRClient	/etc/logrotate.d/fss-srclient.conf

Конфигурационные файлы Logrotate описывают правила обработки логов. Описание секции начинается с указания файлов, над которыми будет производиться ротация. Имена файлов можно задавать по маске или указывать явно. Параметры указываются в фигурных скобках. Ротацию можно производить по расписанию (ежедневно, еженедельно, ...) или по достижению определенного размера LOG-файлом – это взаимоисключающие параметры.

Краткий список параметров Logrotate:

Параметр	Описание
rotate <число>	Количество хранимых файлов.
daily weekly monthly	Производить ротацию раз в день/неделю/месяц.
size <байт> size 1000 size 100k size 1M	Производить ротацию если log-файл превысил указанный размер байт Кбайт Мбайт
start <число>	Число, с которого начнётся нумерация файлов.
compress	Архивировать файлы (по умолчанию gzip).
nocompress	Выключение сжатия.
delaycompress	Не сжимать «свежесозданный» архив. Например access.log.1 не будет сжат. Используется с параметром compress.
create <права> <владелец> <группа> create 640 root root	После ротации создать пустой LOG-файл. Любые из этих атрибутов могут быть опущены, в этом случае вместо них для нового файла будут использованы атрибуты, имеющие те же значения, что и первоначальный LOG-файл.
nocreate	Не создавать файл.
copy	Создать копию оригинального LOG-файла, не изменяя его. Исключает create.

Параметр	Описание
nocoru	Отключает сору.
copytruncate	Создать копию оригинального log-файла, а потом его «обнулить». Таким образом сам файл не удаляется. Исключает сору, create.
notifempty	Не архивировать пустые файлы.
missingok	В случае отсутствия оригинального log-файла не вызовет ошибку.
olddir <путь>	Перемещать архивные файлы в указанную директорию. Например: olddir /home/logs
dateext	К имени файлов журналов добавляется дата (%Y%m%d), вместо номера.

Пример конфигурационного файла для ядра SIP SoftSwitch:

```
/etc/logrotate.d/switchserver.conf

/var/log/switchserver/*.txt {
daily
rotate 7
dateext
missingok
copytruncate
compress
notifempty
}
```

Эти настройки означают, что обработке подлежат все логи из папки /var/log/switchserver/ с расширением «.txt», ротация журналов будет выполняться ежедневно, будут храниться семь последних журналов, более старые копии будут автоматически удаляться, будет использоваться сжатие, а к имени файла архива журнала будет добавляться дата создания.

Полная информация о настройках логирования и путях хранения логов по умолчанию приведена в документе «ФЛАТ SoftSwitch. Руководство администратора» (ссылку на документ см. в разделе [Связанные документы](#)).

За более подробным описанием утилиты Logrotate, поставляемой с используемым дистрибутивом Linux, следует обратиться к документации по ОС.

8.2. Ротация логов сервиса FlatFileManager, бэкенда SoftSwitch и ЛК

Ротация логов для сервиса FlatFileManager, бэкенда SoftSwitch и бэкенда ЛК выполняется модулями самостоятельно.

Настройки логирования и ротации настраиваются в конфигурационных файлах каждого модуля:

Подсистема	Имя конфигурационного файла	Путь хранения логов по умолчанию
Сервис FlatFileManager	/opt/flat/flat-file/config.yml	/var/log/flat/flat-file/
Бэкенд SoftSwitch	/usr/lib/flatSoftSwitchBackend/config.yml	/var/log/flatSoftSwitchBackend/
Бэкенд ЛК	/opt/flat/lc-backend/config.yml	/var/log/flat/lc-backend/

Покажем настройки на примере конфигурационного файла бэкенда ЛК (приведена часть файла):

```
/opt/flat/lc-backend/config.yml
```

```
# Настройка логирования
```

```
log:
```

```
  # Архивация файлов -> max_backups.
```

```
  # Каждый файл архивируется отдельно
```

```
  compress: true
```

```
  # production или development
```

```
  debug: production
```

```
  # Путь к папке с логами
```

```
  # Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
```

```
  folder: /var/log/flat/lc-backend
```

```
  # Максимальное время хранения
```

```
  max_age: 28
```

```
  # Максимальное количество файлов
```

```
  max_backups: 10
```

```
  # Максимальный размер файла
```

```
  max_size: 10
```

9. Доступность WEB-интерфейса и проверка работоспособности

9.1. Настройки для формы авторизации

Перед проверкой доступности WEB-интерфейса уточните список администрируемых систем в форме авторизации фронтенда ФЛАТ SoftSwitch.

В параметре **addresses** конфигурационного файла `/opt/flat/fss-frontend/apps/softswitch/public/config.json` должен быть указан IP-адрес (или FQDN) и порт взаимодействия бэкенда ФЛАТ SoftSwitch.

При указании через запятую нескольких адресов форма авторизации будет дополнена полем выбора администрируемой системы, при указании одного адреса (по умолчанию) поле выбора отображаться не будет.

Пример конфигурационного файла с адресами двух администрируемых систем и включенными дополнительными способами аутентификации:

```
/opt/flat/fss-frontend/apps/softswitch/public/config.json
{
  "addresses": ["10.77.13.11:443", "10.77.15.194:443"]
  "isDomainAuthEnable": false,
  "isSSOEnable": false
}
```

Для включения в форме авторизации фронтенда ФЛАТ SoftSwitch элементов дополнительных способов аутентификации измените значение следующих параметров и перезапустите сервис:

isDomainAuthEnable – укажите **true** при аутентификации с использованием AD, или **false** без использования.

isSSOEnable – укажите **true** при аутентификации с использованием SSO, или **false** без использования.

Описание дополнительных способов аутентификации приведено в главе «Аутентификация пользователей с использованием AD и SSO» документа «ФЛАТ SoftSwitch. Руководство администратора» (ссылку на документ см. в разделе [Связанные документы](#)).

9.2. Вход в WEB-интерфейс

Для входа в WEB-интерфейс администратора в адресной строке браузера введите FQDN или IP-адрес фронтенда ФЛАТ SoftSwitch (указание http/https зависит от настроек сервиса nginx).

Для примера из данного руководства необходимо набрать <https://10.77.13.11> без указания порта.

При корректном вводе IP-адреса отобразится форма авторизации, в поля которой введите *Логин* и *Пароль* администратора (см. [Рисунок 19](#)). По умолчанию в системе создан пользователь «admin» с правами администратора и паролем «admin».

Рисунок 19. Форма авторизации

После входа в интерфейс администратора на главной странице проверьте версию установленной системы, общее количество лицензий, их тип и срок действия (см. [Рисунок 20](#)):

Рисунок 20. Главная страница интерфейса

9.3. Проверка работоспособности

Недоступность WEB-интерфейса может говорить либо о некорректно введенном лицензионном ключе, либо о проблемах с запуском сервисов. Для выяснения причины необходимо проанализировать журналы событий ядра системы (логи).

По умолчанию журналы событий ядра системы ФЛАТ SoftSwitch хранятся в каталоге `/var/log/flat/switchserver/`.

Для проверки корректности ввода лицензионного ключа откройте журнал `licenseLog.txt`, найдите следующие параметры:

```
14:05:42.513: license=m7it95xdnTEIPML33jLybPeB2pToGy2e14pLYBXbXX0+Rm6C7jPqAZ14mks=
14:05:42.513: MAC=080863451
14:05:42.513: CheckMac=True
14:05:42.513: License result=1
14:05:42.513: License count=1000
14:05:42.513: license ibtained from local source
14:05:42.513: License days remaining: 137
```

Параметр **CheckMac** описывает соответствие MAC-адреса сервера сохраненному в ключе.

Параметр **License count** описывает количество доступных лицензий. Его значение больше нуля косвенно говорит о корректности ввода лицензионного ключа.

Сравните введенную лицензию с полученной от вендора. При необходимости введите корректное значение (см. раздел [Обновление лицензионных ключей](#)).

Протокол запуска системы сохраняется в журнале **initLog.txt**, в последней строке которого показан результат запуска системы – «Server started».

Полная информация по администрированию системы приведена в документе «ФЛАТ SoftSwitch. Руководство администратора» (ссылку на документ см. в разделе [Связанные документы](#)).

10. Настройка системы

Перед началом работы ознакомьтесь с главой [Взаимодействие с пользовательским интерфейсом](#).

10.1. Этапы настройки системы

Первоначальную настройку системы ФЛАТ SoftSwitch рекомендовано проводить в следующем порядке:

1. Подключение к системе ([Подключение к WEB-интерфейсу](#)), уточнение ролей пользователей системы и создание учетных записей администраторов ([Администраторы](#)).
2. Создание зон ([Создание зон](#)) и локаций ([Создание локаций](#)).
3. Создание абонентов ([Абоненты](#)).
4. Создание транков (см. [Транки](#)).
5. Определение сервисных кодов (см. [Сервисные коды](#)).
6. Настройка классификации ([Классификация](#)), маршрутизации ([Маршрутизация](#)), АОН ([АОН](#)).
7. Настройка резервного копирования БД ([Резервные копии](#))
8. Настройка дополнительных видов обслуживания ([Дополнительные виды обслуживания](#)).

10.2. Подключение к WEB-интерфейсу

Администрирование систем семейства ФЛАТ осуществляется через WEB-интерфейс. Для подключения к интерфейсу администратора в адресной строке браузера введите FQDN или IP-адрес установленного фронтенда ФЛАТ SoftSwitch (пример: <http://10.77.13.11>, указание http/https зависит от настроек сервиса nginx и фронтенда ФЛАТ SoftSwitch, см. документ «ФЛАТ SoftSwitch. Руководство по установке»). При корректном вводе адреса в окне браузера отобразится форма авторизации (см. [Рисунок 21](#)):

Рисунок 21. Форма авторизации

Далее в форме авторизации введите *Логин* и *Пароль* администратора, выберите в раскрывающемся списке IP-адрес администрируемой системы. По умолчанию создан пользователь «admin» с правами администратора и паролем «admin». После первого входа в интерфейс обязательно измените пароль.



Выбор IP-адреса в форме авторизации позволяет управлять несколькими системами из одного интерфейса (см. [Список администрируемых систем в форме авторизации](#)).

В дополнение к механизму авторизации по логину и паролю могут применяться способы аутентификации с использованием Active Directory и технологии единого входа. В первом случае после ввода логина и пароля отметьте чек-бок **Доменная авторизация**, а в случае аутентификации с использованием SSO нажмите кнопку **SSO**. См. [Аутентификация пользователей с использованием AD и SSO](#).

После успешной авторизации откроется главная страница интерфейса с информацией о версиях входящих в систему модулей, количестве активированных и доступных лицензий, типе лицензий и периоде их действия, проценте пространства, занимаемом лог-файлами (см. [Рисунок 22](#)):

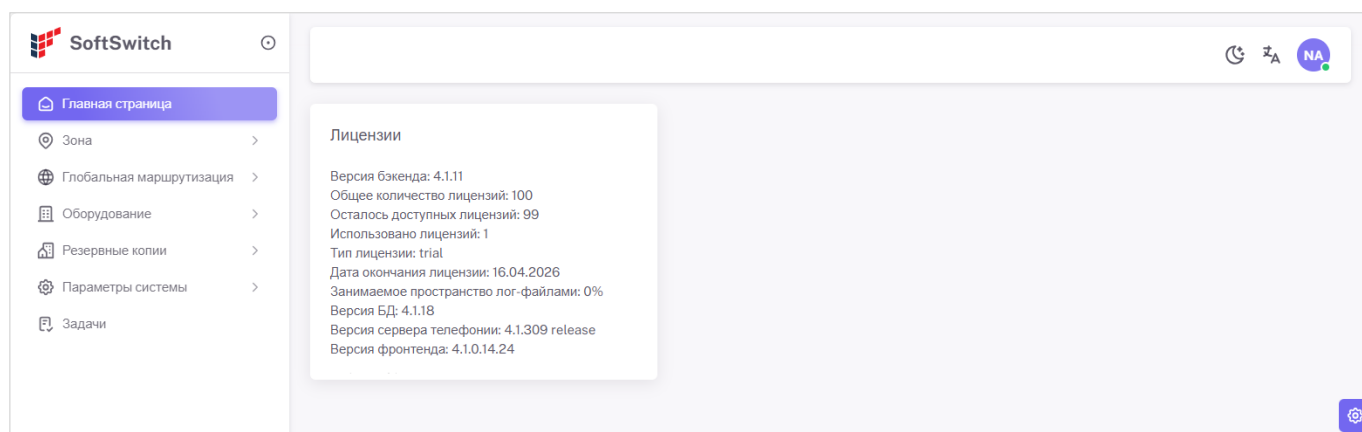


Рисунок 22. Главная страница интерфейса

10.3. Параметры системы

Раздел **Параметры системы** позволяет получить доступ к настройкам тарификации и логирования, инструменту тестирования маршрутов и созданию учетных записей пользователей системы, списку сохраненных фильтров.

10.3.1. Администраторы

Раздел предназначен для настройки ролей пользователей, управления учетными записями администраторов системы, просмотра журналов безопасности и заблокированных адресов.

10.3.1.1. Разрешения

В системе ФЛАТ SoftSwitch предусмотрен ролевой принцип разграничения прав доступа к настройкам и функциям в соответствии с решаемыми задачами и используемыми разрешениями.

Для просмотра predetermined в системе разрешений выберите меню **Параметры системы/Администраторы/Разрешения**, после чего в окне отобразится список сущностей с указанием названия разрешения и его описания (см. [Таблица 1](#)). Разрешения доступны только для просмотра, их нельзя изменять и дополнять.

Таблица 1. Список разрешений

ID	Название	Права
93	abonent-profile-features/types	Функции абонентов/Типы
37	abonents	Абоненты
20	abonents-query-history	История запросов абонентов
30	auth/roles	Роли
70	auth/sessions	Активные сеансы
69	auth/users	Пользователи
92	balance-types	Типы балансировки
9	blocked-ips	Заблокированные адреса
62	branches	Живучий офис

ID	Название	Права
71	cdr	Тарификация
46	classifications/cot	Классификация/Классы трафика
51	clusters	Кластеры
74	codec-profiles	Наборы кодеков
52	codec-profiles/codecs	Наборы кодеков/Кодеки
90	codecs	Кодеки
40	diagnostic/route-test	Тест маршрута
85	global-areas	Глобальные области
82	global-areas/zones	Глобальные области/Зоны
26	global-balancers	Глобальные балансировщики
34	global-balancers/zones	Глобальные балансировщики/Зоны
22	global-routes	Глобальные маршруты
97	global-source-types	Типы источников глобальной маршрутизации
102	global-target-types	Типы целей глобальной маршрутизации
91	groups/types	Группы/Типы групп
6	line-classes	Классы линии
60	line-classes/rules	Классы линии/Правила
11	line-classes/rules/bitrates	Классы линии/Правила/Битрейты
103	location-settings-names	Имена настроек локаций
72	locations	Локации
23	log-level-settings	Логирование/Настройка
99	log-levels	Уровни логирования
27	logs	Файлы логирования
19	maintenance-backup	Резервное копирование/Ручное
54	maintenance-backup-settings	Резервное копирование/Задания
58	maintenance-ftp-servers	Резервное копирование/Цели/FTP-серверы
53	maintenance-local-paths	Резервное копирование/Цели/Локальные пути
95	maintenance-target-types	Типы целей тарификации
79	media-resources	Медиа ресурсы
81	media-resources/media-servers	Медиа ресурсы/Медиа серверы
10	media-resources/roles	Медиа ресурсы/Роли
96	media-types	Типы медиа
98	pickup-notification-types	Типы уведомлений
94	protocols	Протоколы
36	query-history	История запросов
101	routing-target-types	Типы целей маршрутизации
100	service-codes/types	Сервисные коды/Типы

ID	Название	Права
83	tasks	Задачи
31	zones	Зоны
68	zones/abonents	Зоны/Абоненты
2	zones/abonents/black_list	Зоны/Абоненты/Черный список
15	zones/abonents/groups	Зоны/Абоненты/Группы
32	zones/abonents/profiles	Зоны/Абоненты/Профили
66	zones/abonents/profiles/features	Зоны/Абоненты/Профили/Функции
16	zones/abonents/services	Зоны/Абоненты/Сервисы
84	zones/abonents/white_list	Зоны/Абоненты/Белый список
47	zones/ani-mod-sets	Зоны/АОН/Список групп модификаторов
73	zones/ani-mod-sets/numbers	Зоны/АОН/Пул номеров
63	zones/ani-mod-sets/rules	Зоны/АОН/Список модификаторов
78	zones/classifications	Зоны/Классификация
61	zones/classifications/cor	Зоны/Классификация/Классы ограничения
75	zones/classifications/cor/cot	Зоны/Классификация/Классы ограничения/Классы трафика
55	zones/classifications/cos	Зоны/Классификация/Классы сервиса
12	zones/classifications/cos/cot	Зоны/Классификация/Классы сервиса/Классы трафика
49	zones/classifications/cot	Зоны/Классификация/Классы трафика
64	zones/classifiers	Зоны/Маршрутизация/Классификаторы
35	zones/codes	Зоны/Маршрутизация/Коды
29	zones/codes-backup	Зоны/Маршрутизация в аварийном режиме/Коды
39	zones/groups	Зоны/Группы
4	zones/groups/pickup_groups	Зоны/Группы/Группы перехвата
28	zones/groups/pickup_groups/abonents	Зоны/Группы/Группы перехвата/Абоненты
41	zones/groups/search_groups	Зоны/Группы/Группы поиска
1	zones/groups/search_groups/abonents	Зоны/Группы/Группы поиска/Абоненты
21	zones/load-balancers	Зоны/Маршрутизация/Направления
7	zones/load-balancers/trunks	Зоны/Маршрутизация/Направления/Транки
80	zones/locations	Зоны/Локации
13	zones/locations/media_servers	Зоны/Локации/Медиасерверы
33	zones/routes	Зоны/Маршрутизация/Первичная
77	zones/routes-backup	Зоны/Маршрутизация в аварийном режиме/Первичная
67	zones/schedulers	Зоны/Маршрутизация/Расписание
18	zones/service-codes	Зоны/Сервисные коды
50	zones/trunks	Зоны/Транки/Список транков
57	zones/trunks/features	Зоны/Транки/Список транков/Функции

ID	Название	Права
76	zones/trunks/profiles	Зоны/Транки/Профили
44	zones/trunks/profiles/features	Зоны/Транки/Профили/Функции
56	zones/zone-bw-profiles	Зоны/Черные-белые списки
65	zones/zone-bw-profiles/numbers	Зоны/Черные-белые списки/Номера

10.3.1.2. Роли пользователей

В системе ФЛАТ SoftSwitch предусмотрена возможность создания новых ролей пользователей и гибкой настройки их полномочий.



При установке системы создается неизменяемая и неудаляемая роль **SuperAdmin** с максимальными правами.

Для управления ролями пользователей выберите меню **Параметры системы/Администраторы/Роли**, после чего в окне отобразится список ранее созданных сущностей с указанием названия роли, количества пользователей с указанной ролью и назначенными правами на чтение/запись/выполнение действия или удаление по каждому разрешению (см. [Рисунок 23](#)):

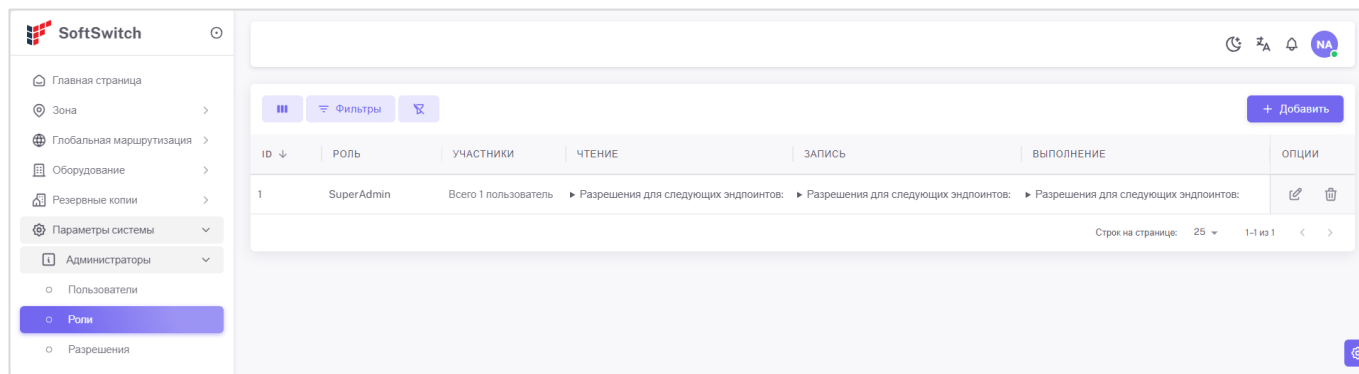


Рисунок 23. Список ролей пользователей

Для создания новой роли нажмите кнопку **Добавить**, а для редактирования параметров существующей – значок редактирования . После чего в поля открывшейся формы внесите ее название и назначьте по каждому разрешению права на чтение, запись и выполнение действия или удаление (см. [Рисунок 24](#)):

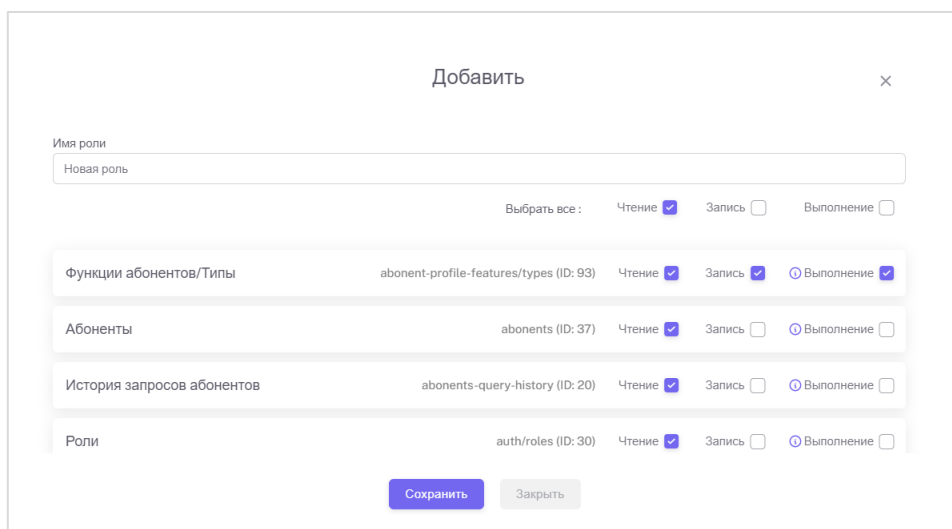


Рисунок 24. Создание новой роли

В форме доступны следующие поля:

Поле	Значение
Имя роли	Название роли.
Выбрать все	Отметка в чек-боксе. Выделение или снятие выделения со всех разрешений на чтение, запись и выполнение действия или удаление.
Список разрешений	Отметка в чек-боксе прав на чтение/запись/выполнение действия или удаление по каждому виду разрешений. Названия разрешений соответствуют методам REST API. Описание разрешений см. Разрешения .

Примеры использования ролей см. [Применение ролей пользователей](#).

10.3.1.3. Пользователи



При установке системы создается неудаляемый пользователь **admin** с неизменяемой ролью **SuperAdmin**, у которого доступны к изменению только ФИО, E-mail и пароль.

Для управления учетными записями пользователей выберите меню **Параметры системы/Администраторы/Пользователи**, после чего в окне отобразится список ранее созданных сущностей с указанием регистрационных данных (см. [Рисунок 25](#)):

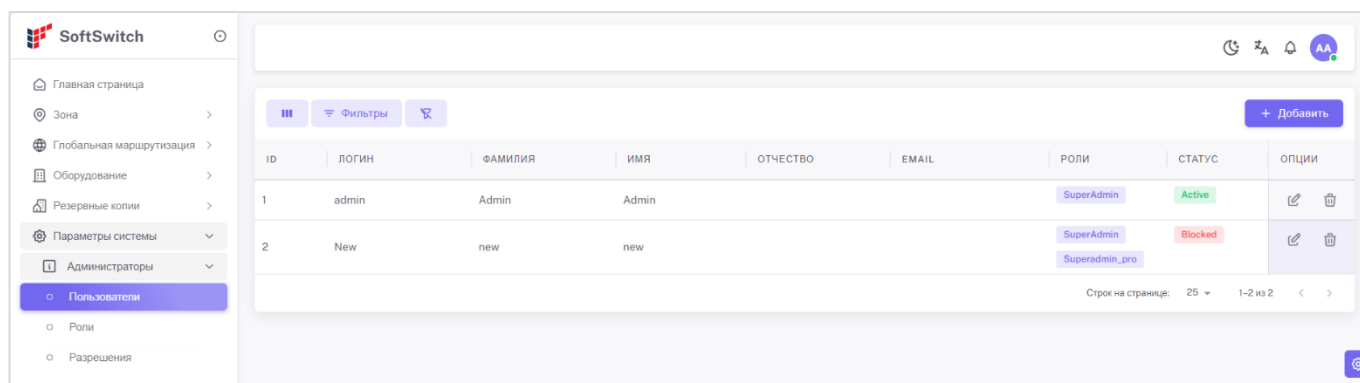


Рисунок 25. Список пользователей системы


Для создания нового пользователя нажмите кнопку **Добавить**, а для редактирования параметров существующего – значок редактирования , после чего в поля открывшейся формы внесите его параметры (см. [Рисунок 26](#)):

Рисунок 26. Создание пользователя

В форме доступны следующие поля:

Поле	Значение
Логин	Логин пользователя.
ФИО	ФИО пользователя.
E-mail	Электронная почта пользователя.
Пароль	Пароль пользователя. Пароль должен соответствовать следующим требованиям к сложности: минимальная длина пароля – 8 знаков, использование цифр и специальных символов.
Права доступа пользователя	Назначение пользователю одной или нескольких ролей. При назначении пользователю нескольких ролей их полномочия складываются. Это означает, что пользователю предоставляются права, доступные в каждой назначенной ему роли. См. Роли пользователей .
Заблокировать пользователя	Блокировка учетной записи пользователя. Статус отображается в строке пользователя: Active / Blocked .

10.3.1.4. Журнал безопасности

В системе ведется журнал действий пользователей, который доступен при выборе меню **Параметры системы/Администраторы/Журнал безопасности**. Сохраняется информация об ID пользователя, его ФИО и IP-адресе подключения, методе и коде ответа, ID операции, пути и времени события (см. [Рисунок 27](#)):

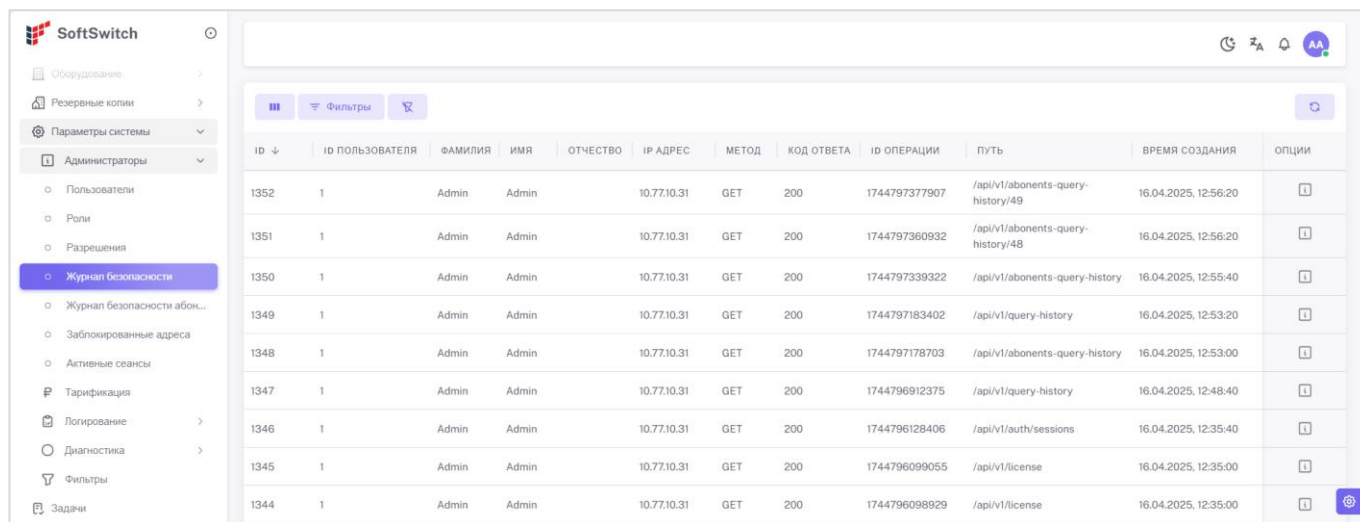



Рисунок 27. Журнал безопасности

При нажатии на кнопку , расположенную в строке действий пользователя, на экран будет выведена подробная информация о событии (см. [Рисунок 28](#)):

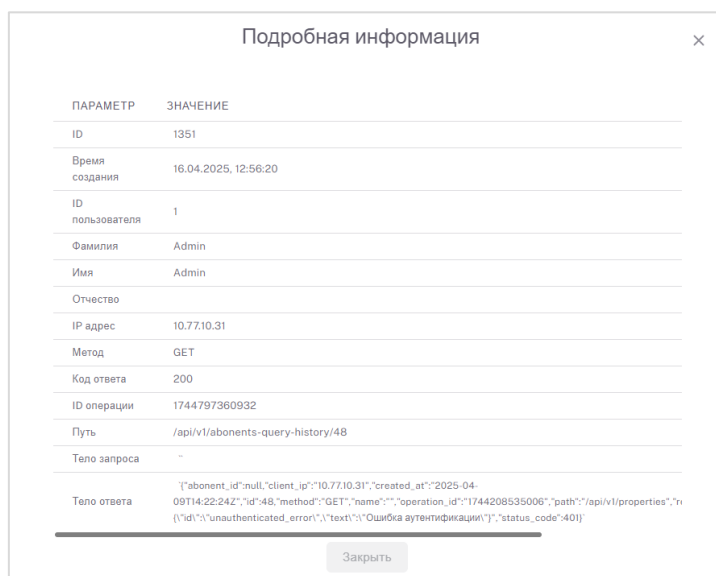


Рисунок 28. Подробная информация о событии

10.3.1.5. Журнал безопасности абонентов

В системе ведется журнал действий абонентов, который доступен при выборе меню **Параметры системы/Администраторы/Журнал безопасности абонентов**. Сохраняется информация об ID абонента, его ФИО и IP-адресе подключения, методе и коде ответа, ID операции, пути и времени события (см. [Рисунок 29](#)):

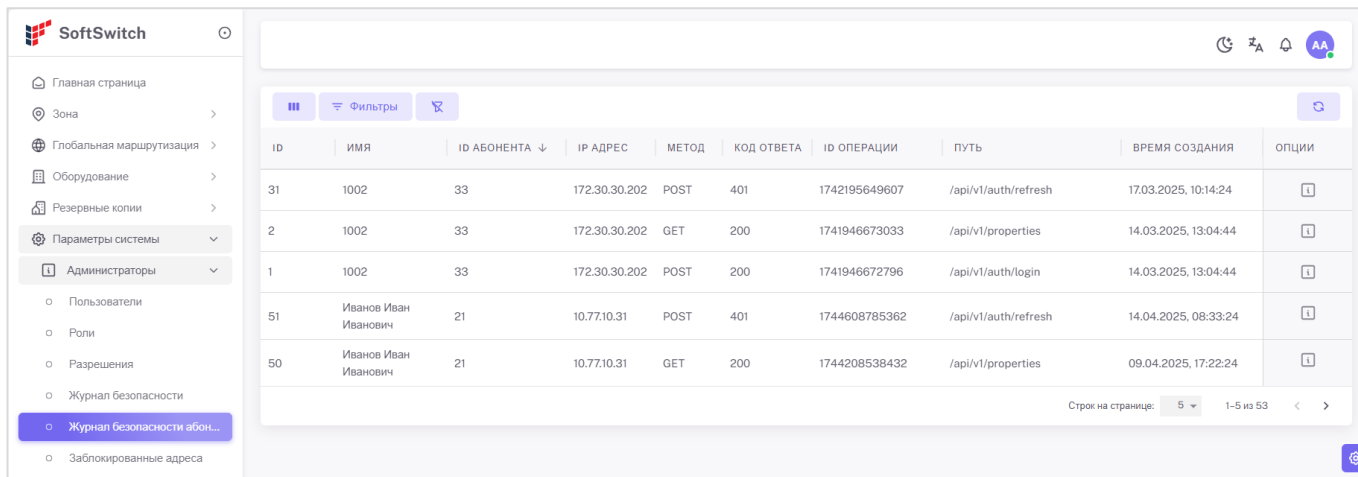



Рисунок 29. Журнал безопасности абонентов

При нажатии на кнопку , расположенную в строке действий абонента, на экран будет выведена подробная информация о событии (см. Рисунок 30):

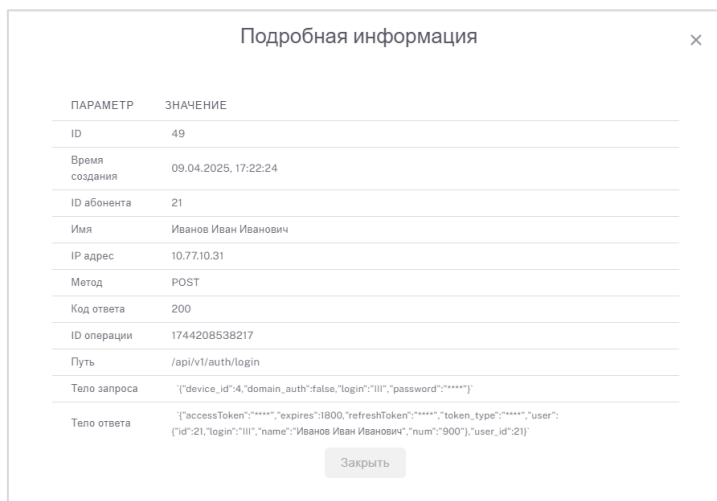


Рисунок 30. Подробная информация о действии абонента

10.3.1.6. Заблокированные адреса

В системе ФЛАТ SoftSwitch ограничивается количество неудачных попыток регистрации абонентских устройств, включая попытки без авторизации. При превышении максимально количества неудачных попыток регистрации IP-адрес этого оборудования блокируется, новые попытки регистрации игнорируются до разблокировки администратором.

Журнал блокировок доступен в пункте меню **Параметры системы/Администраторы/Заблокированные адреса**.

Максимальное количество попыток регистрации абонентских устройств описывается параметром RegisterMaxAttempts в `/opt/flat/fss-server/settings.ini` раздела [SIP]:

```
[SIP]
RegisterMaxAttempts=5
```

При пустом значении параметра или его отсутствии количество попыток регистрации абонентских устройств не ограничено.

10.3.1.7. Активные сеансы

В меню **Параметры системы/Администраторы/Активные сеансы** доступен список активных учетных записей с указанием ID пользователя, логином, ФИО, типом устройства подключения, времени авторизации в системе и возможностью ручного завершения сеанса:

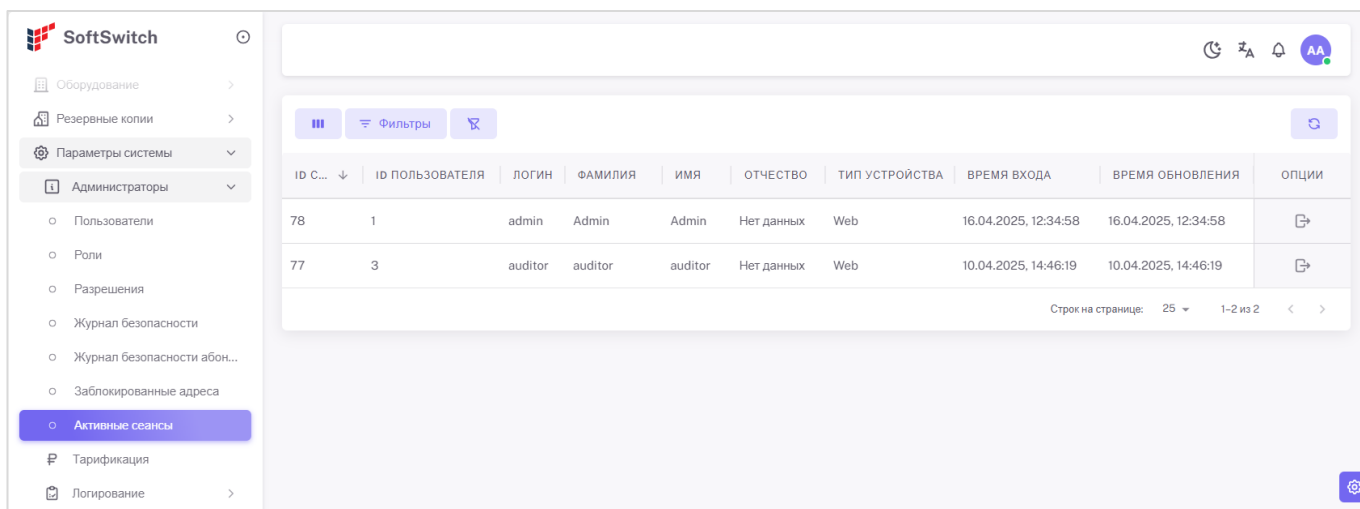



Рисунок 31. Активные сеансы

При нажатии кнопки , расположенной в строке пользователя возможно завершить его текущий сеанс.

10.3.2. Тарификация

Система ФЛАТ SoftSwitch собирает информацию о вызовах на основе CDR (Call Detail Recording).

Формат имени формируемого CDR-файла: `CDR_id_dd_mm_YYYY_hh_mm_ss.zzz.txt`

Таблица 2. Описание полей строки в CDR-файле формата CSV:

Поле	Значение
StartDatetime	Время начала сессии. Время поступления запроса INVITE от удаленного хоста.
FromNum	Номер FROM. User part поля FROM из заголовка запроса INVITE.
SourceType	Тип источника вызова. 1 - абонент, 2 - транк.
ToNum	Номер TO. Uer part поля TO из заголовка запроса INVITE.
DstType	Тип получателя вызова. 1 - абонент, 2 - транк.
TalkDuration	Длительность соединения. Длительность в формате hh:mm:ss между ответом OK и поступлением BYE с одной из сторон.
RingDuration	Длительность до ответа OK. Длительность в формате hh:mm:ss между INVITE и поступлением OK с вызываемой стороны.
TotalDuration	Длительность до ответа OK. Общая длительность SIP сессии.
SourceTrunk	Идентификатор транка-источника. ID транка, с которого поступил вызов (-1 если это не транк).
DstTrunk	Идентификатор транка-получателя. ID транка, на который поступил вызов (-1 если это не транк).
ConditionCode	Причина завершения вызова. Идентификатор, указывающий на причину завершения (перевод, переадресация и т.д.).

Поле	Значение
UTCStartDateTime	Время начала сессии в UTC. Время поступления запроса INVITE от удаленного хоста.
SourceTimeZone	Тайм-зона источника.
DstTimeZone	Тайм-зона получателя.
DisconnectInitiator	Инициатор окончания соединения. 1 - вызывающая сторона, 2 - вызываемая сторона.
Cause	Причина завершения соединения. Текстовое значение, в соответствие со справочником.
SUID	Уникальный идентификатор сессии.
SourceName	Имя вызывающей стороны. Для абонента - URI, для транка - название транка.
DstName	Имя вызываемой стороны. Для абонента - URI, для транка - название транка.
OriginalToNum	Набираемый номер до модификации.

Для доступа к записям вывода тарификации выберите меню **Параметры системы/Тарификация**. После чего в окне отобразится список ранее сохраненных настроек с указанием названия, места и периодичности сохранения (см. [Рисунок 32](#)):

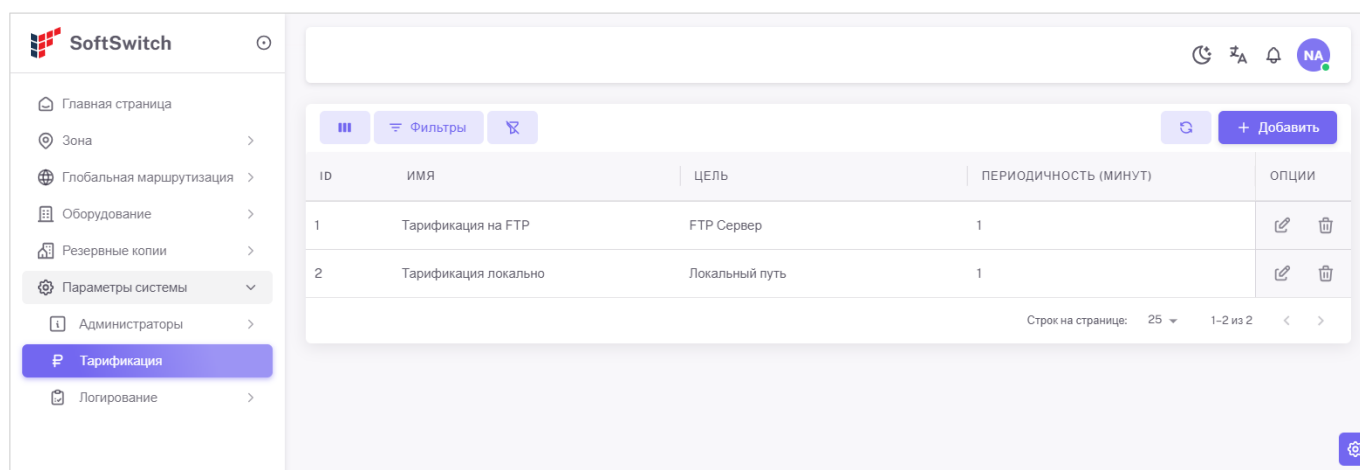


Рисунок 32. Список записей вывода тарификации

Для создания новой записи нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего откроется форма, в поля которой внесите необходимые параметры (см. [Рисунок 33](#)):

Добавить ×

Имя

Тип цели

Имя локальной цели

Периодичность (минут)

Рисунок 33. Создание записи вывода тарификации

В форме доступны следующие поля:

Поле	Значение
Имя	Название записи тарификации.
Тип цели	Тип места хранения CDR-файлов. Предопределены значения: <ul style="list-style-type: none"> • FTP-сервер • Локальный путь
Имя FTP-сервера/Имя локальной цели	Раскрывающийся список с выбором ранее созданного места хранения CDR-файлов. Определение места хранения CDR-файлов рассматривается в отдельном разделе (см. Цели).
Периодичность (минут)	Периодичность вывода в минутах.

Срок хранения CDR-файлов при локальном хранении задается в свойствах локальных путей (см. [Локальные пути](#)).

10.3.3. Логирование

ФЛАТ SoftSwitch ведет журналы событий, произошедших в системе в хронологическом порядке с сохранением как локально, так и с отправкой на сервер Syslog.



На сервер Syslog отправляются только события ядра системы.
В WEB-интерфейсе может быть задан уровень логирования только для ядра системы.

Путь локального хранения логов для каждой подсистемы ФЛАТ SoftSwitch описывается следующими параметрами:

Подсистема	ini-файл	Параметр(-ы)	Путь хранения по умолчанию
Ядро SIP SoftSwitch	/opt/flat/fss-server/settings.ini	LogPath	/var/log/flat/fss-server/
Фронтенд SoftSwitch	/etc/nginx/sites-available/fss-frontend	error_log access_log	/var/log/nginx/flat-error.log /var/log/nginx/flat-access.log
Бэкенд SoftSwitch	/usr/lib/flatSoftSwitchBackend/config.yml	log: folder	/var/log/flatSoftSwitchBackend/app.log
Сервис Mediasrv (fss-mediasrv)	/opt/flat/fss-mediasrv/config.xml	LogParams	/var/log/flat/fss-mediasrv/mediasrv.log
Сервис SRClient (fss-srclient)	/etc/flat/fss-srclient/settings.ini	logger_fileName	/var/log/flat/fss-srclient/siprecclient.log

Пример описания пути хранения параметром **LogPath** в **/opt/flat/fss-server/settings.ini**, раздел **[Log]**:

```
[Log]
LogPath=/var/log/flat/fss-server/
```

10.3.3.1. Настройки

В разделе приведены настройки уровня логирования по каждому типу журналов для ядра системы ФЛАТ SoftSwitch.

Для управления настройками выберите меню **Параметры системы/Логирование/Настройки**. После чего в окне отобразится список типов журналов ядра системы (см. [Рисунок 34](#)):

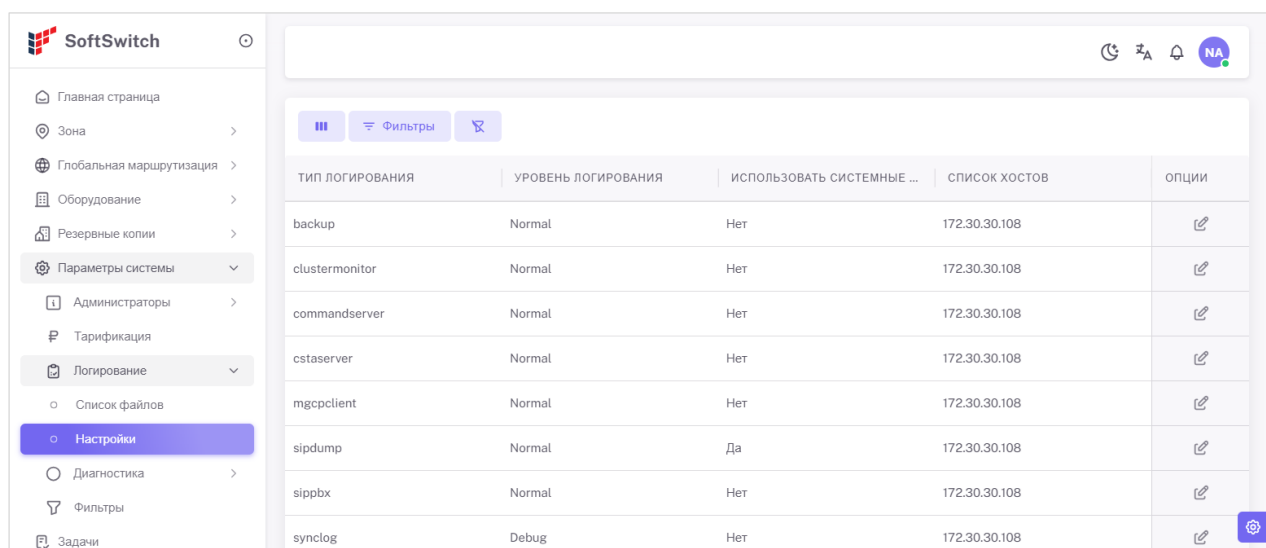



Рисунок 34. Настройки логирования для ядра SIP SoftSwitch

Список журналов регламентирован – допустимо только изменение текущих настроек.

Таблица 3. Типы журналов

Тип логирования	Назначение
backup	Лог бэкапов.
clustermonitor	Лог обмена с узлами кластера.
commandserver	Лог входящих команд по API.
cstaserver	Лог сервера CSTA.
mgcpclient	Лог обмена с MGCP-сервером. Номера логам присваиваются по ID MGCP-сервера.
sipdump	Лог SIP пакетов.
sippbx	Лог SIP сессий.
synclog	Лог синхронизации в кластере при запуске службы.
tariffication	Лог тарификации.

Для изменения настроек выбранного журнала нажмите значок редактирования  в его строке. После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 35](#)):

Редактировать ×

Тип логирования

Уровень логирования

Использовать системные логи

Добавить хост

Хост 1

Сохранить
Заккрыть

Рисунок 35. Изменение настроек журнала

В форме доступны следующие поля:

Поле	Значение
Тип логирования	Выбор типа логирования.
Уровень логирования	Выбор уровня логирования: <ul style="list-style-type: none"> • Error – выводятся только ошибки. • Normal – выводятся ошибки и информационные сообщения. • Debug – выводятся ошибки, сообщения и информация о стадиях обработки.
Использовать системные логи	Включение отправки событий по протоколу Syslog.
Хост 1/Хост 2/...	IP-адрес сервера Syslog. Может быть указано несколько хостов с помощью кнопки Добавить хост .

Для проверки переключения уровня логирования откройте требуемый журнал. Во время переключения в лог добавится соответствующая запись, а следующие события будут записываться с новым уровнем логирования (см. [Рисунок 36](#)):

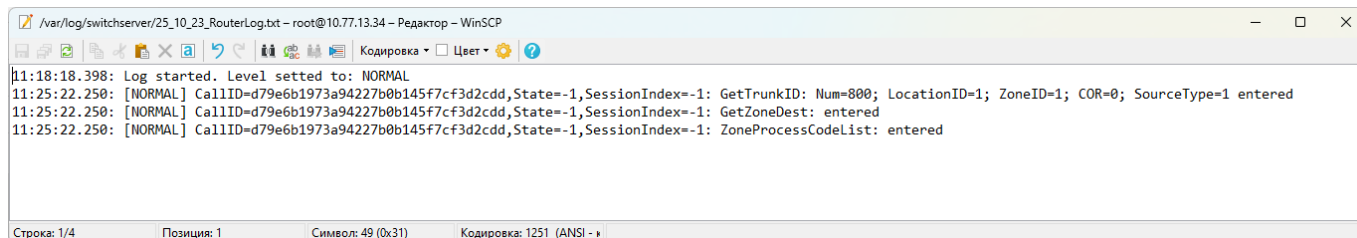


Рисунок 36. Проверка переключения уровня логирования

Важно учесть, что перевод логирования в режим Debug позволяет не только получить максимальную детализацию происходящих событий, но и снижает производительность системы, излишне нагружая ее. Кроме этого, журналы в режиме Debug расходуют много места в системе хранения.



Рекомендуется снижать уровень логирования после настройки системы.

Дополнительные настройки логирования описываются параметрами в разделе **[General]** файла `/opt/flat/fss-server/settings.ini`:

LogSizeLimit=2048M – ограничение размера всех логов системы;

SysLogLevel=normal – ограничение максимального уровня детализации событий при отправке по Syslog, по умолчанию normal. Допустимы значения error, normal, debug. Применение: в Syslog будут отправляться события с детализацией, заданной уровнем логирования в свойствах журнала, но не выше указанного в параметре **SysLogLevel**.

10.3.3.2. Список файлов журналов

Для управления журналами событий ядра системы выберите меню **Параметры системы/Логирование/Список файлов**. После чего в окне отобразится список сохраненных логов с указанием пути к файлу, названия файла, его размера и времени модификации (см. [Рисунок 37](#)):

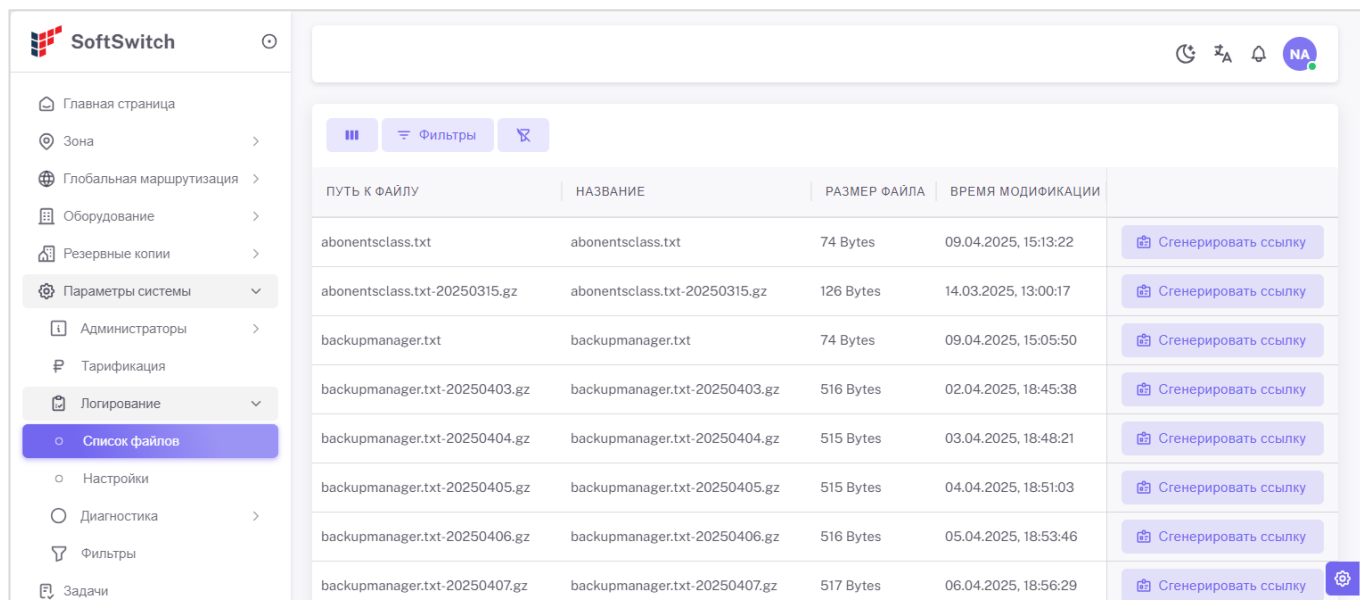


Рисунок 37. Список логов ядра системы

Для скачивания выбранного журнала событий вначале нажмите кнопку [Сгенерировать ссылку](#) в его строке, а затем кнопку [Скачать файл](#), после чего файл будет загружен в папку по умолчанию ПК текущего пользователя.

10.3.4. Диагностика

10.3.4.1. Тест маршрута

Для анализа маршрутизации вызовов выберите меню **Параметры системы/Тест маршрута**, затем в открывшемся окне введите параметры маршрута. После отправки данных на экран будет выведен результат проверки маршрута (см. [Рисунок 38](#)):

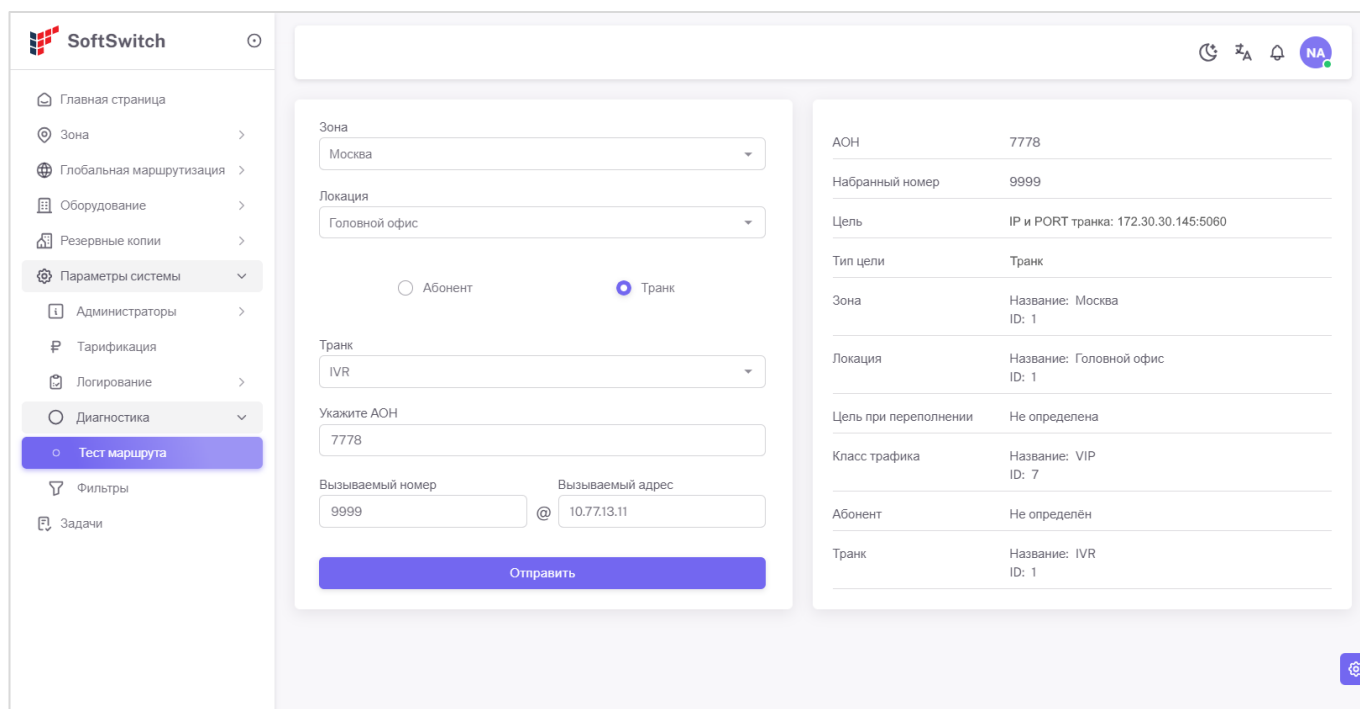


Рисунок 38. Тест маршрута

10.3.5. Фильтры

Для доступа к сохраненным фильтрами выберите меню **Параметры системы/Фильтры**, после чего в окне отобразится свернутый список с названием разделов интерфейса, в которых эти сущности были созданы (см. [Рисунок 39](#)).

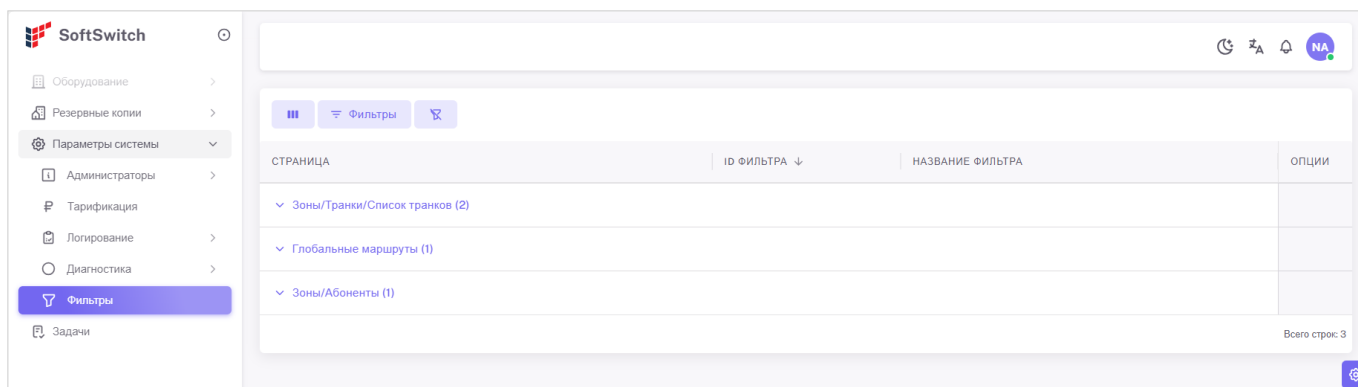


Рисунок 39. Список разделов фильтров

Для просмотра списка сохраненных фильтров разверните интересующий раздел (см. [Рисунок 40](#)):

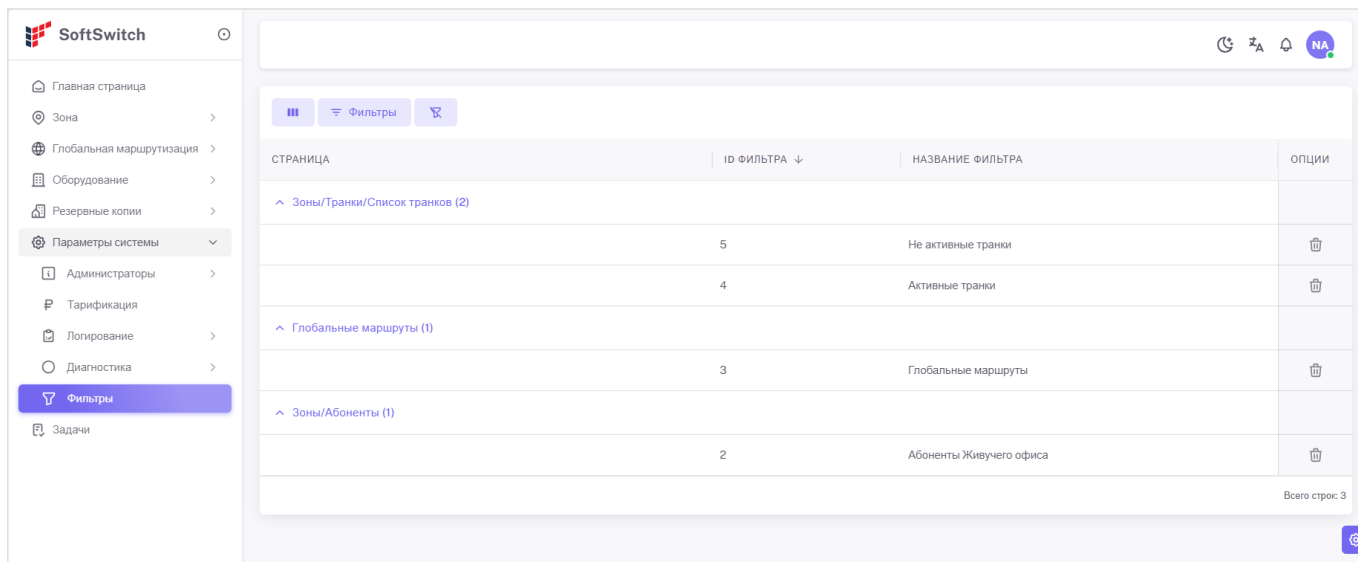


Рисунок 40. Список сохраненных фильтров

В этой части интерфейса возможно только удаление сохраненных фильтров с помощью кнопки . Создание и сохранение фильтров возможно в каждом отдельном разделе меню. Так же см. [Взаимодействие с пользовательским интерфейсом](#).

10.4. Зона

В начале настройки системы ФЛАТ SoftSwitch необходимо определиться с конфигурацией зон и локаций. Если в организации нет разветвленной сети офисов, либо количество абонентов не превышает комфортный для локального администрирования порог, рекомендуется использовать только одну зону, внутри которой необходимо создать хотя бы одну локацию.

Раздел интерфейса **Зона** предназначен для управления всеми относящимися к зоне сущностями, такими как, локации, абоненты, транки, группы, и т.д.

10.4.1. Создание зон

Создание зон рассматривается в главе *Зоны* раздела *Глобальная маршрутизация*.

10.4.2. Создание локаций

После создания новой зоны в ней необходимо создать локацию. Для этого перейдите в меню **Зона/Локации** и в раскрывающемся списке выберите ранее созданную зону. Ниже в окне отобразится список локаций этой зоны (см. *Рисунок 41*):

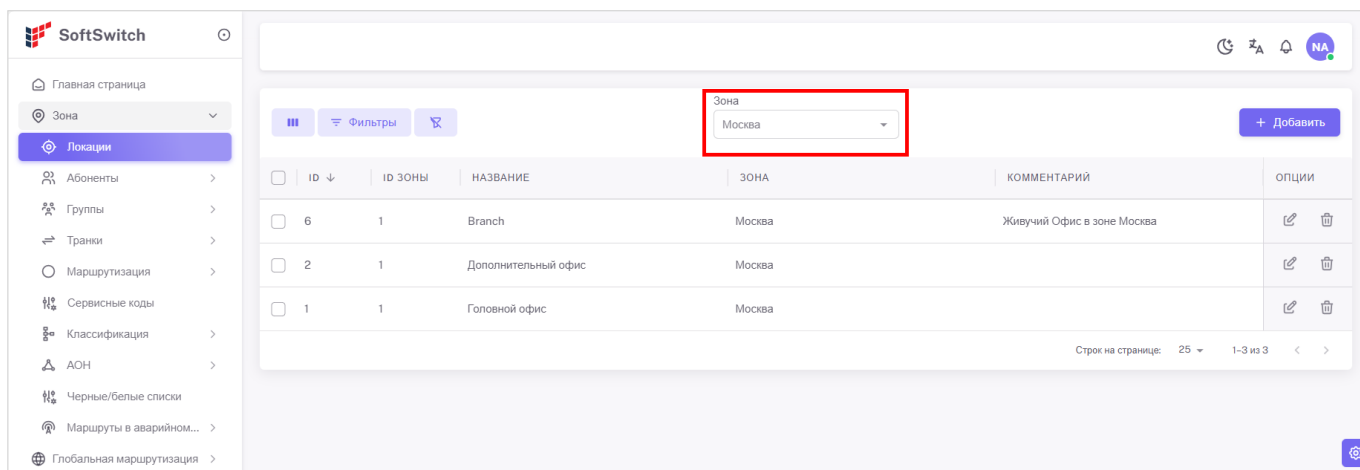


Рисунок 41. Список локаций зоны Москва

10.4.2.1. Вкладка «Основные»

Для создания новой локации нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего в поля открывшейся формы внесите ее название и краткое описание (см. *Рисунок 42*):

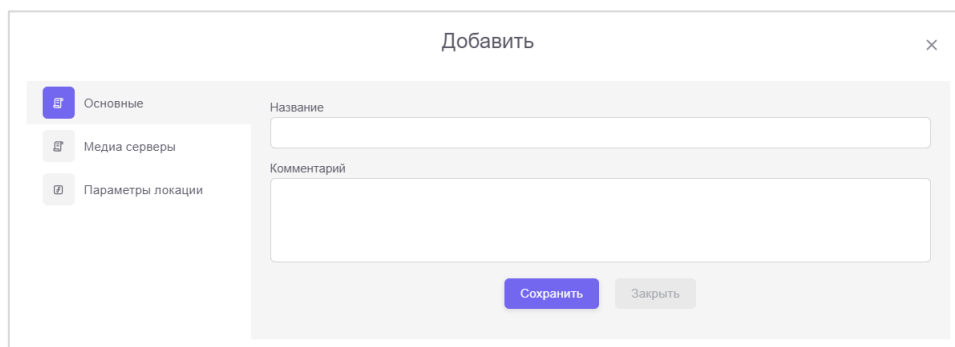


Рисунок 42. Вкладка «Основные»

После сохранения локации станут доступны для редактирования вкладки **Медиа серверы** и **Параметры локации**.

10.4.2.2. Вкладка «Медиасерверы»

На вкладке **Медиасерверы** доступна привязка медиаресурсов выбранной локации. Создание медиаресурсов рассматривается в отдельном разделе ([Медиасерверы](#)).

В области формы **Выбранные медиасерверы** отображается список привязанных медиаресурсов, а в области **Все медиасерверы** – список медиаресурсов текущей зоны, доступных к распределению (см. [Рисунок 43](#)):

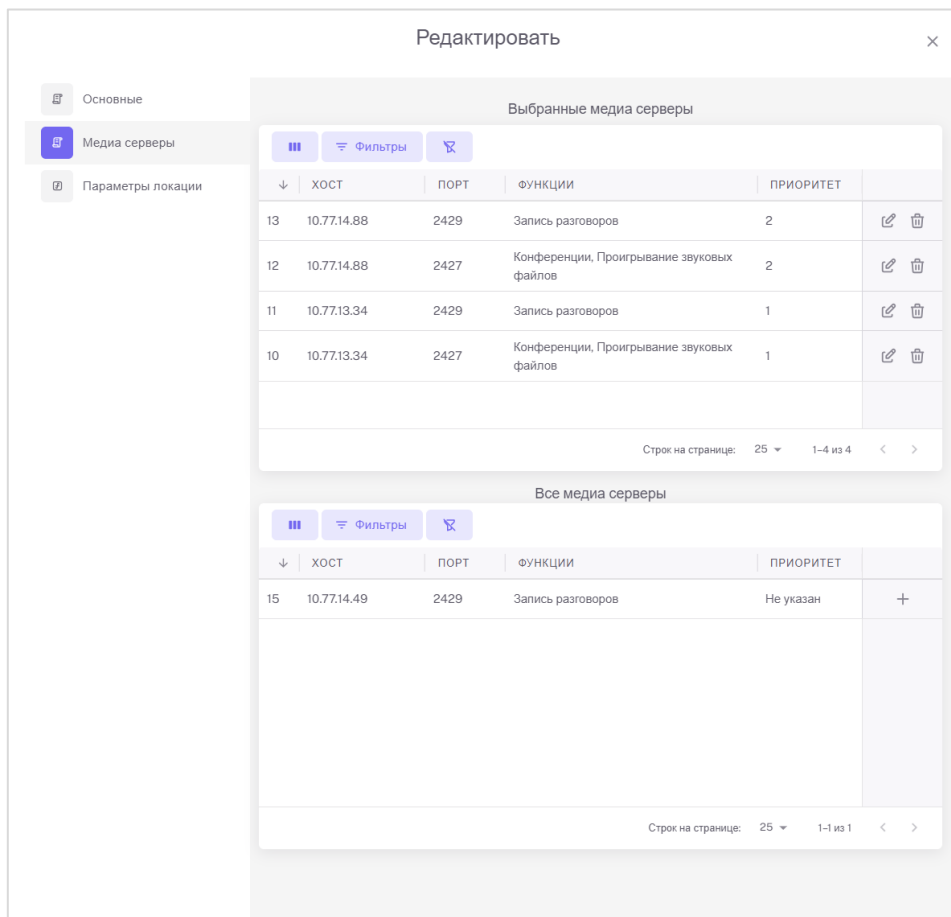


Рисунок 43. Вкладка «Медиасерверы»

Для привязки выбранного медиаресурса нажмите кнопку **+**, в раскрывающемся списке выберите его приоритет и нажмите кнопку **🗑**. Приоритет необходим в случае привязки к локации нескольких медиаресурсов и указывает порядок переключения на новый медиаресурс при недоступности основного. При одинаковом приоритете выбирается первый работающий, а при включенной опции «Балансировка между медиасерверами» – нагрузка распределяется равномерно (описание параметра см. [Вкладка «Параметры локации»](#)).



Один медиаресурс может быть привязан к различным локациям текущей зоны.

К любой локации можно привязать любое количество медиаресурсов.

Отсутствие в локации привязанных медиаресурсов ограничивает применение системы ФЛАТ Запись и ДВО, использующих МОН (Music On Hold).

Для изменения приоритета привязанного медиаресурса нажмите кнопку **✎**, расположенную в его строке, укажите новое значение и сохраните кнопкой **🗑**.

10.4.2.3. Вкладка «Параметры локации»

На вкладке **Параметры локации** доступны включаемые чек-боксом дополнительные параметры, в том числе, назначение пользовательских звуковых файлов вместо стандартных звуковых оповещений (см.

Рисунок 44). Загрузку пользовательских звуковых файлов и их допустимый формат см. в главе Медиасерверы.

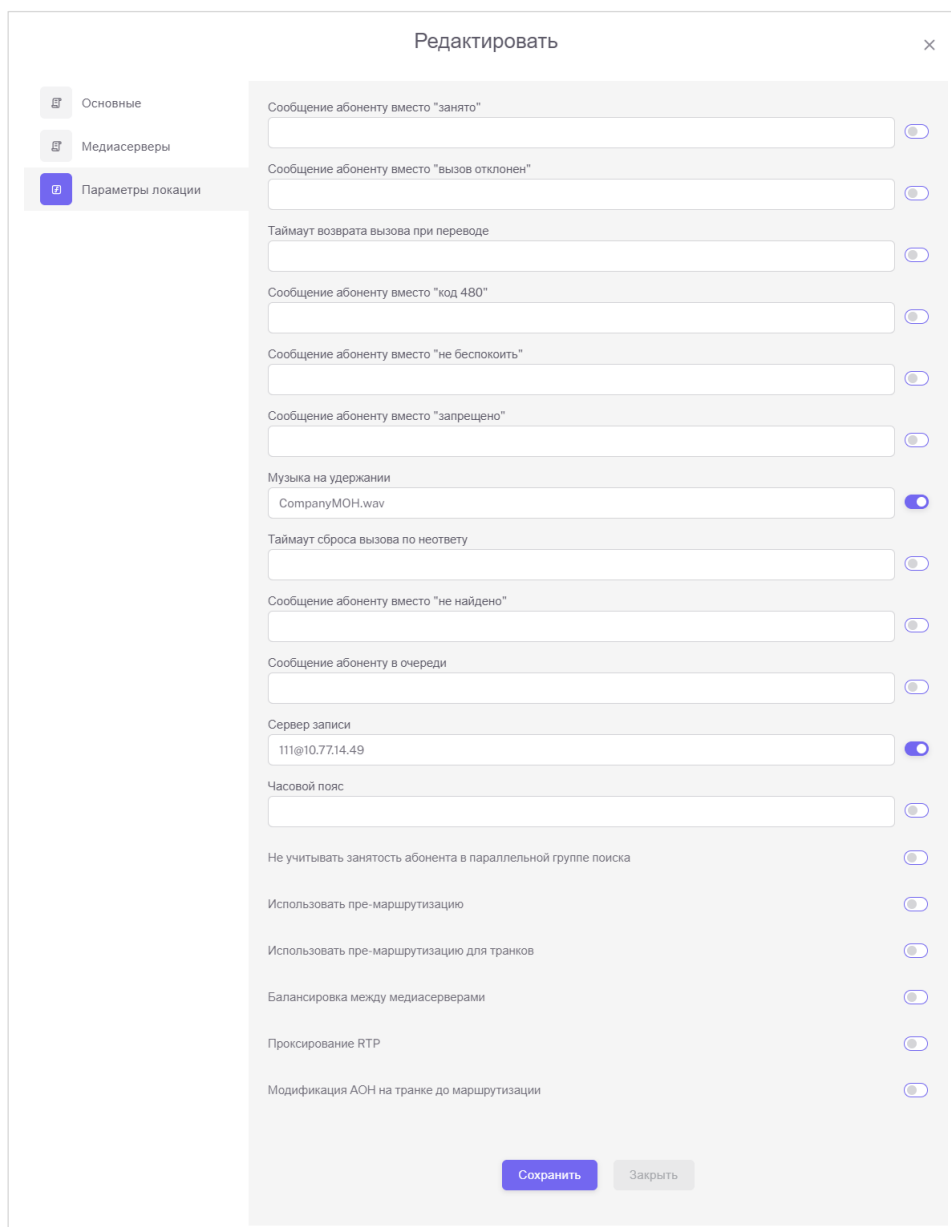


Рисунок 44. Вкладка «Параметры локации»

На вкладке **Параметры локации** доступны следующие поля:

Поле	Значение
Сообщение абоненту вместо «занято»	Имя пользовательского звукового файла с расширением.
Сообщение абоненту вместо «вызов отклонен»	Имя пользовательского звукового файла с расширением.
Тайм-аут возврата вызова при переводе	Тайм-аут возврата вызова при переводе в секундах. Параметр по умолчанию 60 секунд.
Сообщение абоненту вместо «код 480»	Имя пользовательского звукового файла с расширением.
Сообщение абоненту вместо «не беспокоить»	Имя пользовательского звукового файла с расширением.

Поле	Значение
Сообщение абоненту вместо «запрещено»	Имя пользовательского звукового файла с расширением.
Музыка на удержании	Имя пользовательского звукового файла с расширением.
Тайм-аут сброса вызова по неответу	Тайм-аут сброса вызова по неответу в секундах. Параметр по умолчанию 60 секунд.
Сообщение абоненту вместо «не найдено»	Имя пользовательского звукового файла с расширением.
Сообщение абоненту в очереди	Имя пользовательского звукового файла с расширением.
Сервер записи	<p>Номер, используемый при обработке ФЛАТ Запись медиатрафика с АТС различных типов для выбора необходимого скрипта (см. документацию ФЛАТ Запись). По умолчанию – 111.</p> <p>Формат номера:</p> <ul style="list-style-type: none"> • 111@10.77.13.145 – номер и IP-адрес сервера записи. • 111 – указывается только номер. Для этого варианта необходимо настроить маршрутизацию в сторону сервера записи. Использование Направлений целевой маршрутизации позволяет направить медиаданные на разные серверы записи в зависимости от их доступности (см. Направления). <p>При подключении нескольких серверов записи для одновременной обработки медиатрафика их адреса должны указываться через запятую. Пример: «111@10.77.13.145, 111@10.77.13.127», или «111, 222».</p> <p>Исключением является запись телефонных аппаратов Cisco методом «Built in bridge», при котором указывается только один адрес сервера записи. Включение метода см. Вкладка «Параметры абонента».</p> <p>При записи телефонных аппаратов Cisco через Медиасервер (включение – поле Запись Cisco ВІВ через MGCP, Вкладка «Параметры абонента») допустимо указывать несколько серверов записи.</p>
Часовой пояс	Указывается часовой пояс локации в формате +/-hh:mm. Например, для Москвы «+03:00».
Не учитывать занятость абонента в параллельной группе поиска.	<p>Включается возможность для ТА с несколькими SIP-линиями при ответе на вызов, поступивший из одной группы поиска, принять второй вызов из другой группы поиска.</p> <p>Необходимо учитывать ограничение количества входящих вызовов, настраиваемое в параметрах абонента (см. Вкладка «Параметры абонента»).</p>
Использовать пре-маршрутизацию	<p>Включение пре-маршрутизации для вызовов, поступающих от абонентов из локации. В этом случае, перед маршрутизацией вызова происходит поиск совпадений в локальной базе абонентов, и при его нахождении вызов переключается на абонента. При отключенной опции вызов направляется на первичную маршрутизацию.</p> <p>Пример. При постепенном переключении абонентов со старой АТС на новый ФЛАТ SoftSwitch включение пре-маршрутизации позволит сразу направить вызов на абонента минуя маршрутизацию.</p>

Поле	Значение
Использовать пре-маршрутизацию для транков	Включение пре-маршрутизации для вызовов, поступающих с транков, относящихся к локации. В этом случае, перед маршрутизацией вызова происходит поиск совпадений в локальной базе абонентов, и при его нахождении вызов переключается на абонента. При отключенной опции вызов направляется на первичную маршрутизацию. Пример. При постепенном переключении абонентов со старой АТС на новый ФЛАТ SoftSwitch включение пре-маршрутизации позволит сразу направить вызов на абонента минуя маршрутизацию.
Балансировка между медиасерверами	Включение балансировки между медиасерверами при указании у них одинакового приоритета. Так же см. Вкладка «Медиасерверы» .
Проксирование RTP	Включение проксирования RTP-трафика. В обычном режиме телефоны передают RTP-трафик напрямую друг другу.
Модификация АОН на транке до маршрутизации	Включение модификации АОН перед выполнением проверки вызовов на соответствие правилам целевой маршрутизации.

10.4.3. Абоненты

Раздел предназначен для управления абонентами и их профилями.

10.4.3.1. Список абонентов

Для управления абонентами выберите меню **Зона/Абоненты/Список абонентов**, после чего в окне отобразится список учетных записей с указанием имени и номера абонента, статуса регистрации, присвоенного абонентскому устройству IP-адреса, назначенному профилю, и узлу регистрации (см. [Рисунок 45](#)):

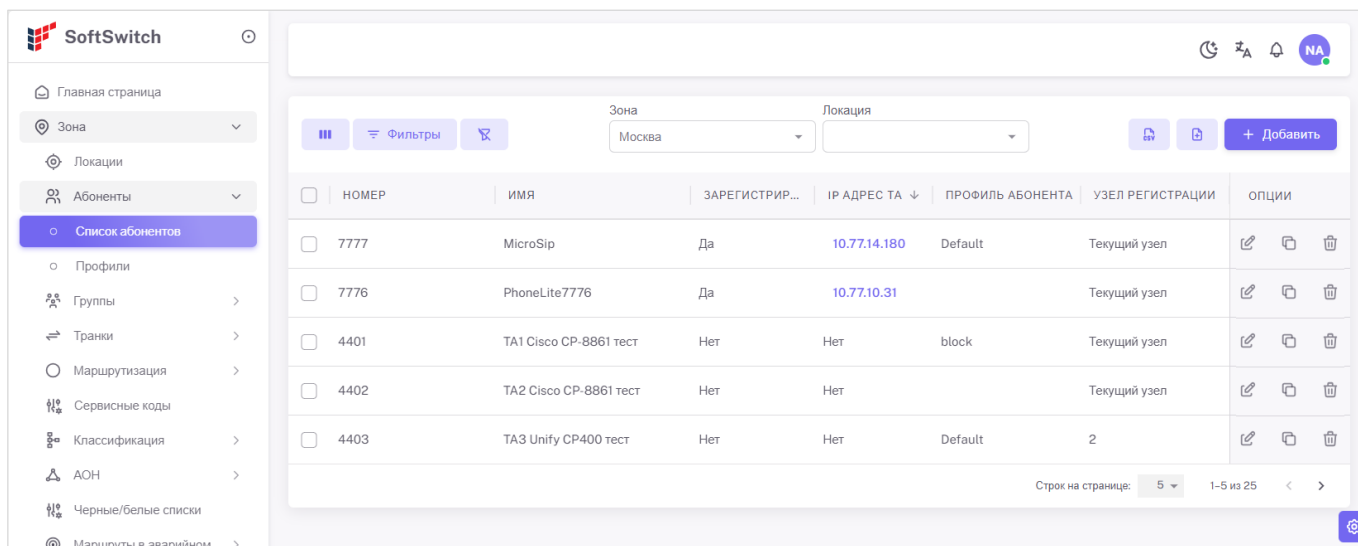


Рисунок 45. Список абонентов

Перед регистрацией новых абонентов удобнее сразу выбрать в раскрывающемся списке в верхней части окна зону и локацию принадлежности абонента, тогда не придется их указывать при редактировании его учетных данных.

В столбце **Узел регистрации** указывается нода регистрации абонента (текущий узел/удаленный узел) при построении отказоустойчивой системы ФЛАТ SoftSwitch на базе двух объединенных в кластер серверов.

10.4.3.1.1. Вкладка «Свойства абонента»


Для создания нового абонента нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите учетные данные и его параметры (см. [Рисунок 46](#) и [Рисунок 47](#)):

Рисунок 46. Вкладка «Свойства абонента». Часть 1

Рисунок 47. Вкладка «Свойства абонента». Часть 2

В форме доступны следующие поля:

Поле	Значение
Авторизация в личном кабинете	Включение абоненту доступа к личному кабинету.
Логин	Логин для регистрации абонента в личном кабинете.
Пароль	Пароль для регистрации абонента в личном кабинете.
Имя	Имя абонента.

Поле	Значение
Номер	Номер абонента.
Авторизация SIP	Включение опции авторизации абонентского устройства.
Логин абонента	Логин для авторизации абонентского устройства.
Пароль абонента	Пароль для авторизации абонентского устройства.
Зона	Выбор зоны принадлежности абонента. См. Создание зон .
Локация	Выбор локации принадлежности абонента. См. Создание локаций .
Класс сервиса	Класс сервиса. Применяется для управления маршрутизацией при совершении исходящих вызовов. Создание классов сервиса см. в главе Классы сервиса .
Класс ограничения	Указывается класс ограничения. Применяется для управления маршрутизацией при необходимости запрета вызовов на заданные направления. Создание классов ограничений см. в главе Классы ограничений .
Протокол	Выбор транспортного протокола SIP сигнализации: <ul style="list-style-type: none"> • UDP • TCP • TLS
Множественная регистрация	Включение поддержки регистрации на один номер нескольких телефонных аппаратов. Применяется в случае, когда сотрудникам необходимо зарегистрировать на один номер несколько устройств (в зависимости от выбранной лицензии до 10 регистраций на один номер со стационарных телефонов, либо программных клиентов ФЛАТ Партнер для различных ОС). См. Множественная регистрация .
Запись разговора	Включает для абонента функцию записи разговора.
Описание	Описание абонента (информационное поле).

10.4.3.1.2. Вкладка «Параметры абонента»

На вкладке **Параметры абонента** (см. [Рисунок 48](#) и [Рисунок 49](#)) доступны следующие поля:

Поле	Значение
Обратный вызов	Включение услуги обратного вызова при занятости или неответе вызываемого абонента (см. Сервисные коды и Функция «Обратный вызов»).
Переадресация статус	Включение переадресации вызова. Необходимо указать условия переадресации, номер перевода и дополнительные параметры.
Условия переадресации	Из раскрывающегося списка выбирается признак: <ul style="list-style-type: none"> • Безусловная. • По занятости. • По неответу. При выборе этого параметра форма дополняется полем указания таймаута – задержки перевода вызова. При пустом значении (по умолчанию) таймаут – 10 секунд.

Поле	Значение
	<ul style="list-style-type: none"> По времени. При выборе этого параметра форма дополняется полями выбора дней недели и диапазона времени для переадресации. Учитывается часовой пояс локации абонента.
Переадресация на номер	Указывается номер, на который переводятся вызовы.
Не беспокоить	Включение услуги DND («do not disturb»).
Альтернативный номер	<p>Включение опции альтернативного номера, вызываемого одновременно с основным номером.</p> <p>С помощью кнопки Добавить номер возможно указать несколько альтернативных номеров без ограничения их количества.</p>
E-mail для уведомления о пропущенных вызовах	Включается опция и указывается E-mail абонента, на который будут направляться уведомления о пропущенных вызовах (см. Настройка отправки уведомлений о пропущенных вызовах).
Переадресация при недоступности на номер	<p>Включение переадресации. Указывается номер, на который переводятся вызовы.</p> <p>Коды SIP-ответов при которых происходит переадресация:</p> <ul style="list-style-type: none"> 480 – недоступен; 486 – занято; 603 – отклонен.
Ограничение количества входящих вызовов	Включение опции с указанием ограничения количества одновременных входящих вызовов.
Выключить из групп поиска	<p>Исключение абонента из группы поиска. Фактически абонент остается в группе, но не участвует в распределении вызова.</p> <p>Включение/исключение абонента из группы поиска так же возможно выполнить с телефонного аппарата абонента с помощью ввода сервисного кода (см. Сервисные коды).</p>
Переадресация по Ч/Б списку	Включение переадресации вызова на группу или номер при срабатывании проверки по Ч/Б списку (см. Вкладка «Черные/Белые списки», Черные/Белые списки на уровне зон).
Shared line	<p>Включение опции совместного использования общей линии несколькими телефонными аппаратами Cisco и Yealink (до 50 линий).</p> <p>В дополнительном поле указывается номер общей линии. См. Функция «Shared line».</p> <p>Ответная часть настроек выполняется в ФЛАТ Device Manager для каждого подключаемого телефонного аппарата (см. соответствующий документ).</p>
Серверный BLF	<p>Включение отображения индикаторов BLF для телефонных аппаратов Cisco при включенной опции «Shared line», при которой отключается стандартный механизм индикации BLF.</p> <p>В дополнительном поле указывается номер контролируемого абонента. С помощью кнопки Добавить номер возможно указать несколько таких номеров без ограничения их количества.</p> <p>Ответная часть настроек выполняется в ФЛАТ Device Manager (см. соответствующий документ).</p>

Поле	Значение
	Так же см. <i>Индикация статусов BLF</i> .
Запись Cisco BIB	Включение поддержки записи для телефонных аппаратов Cisco методом Built In bridge (BIB). Адрес сервера записи указывается в настройках локации, на вкладке <i>Вкладка «Параметры локации»</i> , поле Сервер записи .
Запись Cisco BIB через MGCP	Включение записи телефонных аппаратов Cisco через Медиасервер. Необходимо предварительно включить поддержку параметром «Запись Cisco BIB». Адрес сервера записи указывается в настройках локации, на вкладке <i>Вкладка «Параметры локации»</i> , поле Сервер записи .
Безусловная переадресация при вызовах в группу поиска	Включение безусловной переадресации при поступлении вызова через группу поиска.
Авто-выход из групп поиска при отсутствии ответа на вызов	Включение опции.
Функция мобильность Cisco (указать таймаут при возврате вызова)	Включение опции с указанием таймаута. При включенной опции «Альтернативный номер» и при завершении вызова, выполненного с альтернативного номера, появляется возможность в течение указанного таймаута выполнить перехват вызова с основного номера. Ответная часть настроек выполняется в ФЛАТ Device Manager (см. соответствующий документ).
Функция приватности для Cisco	Включение опции ограничивает отображение номера вызываемого абонента на остальных ТА, подключенных к общей линии при использовании Shared line. Ответная часть настроек выполняется в ФЛАТ Device Manager (см. соответствующий документ).

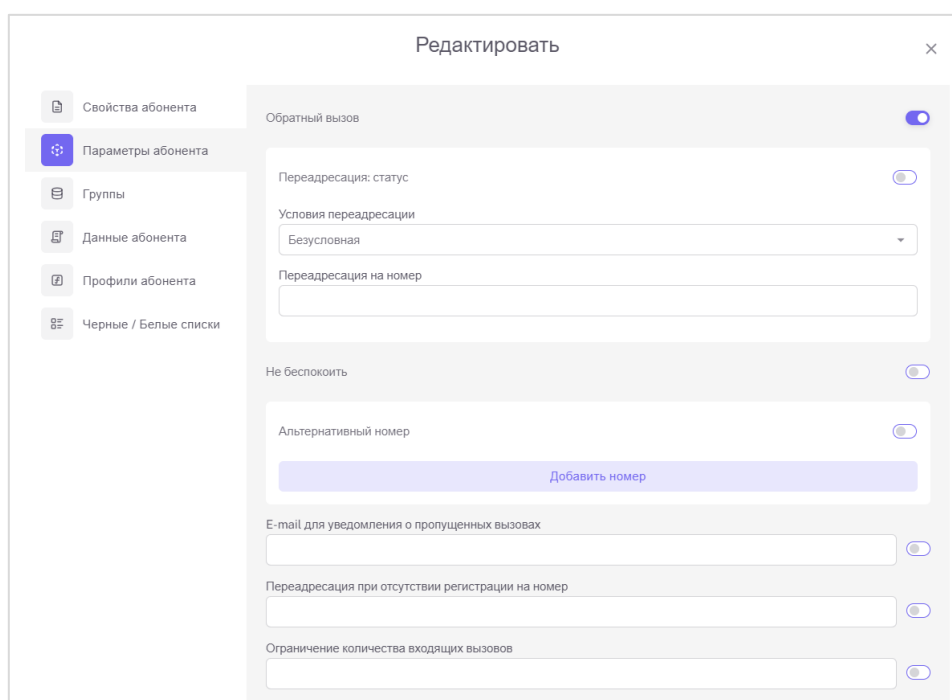


Рисунок 48. Вкладка «Параметры абонента». Часть 1

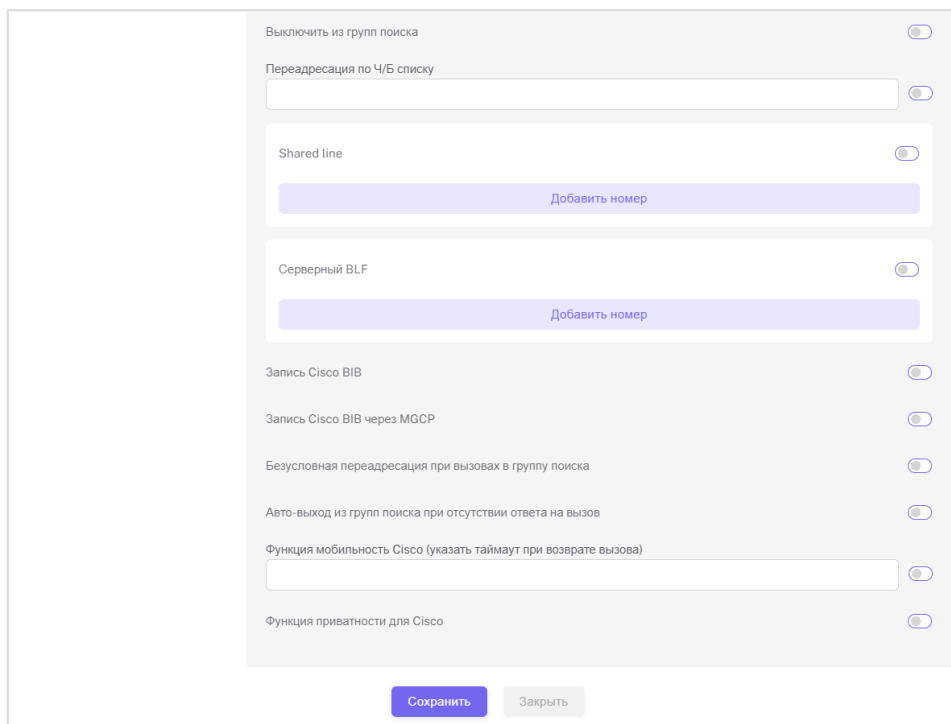


Рисунок 49. Вкладка «Параметры абонента». Часть 2

10.4.3.1.3. Вкладка «Группы»

На вкладке **Группы** приводится информация о принадлежности абонента к группам перехвата и поиска. (см. [Рисунок 50](#)). Назначение и создание групп см. в главе [Группы](#).

В верхней части формы выводится список групп, в которые входит абонент, а в нижней части – список групп выбранной зоны, доступных к распределению.

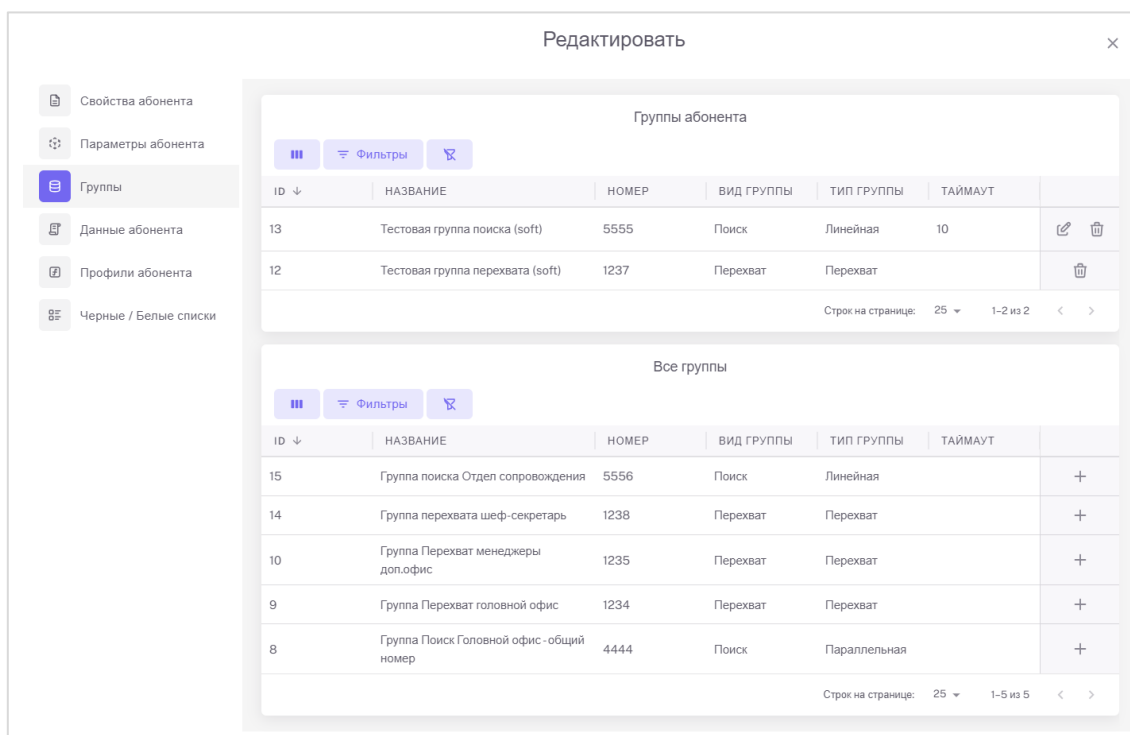


Рисунок 50. Вкладка «Группы»

Для включения абонента в группу нажмите кнопку **+** в строке выбранной группы, а для удаления из группы – кнопку **🗑️**.



Абонент может одновременно входить в несколько групп поиска и одну группу перехвата.

Для группы поиска с помощью кнопки **🕒** устанавливается таймаут ожидания в очереди. См. [Группа поиска](#).

Сохранение изменений состава групп происходит автоматически.

Включение абонента в группу перехвата или поиска также возможно в свойствах группы (см. [Группы перехвата](#) и [Группа поиска](#)).

10.4.3.1.4. Вкладка «Данные абонента»

На вкладке **Данные абонента** приводится статистика по абоненту с указанием учетных данных и технических параметров регистрации (см. [Рисунок 51](#)):

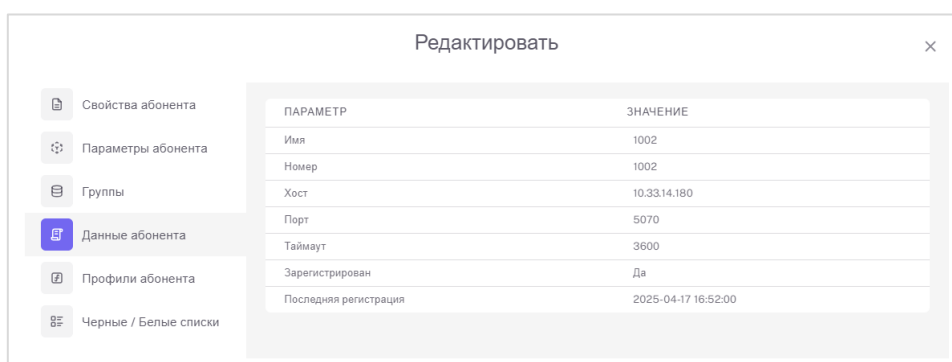


Рисунок 51. Вкладка «Данные абонента»

10.4.3.1.5. Вкладка «Профили абонента»

На вкладке **Профили абонента** происходит назначение абоненту ранее созданного профиля. При выборе профиля на экран выводятся его параметры и перечень входящих функций (см. [Рисунок 52](#)):

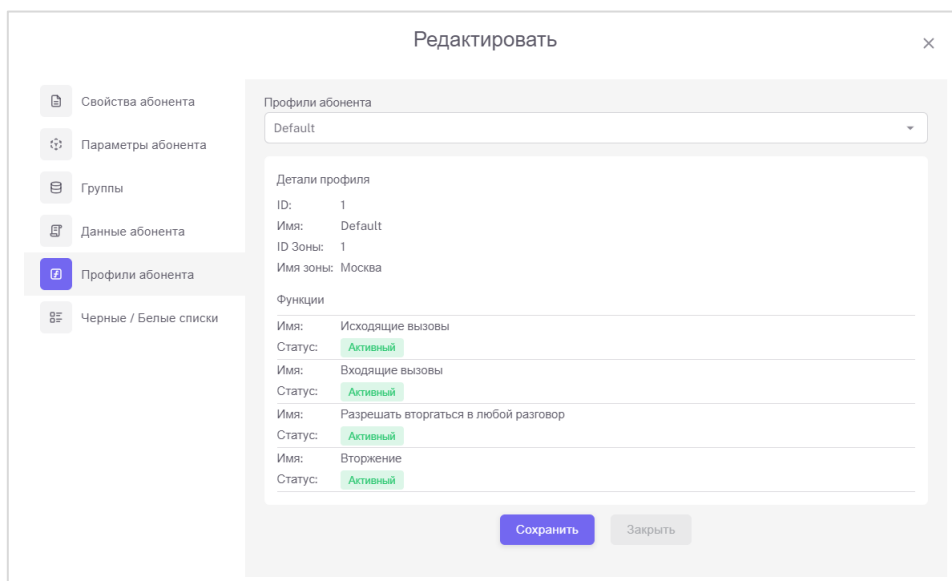


Рисунок 52. Вкладка «Профили абонента»

Настройка профиля, создание списка функций и их применение рассматривается в отдельном разделе (см. [Профиль абонента](#)).

10.4.3.1.6. Вкладка «Черные/Белые списки»

На вкладке **Черные/Белые списки** доступно формирование персональных списков, регулирующих звонки с определенных номеров. Описание функционала см. [Работа с черными/белыми списками](#).

Одновременно может быть включена обработка только одного вида списков – черных или белых. При создании абонента обработка отключена по умолчанию (см. [Рисунок 53](#)).

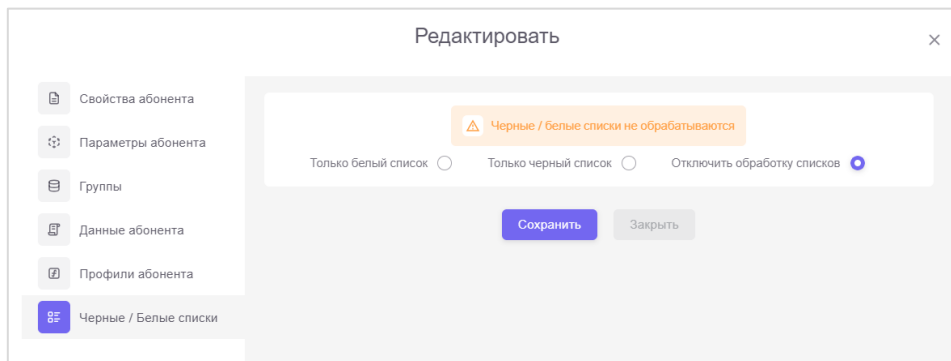


Рисунок 53. Вкладка «Черные/Белые списки»

При включении обработки одного из списков на экране отобразится форма для его формирования (см. [Рисунок 54](#)):

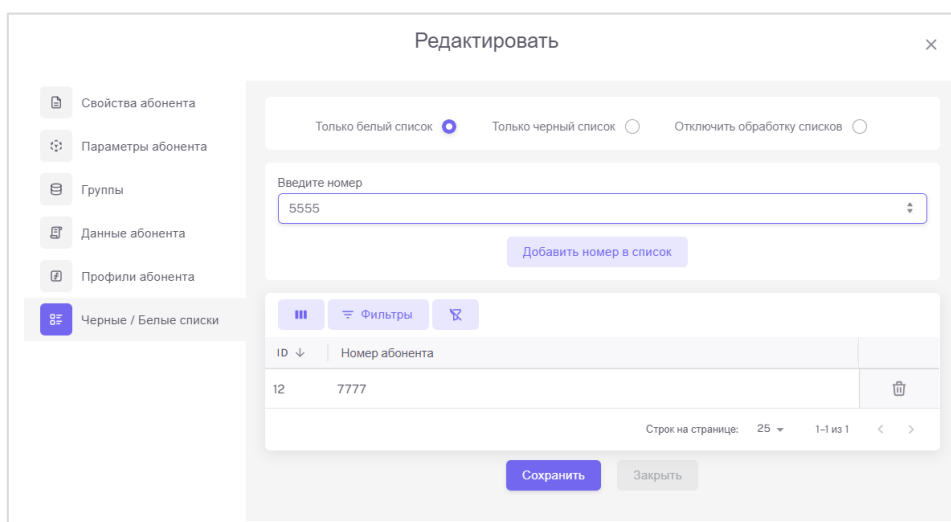


Рисунок 54. Формирование белого списка абонента

Примеры использования черных и белых списков рассматриваются в разделе [Работа с черными/белыми списками](#).

10.4.3.2. Импорт и экспорт абонентов


Список абонентов может быть подготовлен в отдельном файле формата CSV и загружен в систему.



Рекомендуется использовать кодировку Unicode UTF-8 и разделитель значений колонок – символ запятой.

Для загрузки в систему списка абонентов нажмите кнопку , отметьте подготовленный файл и подтвердите выбор. После чего будет сформировано соответствующее задание, результат выполнения которого отразится в разделе [Задачи](#). В качестве шаблона удобно использовать ранее выгруженный список.

При некорректном содержимом импортируемого файла на экран будет выведено сообщение об ошибке.

Для сохранения всех абонентов ФЛАТ SoftSwitch в файл формата CSV нажмите кнопку , после чего будет сформировано соответствующее задание, результат выполнения которого отразится в разделе [Задачи](#).



У абонентов с включенной опцией «Авторизация по логин/пароль» (см. [Вкладка «Свойства абонента»](#)) в экспортируемый файл будут выгружены их логины и пароли в открытом виде.

10.4.3.3. Поиск абонентов в глобальном списке

Поиск абонентов в глобальном списке рассматривается в разделе [Все абоненты](#).

10.4.3.4. Профиль абонента

ФЛАТ SoftSwitch позволяет объединять в профили набор параметров, которые можно назначить абоненту или списку абонентов. Это позволяет гибко настраивать допустимый абонентам функционал.

Для управления профилями выберите меню **Зона/Абоненты/Профили** и укажите в раскрывающемся списке зону, после чего в окне отобразятся ранее сформированные сущности (см. [Рисунок 55](#)):

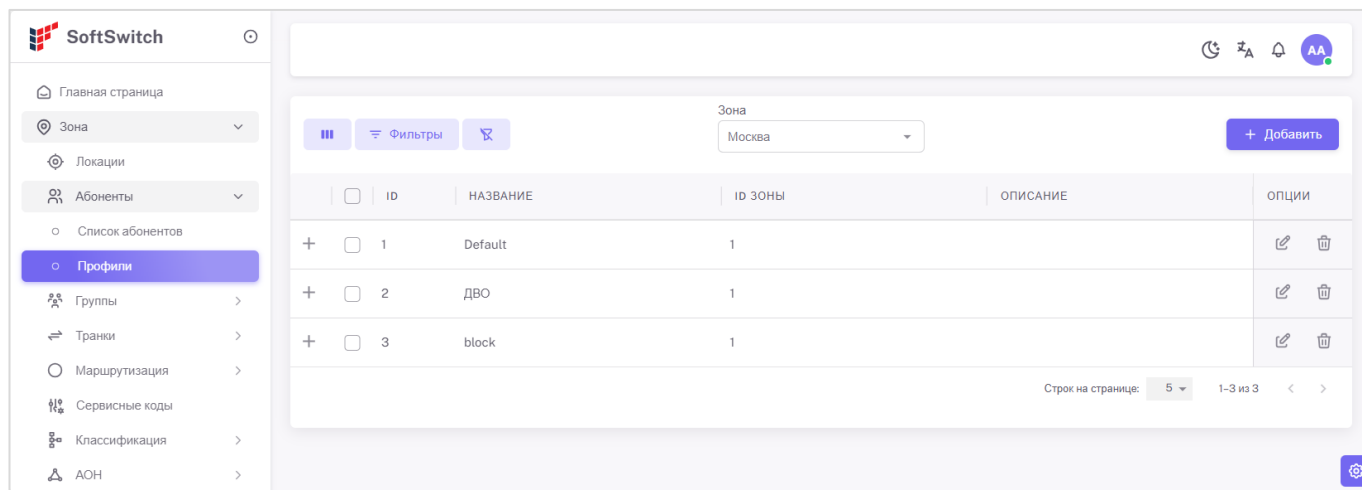



Рисунок 55. Список сформированных профилей

Для создания нового профиля нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы на вкладке **Основные** внесите название профиля и описание. После сохранения изменений станет доступна вкладка **Функции** (см. [Рисунок 56](#)):

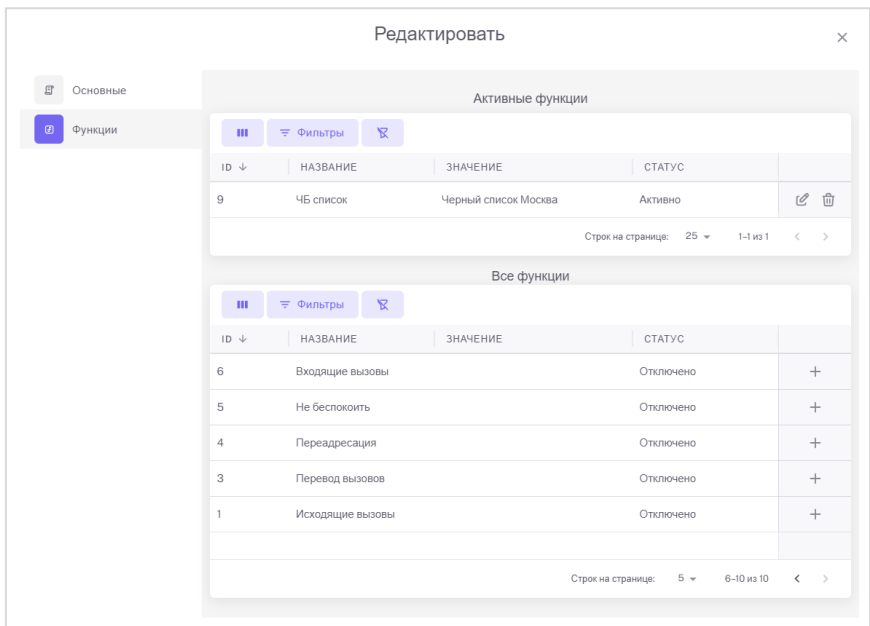


Рисунок 56. Параметры профиля, вкладка «Функции»

В области формы **Активные функции** отображается список включенных в профиль функций с указанием названия, описания и статуса активности, а в области **Все функции** – список функций, доступных к распределению.

Для включения функции в профиль нажмите кнопку **+**, а для удаления из профиля – кнопку **🗑**. У включенной в профиль функции появляется возможность с помощью кнопки **📝** установить ее статус – активна или отключена.

Сохранение изменений состава профиля происходит автоматически.

Для назначения доступны следующие функции:

ID	Название	Значение
1	Исходящие вызовы	Разрешение исходящих вызовов.
3	Перевод вызовов	Разрешение перевода вызовов.
4	Переадресация	Разрешение переадресации вызова.
5	Не беспокоить	Разрешение включения режима «не беспокоить».
6	Входящие вызовы	Разрешение входящих вызовов.
7	Вторжение	Разрешение вторжения в разговор.
8	Разрешать вторгаться в любой разговор	Разрешение вторжения в любой разговор. Более высокий уровень возможностей по отношению к предыдущей функции. Предварительно должна быть включена опция « Вторжение »
9	ЧБ список	Включение в профиль проверки входящих вызовов на принадлежность к черным и белым спискам.
11	Вторжение в режиме конференции	Разрешение вторжения в разговор в режиме конференции. Предварительно должна быть включена опция « Вторжение ».
12	Выбрать способ уведомления в группе перехвата (CISCO)	Выбор способа уведомления о вызове в группе перехвата: <ul style="list-style-type: none"> • Звуковое уведомление; • Визуальное уведомление; • Звуковое и визуальное уведомление; • Уведомление выключено.

ID	Название	Значение
13	Отключить BLF уведомление early	Отключение раннего (early) уведомления на BLF о статусе линии до ответа на вызов. Пример. Вызов поступает в группу поиска в режиме параллельная. Функция выключена. У всех участников группы отображается BLF-статус «занято» до ответа на вызов одним из участников. Функция включена. У всех участников группы BLF-статус «свободно», BLF-статус «занято» отобразится только у принявшего вызов.

10.4.3.4.1. Модель разрешений

При применении профиля активируется модель разрешений, в которой по умолчанию все запрещено. Если применен пустой профиль, либо в профиль добавлены функции с признаком «Выкл.», то абоненту никакие функции недоступны.

При применении профиля, в который добавлены функции с различными признаками («Вкл.»/«Выкл.»), абоненту будут доступны только включенные функции.

Примеры реализации функции вторжения рассматриваются в главе [Применение профиля абонента](#).

Примеры проверки входящих вызовов на принадлежность к черным и белым спискам рассматриваются в главе [Работа с черными/белыми списками](#).

10.4.4. Группы

В системе ФЛАТ SoftSwitch предусмотрены два вида групп – группы перехвата и группы поиска.

10.4.4.1. Группы перехвата

Группы перехвата предназначены для приема входящего вызова, предназначенного другому абоненту. Перехват возможен только внутри сформированной группы, количество таких групп на платформу не ограничено.



Абонент может входить только в одну группу перехвата.

Для управления группами перехвата раскройте меню **Зона/Группы/Группы перехвата** и выберите необходимую зону и локацию, после чего в окне отобразится список сформированных групп (см. [Рисунок 57](#)):

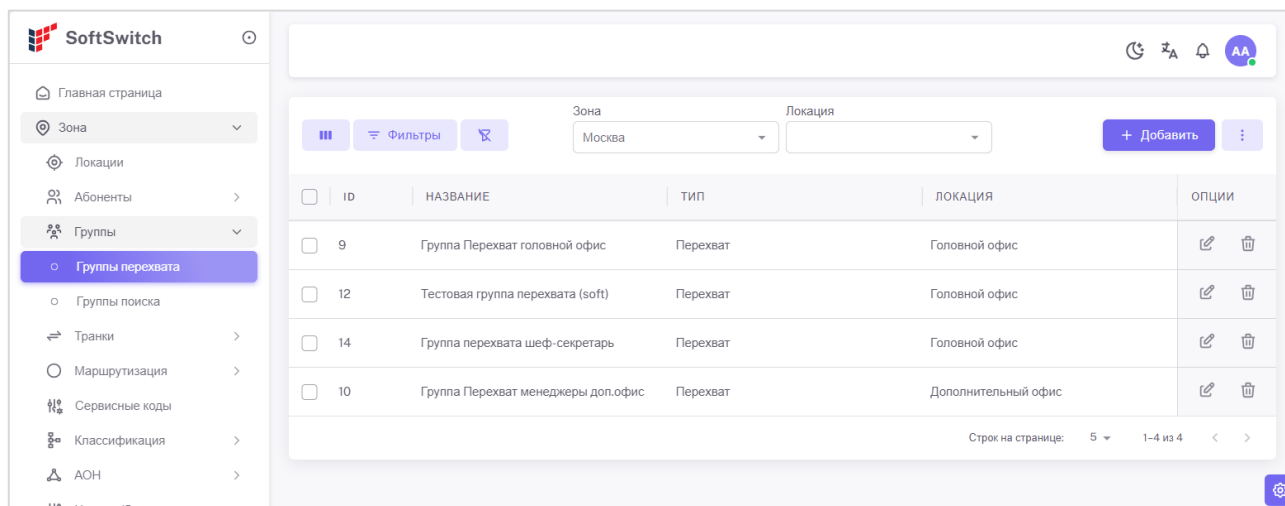



Рисунок 57. Список групп перехвата

Для создания новой группы нажмите кнопку **Добавить**, а для редактирования параметров ранее созданной – значок редактирования . После чего в поля открывшейся формы на вкладке **Основные** внесите название группы и уточните принадлежность к локации текущей зоны (см. [Рисунок 58](#)).

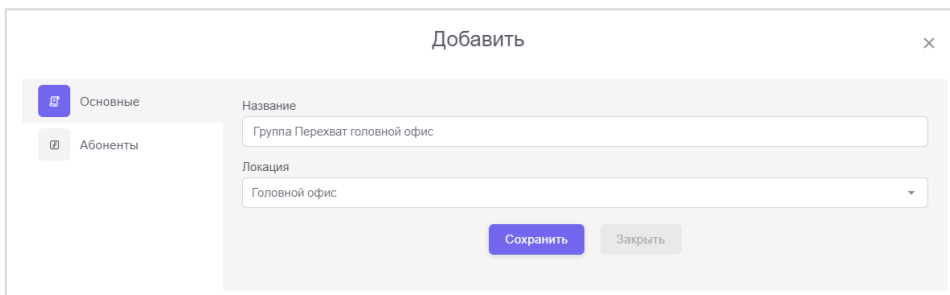
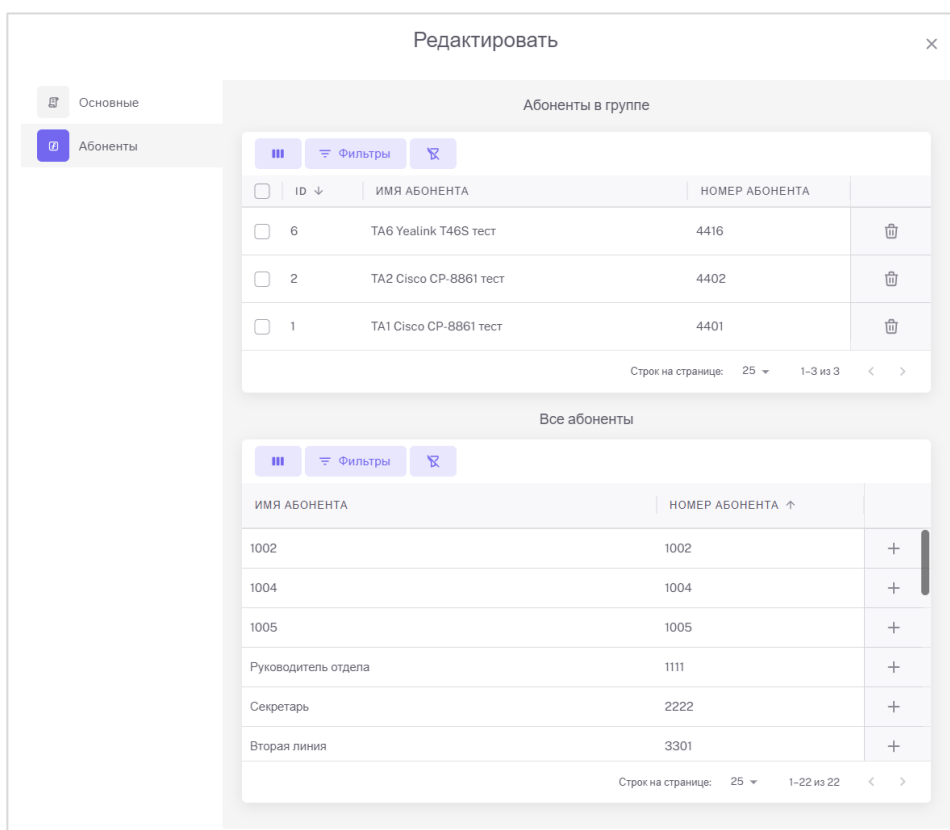


Рисунок 58. Создание группы перехвата. Вкладка «Основные»

После сохранения группы станет доступна вкладка **Абоненты** (см. [Рисунок 59](#)):



ID	ИМЯ АБОНЕНТА	НОМЕР АБОНЕНТА
6	TA6 Yealink T46S тест	4416
2	TA2 Cisco CP-8861 тест	4402
1	TA1 Cisco CP-8861 тест	4401


ИМЯ АБОНЕНТА	НОМЕР АБОНЕНТА
1002	1002
1004	1004
1005	1005
Руководитель отдела	1111
Секретарь	2222
Вторая линия	3301

Рисунок 59. Свойства группы перехвата. Вкладка «Абоненты»

В области формы **Абоненты в группе** отображается список входящих в группу абонентов, а в области **Все абоненты** – список абонентов выбранной зоны, доступных к распределению.



Объединение в группы допустимо только для абонентов локаций текущей зоны. Абоненты из других зон не будут отображаться во вкладке.

Для включения абонента в группу нажмите кнопку **+**, а для удаления из группы – кнопку . Сохранение изменений состава группы происходит автоматически.

Включение абонента в группу также возможно в свойствах абонента на вкладке **Группы** (см. [Вкладка «Группы»](#)).

После создания группы перехвата и добавления в нее абонентов необходимо создать сервисный код (префикс перехвата вызова), при наборе которого абонент может перехватить вызов, адресованный другому

абоненту в группе. Если клиентское устройство поддерживает подписку на уведомления о входящих вызовах в группе перехвата, то данный сервисный код необходимо указать в его настройках. Префикс перехвата вызова задается отдельно для каждой и рассматривается в отдельном разделе (см. [Сервисные коды](#)).

Примеры использования групп перехвата рассматриваются в отдельном разделе (см. [Применение групп перехвата](#)).

10.4.4.2. Группа поиска

Группа поиска предназначена для перенаправления входящего вызова на других абонентов внутри группы согласно выбранному режиму. При поступлении вызова в группу система перенаправляет его свободному абоненту в соответствии с предварительно запрограммированным типом поиска. Предопределены следующие режимы группы поиска:

- **Линейная** — поиск свободного абонента происходит в порядке очередности его вхождения в группу. Если первый участник группы освободился, новый вызов снова поступит на него. Поиск продолжается по кругу до ответа свободного абонента.
- **Циклическая** — поиск свободного абонента происходит в порядке очередности его вхождения в группу. Каждый новый вызов будет поступать на следующего участника, поиск будет продолжаться по кругу.
- **Параллельная** — входящий вызов поступает одновременно на всех абонентов группы, вплоть до ответа на вызов либо его отбоя.
- **Наиболее свободный** – происходит поиск наиболее свободного участника группы (оператора) со времени последнего завершенного вызова. Если вызов не будет принят, следующий вызов будет направлен на другого участника группы.



Абонент может одновременно входить в несколько групп поиска и одну группу перехвата.

Для управления группами поиска раскройте меню **Зона/Группы/Группы поиска** и выберите необходимую зону и локацию, после чего в окне отобразится список сформированных групп с указанием параметров группы (см. [Рисунок 60](#)):

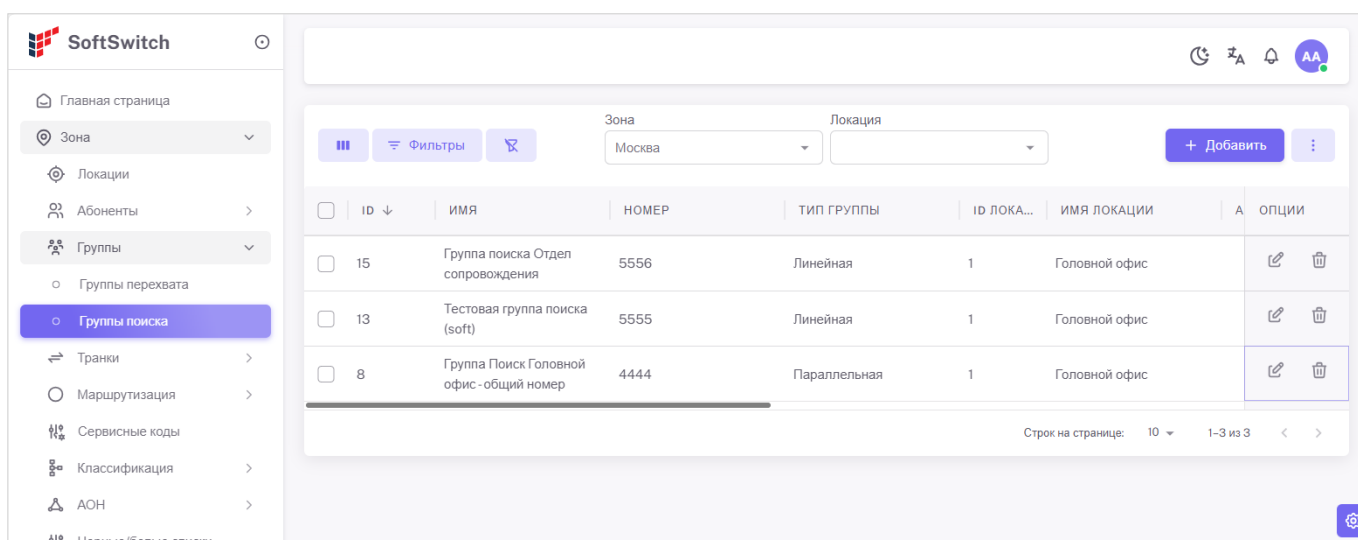


Рисунок 60. Список групп поиска

Для создания новой группы нажмите кнопку **Добавить**, а для редактирования параметров ранее созданной – значок редактирования . После чего в поля открывшейся формы внесите ее параметры (см. [Рисунок 61](#)):

Рисунок 61. Создание группы поиска. Вкладка «Основные»

В форме доступны следующие поля:

Поле	Значение
Название	Имя группы поиска.
Номер	Номер группы поиска. Можно брать из диапазона внутренних абонентских номеров или создать дополнительный диапазон.
Режим	Режим поисковой группы: <ul style="list-style-type: none"> • Линейная. • Циклическая. • Параллельная. • Наиболее свободный (оператор).
Локация	Выбор локации принадлежности группы. См. Создание локаций .
Альтернативный номер	Указывается альтернативный номер. Допустимо указание номера абонента или номера другой поисковой группы. Уточняются условия применения альтернативного номера: <ul style="list-style-type: none"> • При переполнении. • При неответе.
Использовать очередь	Включается использование очереди при поступлении нескольких вызовов в группу поиска. Для звонков, ожидающих в очереди обслуживания, проигрываются настроенные аудио сообщения. Уточняются следующие параметры очереди: <ul style="list-style-type: none"> • Таймаут ожидания в очереди.

Поле	Значение
	<ul style="list-style-type: none"> Максимальное количество ожидающих в очереди.
Контроль группой перехвата	<p>Включается возможность участникам группы перехвата перехватить вызов, пришедший в текущую группу поиска.</p> <p>Указывается группа перехвата.</p>

После сохранения изменений станет доступна вкладка **Абоненты** (см. [Рисунок 62](#)):

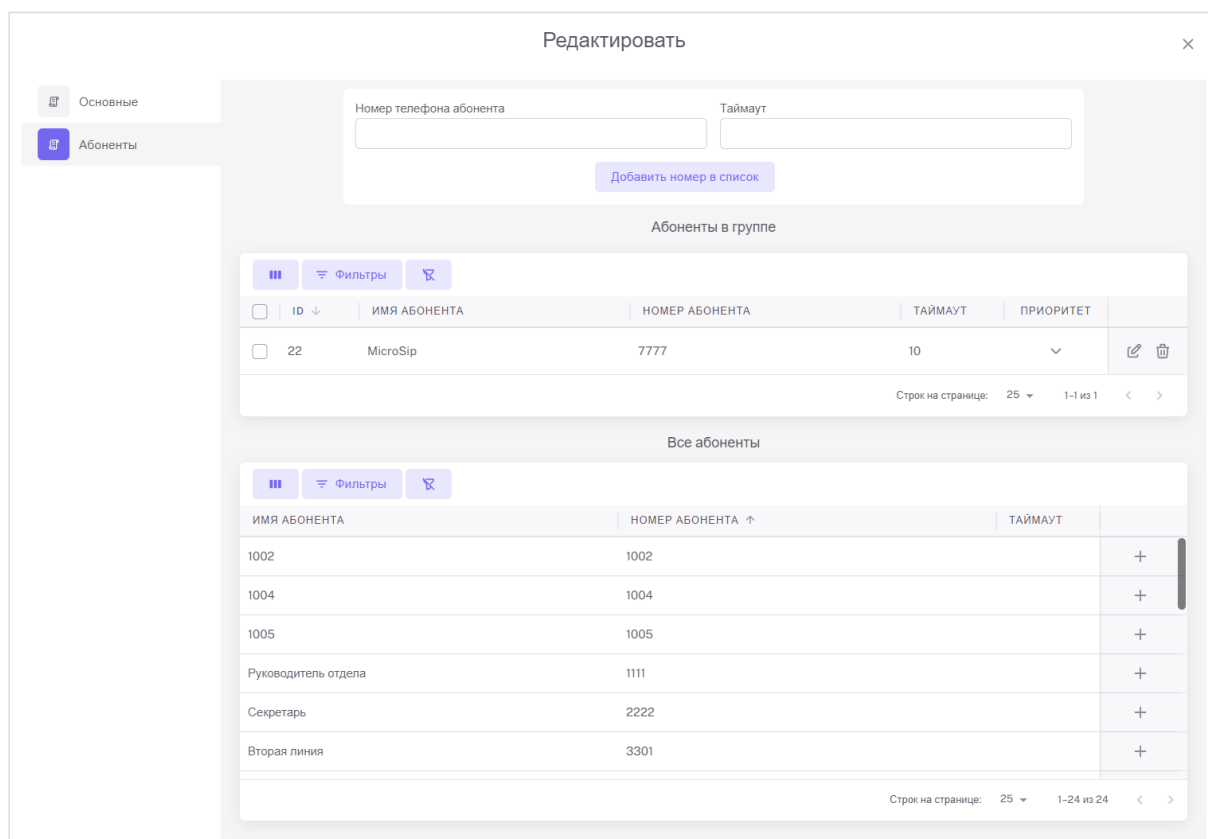


Рисунок 62. Группа поиска, вкладка «Редактирование списка абонентов»

В области формы **Абоненты в группе** отображается список входящих в группу абонентов, а в области **Все абоненты** – список абонентов выбранной зоны, доступных к распределению.



Объединение в группы допустимо только для абонентов локаций текущей зоны. Абоненты из других зон не будут отображаться во вкладке.

Для включения абонента в группу нажмите кнопку **+**, а для удаления из группы – кнопку **🗑**. При включении абонента в группу с помощью кнопки **✎** укажите таймаут – длительность вызова абонента в секундах.

Для включения в группу поиска внешнего абонента укажите его номер, длительность вызова и нажмите кнопку **Добавить номер в список**.

Сохранение изменений состава группы происходит автоматически.

Включение абонента в группу также возможно в свойствах абонента на вкладке **Группы** (см. [Вкладка «Группы»](#)).

10.4.5. Транки

Связать между собой устройства, поддерживающие открытый протокол SIP, возможно с помощью транков.

10.4.5.1. Список транков

Для доступа к настройкам транков выберите меню **Зона/Транки/Список транков**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 63](#)):

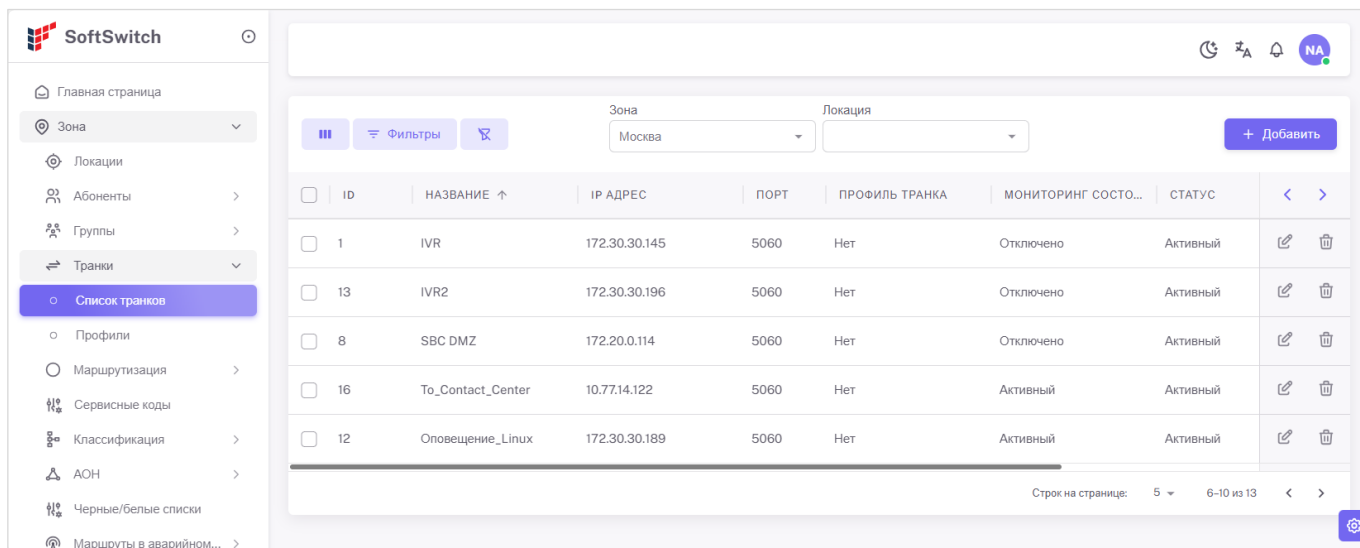


Рисунок 63. Список транков

Перед созданием новых транков удобнее сразу выбрать в раскрывающемся списке в верхней части окна зону и локацию принадлежности транка, тогда не придется их указываться при редактировании его параметров.

10.4.5.1.1. Вкладка «Общие»

Для создания нового транка нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите его параметры (см. [Рисунок 64](#)).

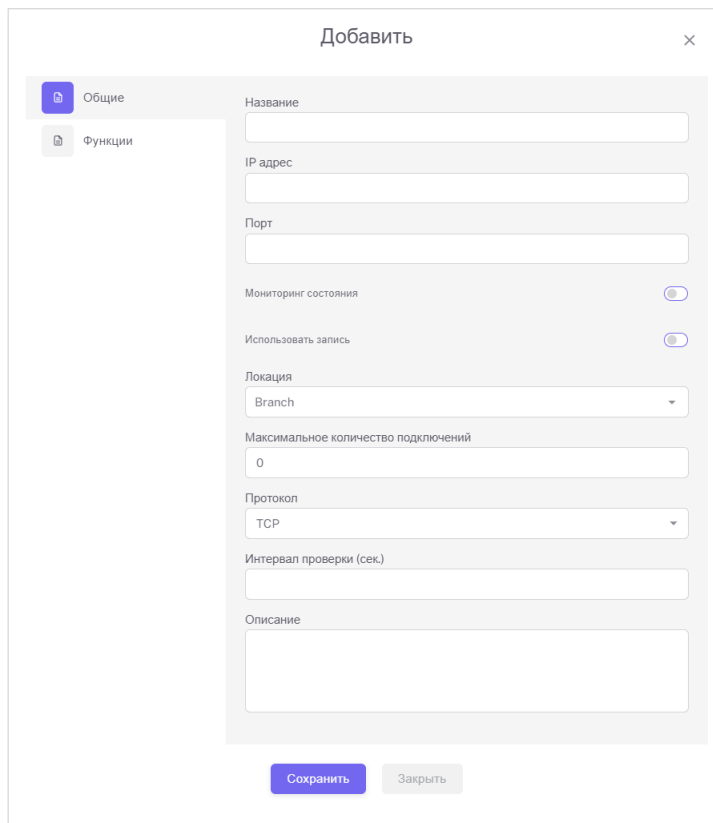


Рисунок 64. Параметры транка, вкладка «Общие»

В форме доступны следующие поля:

Поле	Значение
Название	Название транка.
IP адрес	IP-адрес устройства, на которое создается транк.
Порт	Порт, на который будут отсылаться SIP-сообщения. Порты по умолчанию: UDP/TCP – 5060, TLS – 5061.
Мониторинг состояния	Включение контроля состояния. Во включенном состоянии каждые 5 секунд в транк отправляется сообщение SIP OPTIONS. Ручной интервал проверки задается параметром Интервал проверки (см. ниже в таблице.)
Использовать запись	Включает возможность записи транзитных вызовов.
Локация	Выбор принадлежности транка к определенной локации текущей зоны.
Максимальное количество подключений	Ограничение количества одновременных сессий на направлении. По умолчанию значение 0 – не ограничено.
Протокол	Выбор транспортного протокола SIP сигнализации: <ul style="list-style-type: none"> • UDP • TCP • TLS
Интервал проверки (сек.)	Интервал проверки состояния транка в секундах.
Описание	Описание транка (информационное поле).

После сохранения транка станет доступна для редактирования вкладка **Функции**.

10.4.5.1.2. Вкладка «Функции»

На вкладке **Функции** указывается профиль транка и включается обработка АОН для входящих и исходящих вызовов согласно ранее созданным шаблонам (см. [Рисунок 65](#)). Создание шаблонов обработки АОН рассматривается в разделе [АОН](#).

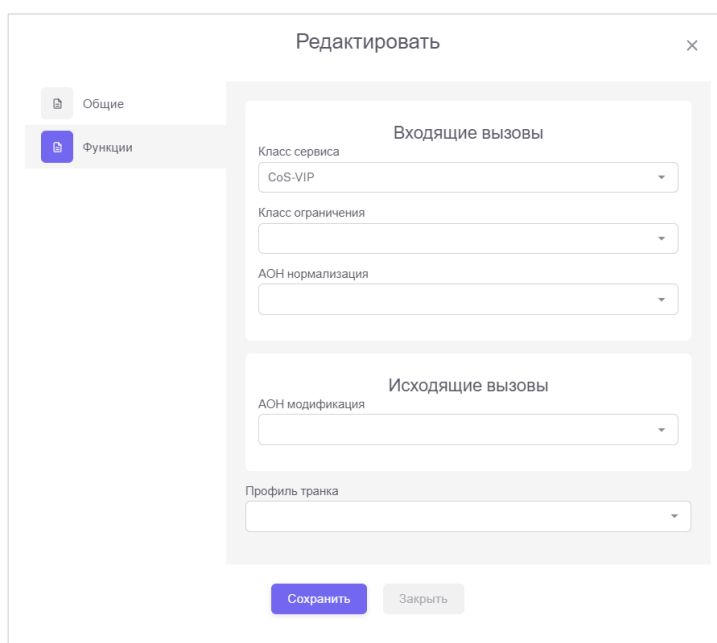


Рисунок 65. Параметры транка, вкладка «Функции»

На вкладке доступны следующие поля:

Поле	Значение
Класс сервиса	Выбор класса сервиса. Применяется для управления маршрутизацией вызовов в зависимости от класса трафика. Создание классов сервиса рассматривается в разделе Классы сервиса .
Класс ограничения	Выбор класса ограничения. Применяется для управления маршрутизацией при необходимости запрета вызовов на заданные направления. Создание классов ограничений рассматривается в разделе Классы ограничений .
АОН нормализация	Выбор шаблона модификаторов. Применяется для модификации номера входящего вызова. Создание шаблонов модификации рассматривается в разделе АОН .
АОН модификация	Выбор шаблона модификаторов. Применяется для модификации номера исходящего вызова. Создание шаблонов модификации рассматривается в разделе АОН .
Профиль транка	Выбор профиля транка. Создание профилей транка рассматривается в разделе Профили .

10.4.5.2. Профили

ФЛАТ SoftSwitch позволяет объединять набор модификаций протокола SIP в профили, которые могут быть назначены транку в его параметрах.

Для доступа к настройкам профилей транков выберите меню **Зона/Транки/Профили**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 66](#)):

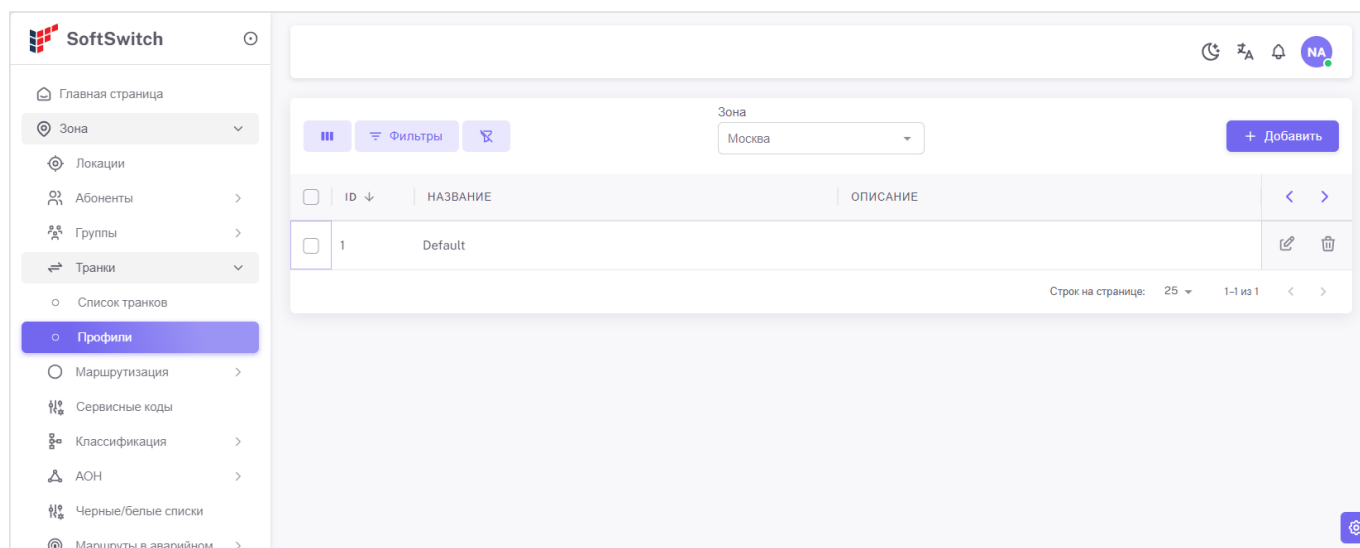


Рисунок 66. Список профилей транков

10.4.5.2.1. Вкладка «Основные»

Для создания нового профиля транка нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите его название и описание (см. [Рисунок 67](#)):

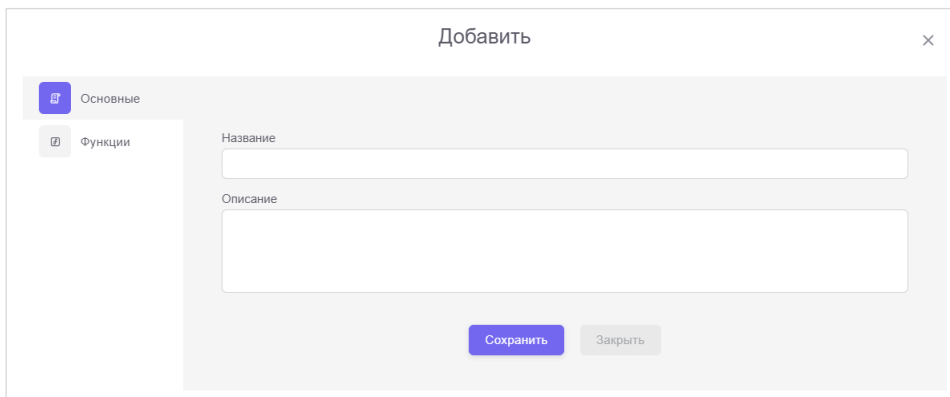


Рисунок 67. Создание профиля транка

После сохранения профиля транка станет доступна для редактирования вкладка **Функции**.

10.4.5.2.2. Вкладка Функции

На вкладке **Функции** в профиль транка добавляются функции модификаций протокола SIP (см. [Рисунок 68](#)):

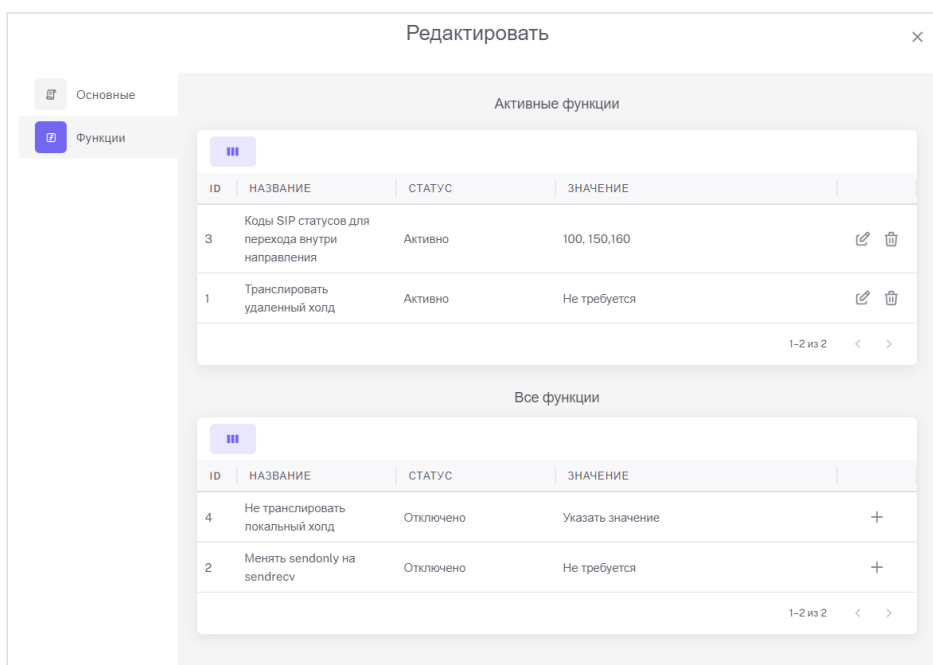


Рисунок 68. Добавление новых функций в профиль транка

В области формы **Активные функции** отображается список входящих в профиль функций, а в области **Все функции** – список функций, доступных к распределению.

Для включения функции в профиль нажмите кнопку **+**, укажите ее параметры и сохраните кнопкой **💾**. Для удаления функции из профиля нажмите кнопку **🗑**.

Для изменения параметров включенной в профиль функции и изменения статуса активности нажмите кнопку **✎**, укажите новое значение и сохраните кнопкой **💾**.

Для назначения доступны следующие функции:

Поле	Значение
Транслировать удаленный HOLD	Опция трансляции в транк удаленной музыки на удержании.
Менять sendonly на sendrecv	Отправка в транк вместо параметра sendonly параметр sendrecv .

Поле	Значение
Коды SIP статусов для перехода внутри направления	<p>Включение перехода на другое направление при ответе на invite.</p> <p>1. Функция выключена – выполняется переход по кодам > 399 исключая статус 487.</p> <p>2. Функция включена – выполняется переход одним из перечисленных диапазонов в формате:</p> <p>код_1 or код_2 or код_n - перечисление списка кодов.</p> <p>код_1 or код_2 till код_n - перечисление списка кодов и задание подмножества кодов через операцию till.</p> <p>Пример 1: 400 till 600 - включает все коды с 400 по 600.</p> <p>Пример 2: 400 till 486 or 488 till 600 – включает все коды с 400 по 600, исключая 487.</p>
Не транслировать локальный HOLD	Отключение трансляции в транк музыки на удержании.
Установить способ согласования	Выбор способа согласования медиа и протоколов в сеансе связи – Early Offer (по умолчанию) или Delay Offer.

10.4.6. Маршрутизация

Маршрутизация телефонных вызовов описывает процесс прохождения вызова на основе исходных данных об источнике вызова, его получателе, классе трафика и цели (см. схему [Общая схема маршрутизации](#)).

Маршруты следования на глобальном уровне описывают направление вызовов между зонами. Внутри зон применяются схемы маршрутизации – первичная и целевая (см. схему [Внутризонавая маршрутизация](#)).

При необходимости создания внешнего подключения (отдельного шлюза) может быть создана отдельная зона, в принадлежности к которой описывается создаваемое подключение.

10.4.6.1. Маршрутизация глобальная

Глобальная маршрутизация обрабатывает вызовы, поступающие из входящих в систему зон, производит их обработку и перенаправляет согласно сконфигурированным маршрутам (см. раздел [Глобальные маршруты](#)).

10.4.6.2. Маршрутизация первичная

Первичная маршрутизация обрабатывает вызовы, которые поступают с телефона пользователя или из принадлежащего зоне шлюза/транка.

При получении набранных пользователем цифр номера система ФЛАТ SoftSwitch выполняет поиск совпадений с внутренним планом нумерации текущей зоны, в который входят сервисные коды, абоненты и группы, затем с зональными маршрутами (первичная маршрутизация), далее задает направление – перенаправляет вовне зоны в область глобальной маршрутизации или передает вызов на целевую маршрутизацию.

Для управления правилами первичной маршрутизации выберите меню **Зона/Маршрутизация/Первичная**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 69](#)):

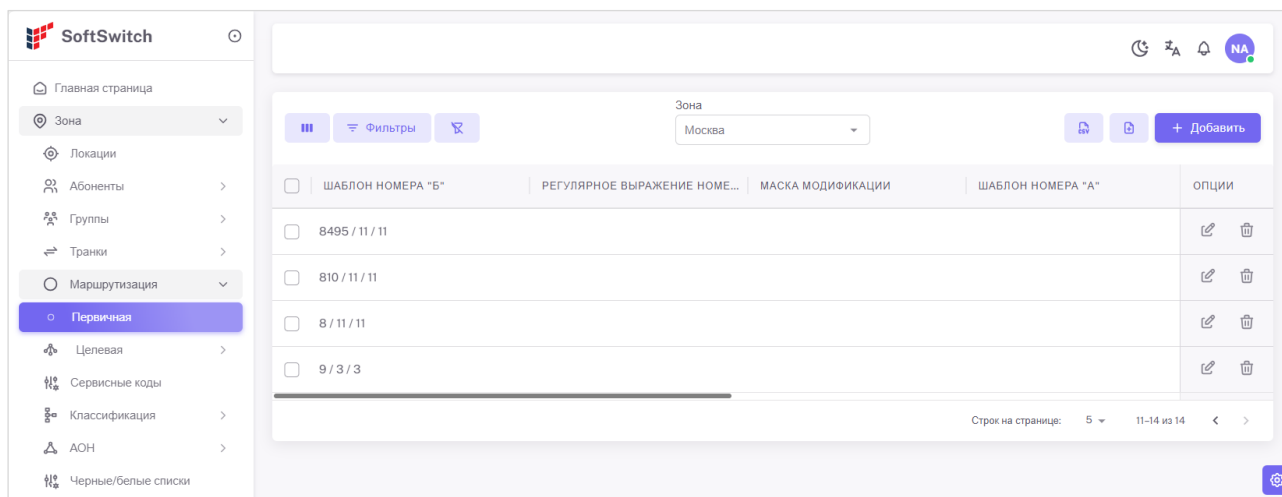


Рисунок 69. Список правил первичной маршрутизации



Рекомендуется при создании правил маршрутизации использовать только один метод обработки номеров – либо с использованием шаблонов, либо с использованием регулярных выражений. Смешение методов может привести к сложно интерпретируемой маршрутизации вызовов.

Для создания правила первичной маршрутизации нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . В открывшейся форме выберите вариант обработки – с использованием шаблонов (см. [Рисунок 70](#)), или с использованием регулярных выражений (см. [Рисунок 71](#)).

Редактировать ×

Использовать шаблоны
Использовать регулярные выражения

Шаблон номера "Б" (Префикс / Мин. / Макс.)

Шаблон номера "А" (Префикс / Мин. / Макс.)

Домен

Модификатор номера Б(удалить / вставить)

Модификатор номера А (удалить / вставить)

Цель

Класс трафика

Зона

Источник

Описание

Сохранить
Закрыть

Рисунок 70. Создание правила первичной маршрутизации с использованием шаблонов

В форме доступны следующие поля:

Поле	Значение
Шаблон номера «Б» (Префикс / Мин. / Макс.)	Шаблон номера получателя вызова. Первое поле – префикс номера, проходящего обработку. Второе и третье поле – минимальное и максимальное количество знаков, ограничивающее диапазон проходящих обработку номеров.
Шаблон номера «А» (Префикс / Мин. / Макс.)	Шаблон номера источника вызова. Первое поле – префикс номера, проходящего обработку. Второе и третье поле – минимальное и максимальное количество знаков, ограничивающее диапазон проходящих обработку номеров.
Домен	Указывается доменное имя при необходимости использования одинакового плана нумерации в разных зонах.
Модификатор номера Б (Удалить / Вставить)	Первое поле – количество удаляемых знаков номера получателя вызова, начиная с первого. Второе поле – символы, вставляемые перед модифицируемым номером.
Модификатор номера А (Удалить / Вставить)	Первое поле – количество удаляемых знаков номера источника вызова, начиная с первого. Второе поле – символы, вставляемые перед модифицируемым номером.
Цель	Направление вызова относительно текущей зоны: Локальная (цель) – внутреннее направление, вызов останется в текущей зоне и будет передан целевой маршрутизации. Глобальная (цель) – внешнее направление, вызов будет передан глобальной маршрутизации.
Класс трафика	Выбор класса трафика. Используется только для проверки ограничения, накладываемого на вызов. Для дальнейшего выбора маршрута не применяется. Определение классов и их назначение см. в разделе Классы трафика .
Зона	Указание зоны принадлежности правила.
Источник	Выбор локации источника вызова. Позволяет выбрать любую ранее сконфигурированную локацию текущей зоны. Пустое значение означает «Любая локация». Правила с определенной выбранной локацией источника вызова имеют больший вес при выборе маршрута даже при меньшем совпадении цифр. См. Пример 3 .
Описание	Описание правила.

Рисунок 71. Создание правила первичной маршрутизации с использованием регулярных выражений

В форме доступны следующие поля:

Поле	Значение
Блок проверки регулярного выражения	Для проверки совпадения регулярного выражения с номером введите в следующие поля: Номер – обрабатываемый номер. Регулярное выражение – проверяемое регулярное выражение. После нажатия кнопки Тест на экран будет выведено сообщение о результате проверки.
Регулярное выражение номера Б	Регулярное выражение для обработки номера получателя вызова (см. Регулярные выражения при проверке номера). Допустимые символы: <code>[]^0123456789-+?!X*#</code>
Маска модификации номера Б	Регулярное выражение для модификации номера получателя вызова (см. Регулярные выражения при модификации номера). Допустимые символы: <code>{ }0123456789-X</code> Указывается маска модификации номера, содержащая цифры, символы удаления и вставки, подстановочные знаки X , соответствующие цифре номера, начиная с последнего. Пример 1: Номер: 7772299, Маска: 1XX, Результат: 199 Пример 2: Номер: 7772299, Маска: XXX{88}XXXX, Результат: 777882299 Пример 3: Номер: 7772299, Маска: XXX--XX, Результат: 77799
Регулярное выражение номера А	Регулярное выражение для обработки номера источника вызова (см. Регулярные выражения при проверке номера). Допустимые символы: <code>[]^0123456789-+?!X*#</code>

Поле	Значение
Маска модификации номера А	<p>Регулярное выражение для модификации номера источника вызова (см. Регулярные выражения при модификации номера).</p> <p>Допустимые символы: {0123456789-X}</p> <p>Указывается маска модификации номера, содержащая цифры, символы удаления и вставки, подстановочные знаки X, соответствующие цифре номера, начиная с последнего.</p> <p>Пример 1: Номер: 7772299, Маска: 1XX, Результат: 199</p> <p>Пример 2: Номер: 7772299, Маска: XXX{88}XXXX, Результат: 777882299</p> <p>Пример 3: Номер: 7772299, Маска: XXX--XX, Результат: 77799</p>
Домен	Указывается доменное имя при необходимости использования одинакового плана нумерации в разных зонах.
Цель	<p>Направление вызова относительно текущей зоны:</p> <p>Локальная (цель) – внутреннее направление, вызов останется в текущей зоне и будет передан целевой маршрутизации.</p> <p>Глобальная (цель) – внешнее направление, вызов будет передан глобальной маршрутизации.</p>
Класс трафика	<p>Выбор класса трафика. Используется только для проверки ограничения, накладываемого на вызов. Для дальнейшего выбора маршрута не применяется.</p> <p>Определение классов и их назначение см. в разделе Классы трафика.</p>
Зона	Указание зоны принадлежности правила.
Источник	<p>Выбор локации источника вызова. Позволяет выбрать любую ранее сконфигурированную локацию текущей зоны. Пустое значение означает «Любая локация».</p> <p>Правила с определенной выбранной локацией источника вызова имеют больший вес при выборе маршрута даже при меньшем совпадении цифр. См. Пример 3.</p>
Описание	Описание правила.



При включенной пре-маршрутизации вызовов выполнение проверки на соответствие правилам первичной маршрутизации зависит от результатов поиска абонента по внутренней базе абонентов текущей локации. См. [Пре-маршрутизация](#).

Система ФЛАТ SoftSwitch выполняет проверку вызовов на соответствие правилам первичной маршрутизации в следующем порядке:

1. Поиск максимального совпадения по трем условиям (логический оператор «И»):
 - a. набранных абонентом цифр вызываемого номера с «**Шаблоном номера "Б"**» правила, или с «**Регулярным выражением номера "Б"**» правила;
 - b. номера вызывающего абонента с «**Шаблоном номера "А"**» правила, или с «**Регулярным выражением номера "А"**» правила (при его наличии);
 - c. доменного имени вызывающего абонента с одноименным шаблоном правила (при его наличии).

В случае если не будет найдено совпадение ни с одним правилом, проверка завершится, а вызывающий абонент услышит сигнал «занято».

2. Проверка вхождения **класса трафика** (при его наличии) текущего правила в список **класса ограничений** (при его наличии), назначенного абоненту. Иными словами, происходит проверка ограничений, наложенных на вызывающего абонента по использованию **класса трафика** текущего правила.

При положительном результате проверки обработка правила завершится, а вызывающий абонент услышит сигнал «занято».

3. Проверка принадлежности вызывающего абонента к определенной локации текущей зоны (при ее указании).

При отрицательном результате проверки обработка правила завершится, а вызывающий абонент услышит сигнал «занято».

4. Модификация номера «А» (при наличии шаблона), модификация номера «Б» (при наличии шаблона) и передача вызова в область глобальной или целевой маршрутизации, в зависимости от **Цели** текущего правила.

Рассмотрим несколько примеров правил первичной маршрутизации.

Пример 1. Вызов на четырехзначный номер, начинающийся с кода 1, приходящий из любой локации текущей зоны «Москва» и имеющий класс трафика «Внутренний», направлять в область целевой маршрутизации без модификации номера (см. [Рисунок 72](#)):

Рисунок 72. Правило первичной маршрутизации - внутренний вызов

Пример 2. Вызов на номер с диапазоном длин от 12 до 21 знака, начинающийся с кода 9810, приходящий из «Головного офиса» текущей зоны «Москва» и имеющий класс трафика «Международный», направлять в область глобальной маршрутизации без модификации номера (см. [Рисунок 73](#)):

Рисунок 73. Правило первичной маршрутизации - международный вызов

Пример 3. Правила с конкретно выбранной локацией источника вызова имеют больший вес при выборе маршрута даже при меньшем совпадении цифр. При проверке вызова от абонента из локации «Головной офис» зоны «Москва» на номер 123456 на соответствие правилам первичной маршрутизации у второго правила будет больший вес (см. [Рисунок 74](#)):

Рисунок 74. Вес правил при указанной локации источника

Пример 4. Правила с максимальным совпадением с регулярным выражением имеют больший вес при выборе маршрута. При проверке вызова на номер 1234 на соответствие правилам первичной маршрутизации у второго правила будет меньше вариантов совпадающих номеров, и соответственно, больший вес (см. [Рисунок 75](#)):

Рисунок 75. Вес правил при разном совпадении регулярного выражения с номером

10.4.6.3. Маршрутизация целевая

Целевая маршрутизация обрабатывает вызовы, которые направлены либо в сторону абонента (группы абонентов), либо в сторону принадлежащего зоне шлюза.

10.4.6.3.1. Коды

Для доступа к правилам целевой маршрутизации выберите меню **Зона/Маршрутизация/Целевая/Коды**, после чего в окне отобразится список ранее созданных сущностей с указанием их параметров (см. [Рисунок 76](#)):

ID	ШАБЛОН НОМЕРА "Б"	РЕГУЛЯРНОЕ ВЫРАЖ...	МАСКА МОДИФИКАЦИИ	ШАБЛОН НОМЕРА "А"	РЕГУЛЯРНОЕ ВЫРАЖ...	ДОМЕН	МОД	ОПЦИИ
29	8070 / 4 / 4							
28	8080 / 4 / 4							
27	8090 / 4 / 4							
26	5 / 3 / 3							
25	800 / 3 / 3							

Рисунок 76. Список кодов целевой маршрутизации



Рекомендуется при создании правил маршрутизации использовать только один метод обработки номеров – либо с использованием шаблонов, либо с использованием регулярных выражений. Смешение методов может привести к сложно интерпретируемой маршрутизации вызовов.

Для создания правила целевой маршрутизации нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . В открывшейся форме выберите вариант обработки – с использованием шаблонов (см. [Рисунок 77](#)), или с использованием регулярных выражений (см. [Рисунок 78](#)).

Рисунок 77. Создание правила целевой маршрутизации с использованием шаблонов

В форме доступны следующие поля:

Поле	Значение
Шаблон номера «Б» (Префикс / Мин. / Макс.)	Шаблон номера получателя вызова. Первое поле – префикс номера, проходящего обработку. Второе и третье поле – минимальное и максимальное количество знаков, ограничивающее диапазон проходящих обработку номеров.
Шаблон номера «А» (Префикс / Мин. / Макс.)	Шаблон номера источника вызова. Первое поле – префикс номера, проходящего обработку. Второе и третье поле – минимальное и максимальное количество знаков, ограничивающее диапазон проходящих обработку номеров.
Домен	Указывается доменное имя при необходимости использования одинакового плана нумерации в разных зонах.
Модификатор номера Б (Удалить / Вставить)	Первое поле – количество удаляемых знаков номера получателя вызова, начиная с первого. Второе поле – символы, вставляемые перед модифицируемым номером.
Цель	Тип цели направления вызова: <ul style="list-style-type: none"> • Внутренний номер. • Транк (см. Транки). • Направление (см. Направления). • Блокировка (вызов блокируется, вызывающему абоненту проигрывается сигнал «занято»). • Расписание (см. По времени). • Классификатор (см. Классификаторы).
Параметр	При выборе типа цели Транк , Направление или Расписание форма дополняется текущим полем с раскрывающимся списком ранее сконфигурированных целей.

Поле	Значение
Описание	Описание правила.

Рисунок 78. Создание правила целевой маршрутизации с использованием регулярных выражений

В форме доступны следующие поля:

Поле	Значение
Блок проверки регулярного выражения	Для проверки совпадения регулярного выражения с номером введите в следующие поля: Номер – обрабатываемый номер. Регулярное выражение – проверяемое регулярное выражение. После нажатия кнопки Тест на экран будет выведено сообщение о результате проверки.
Регулярное выражение номера Б	Регулярное выражение для обработки номера получателя вызова (см. Регулярные выражения при проверке номера). Допустимые символы: <code>[]^0123456789-+?!X*#</code>
Маска модификации номера Б	Регулярное выражение для модификации номера получателя вызова (см. Регулярные выражения при модификации номера). Допустимые символы: <code>{ }0123456789-X</code> Указывается маска модификации номера, содержащая цифры, символы удаления и вставки, подстановочные знаки X , соответствующие цифре номера, начиная с последнего. Пример 1: Номер: 7772299, Маска: 1XX, Результат: 199 Пример 2: Номер: 7772299, Маска: XXX{88}XXXX, Результат: 777882299 Пример 3: Номер: 7772299, Маска: XXX--XX, Результат: 77799
Регулярное выражение номера А	Регулярное выражение для обработки номера источника вызова (см. Регулярные выражения при проверке номера). Допустимые символы: <code>[]^0123456789-+?!X*#</code>

Поле	Значение
Домен	Указывается доменное имя при необходимости использования одинакового плана нумерации в разных зонах.
Цель	Тип цели направления вызова: <ul style="list-style-type: none"> • Внутренний номер. • Транк (см. Транки). • Направление (см. Направления). • Блокировка (вызов блокируется, вызывающему абоненту проигрывается сигнал «занято»). • Расписание (см. По времени). • Классификатор (см. Классификаторы).
Параметр	При выборе типа цели Транк , Направление или Расписание форма дополняется текущим полем с раскрывающимся списком ранее сконфигурированных целей.
Описание	Описание правила.

Система ФЛАТ SoftSwitch выполняет проверку вызовов на соответствие правилам целевой маршрутизации в следующем порядке:

1. Поиск максимального совпадения по трем условиям (логический оператор И):

- a. набранных абонентом цифр вызываемого номера с *«Шаблон номера "Б"»* правила, или с *«Регулярным выражением номера "Б"»* правила;
- b. номера вызывающего абонента с *«Шаблон номера "А"»* правила, или с *«Регулярным выражением номера "А"»* правила (при его наличии);
- c. доменное имя вызывающего абонента с одноименным шаблоном правила (при его наличии).

В случае, если не будет найдено совпадение ни с одним правилом, проверка завершится, а вызывающий абонент услышит сигнал «занято».

2. Модификация номера «Б» (при наличии шаблона) и передача вызова в указанную область, согласно Цели текущего правила.

Рассмотрим несколько примеров правил целевой маршрутизации.

Пример 1. Вызов на четырехзначный номер, начинающийся с кода «330», имеющий тип цели «внутренний номер», направить без модификации на соответствующий внутренний номер текущей зоны (см. [Рисунок 79](#)):

Рисунок 79. Правило целевой маршрутизации – внутренний вызов

Пример 2. Вызов на шестизначный номер, начинающийся с «88», имеющий тип цели «Транк», с модификацией номера – удалением первых двух знаков, направить на транк с наименованием «сист» текущей зоны (см. [Рисунок 80](#)):

Рисунок 80. Правило целевой маршрутизации – транк

Пример 3. Вызов на номер длиной 11 знаков, с одним из трех вариантов кода («903», «904», «905»), имеющий тип цели «Транк», с модификацией номера – удалением первого знака, направить на транк с наименованием «Gorod» текущей зоны (см. [Рисунок 81](#)):

Рисунок 81. Правило целевой маршрутизации с использованием регулярного выражения

10.4.6.3.2. Направления

Направления в системе ФЛАТ SoftSwitch позволяют настроить балансировку нагрузки внутри зоны путем перераспределения трафика по разным транкам.

Для доступа к настройкам направлений выберите меню **Зона/Маршрутизация/Целевая/Направления**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 82](#)):

ID ↓	ИМЯ	ТИП	РЕЗЕРВНЫЙ НОМЕР	ОПИСАНИЕ	ОПЦИИ
1	IVR	Распределенная			

Рисунок 82. Список направлений целевой маршрутизации

Для создания нового направления нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите его параметры (см. [Рисунок 83](#)):

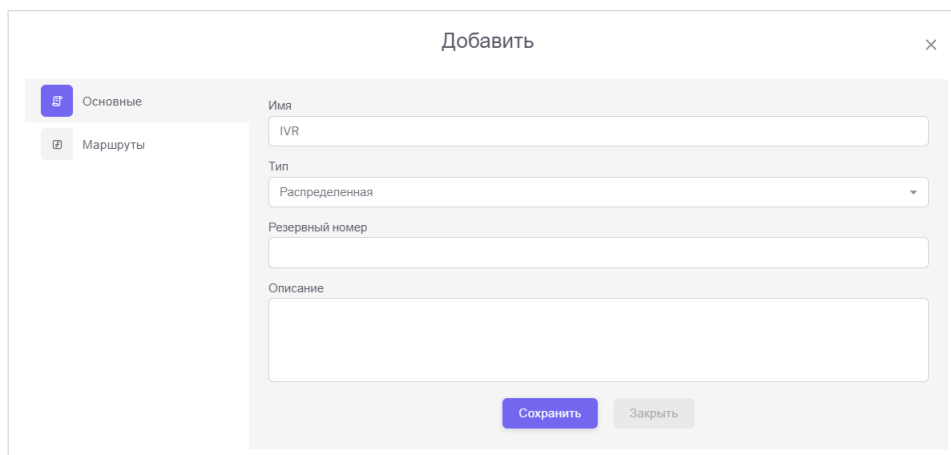


Рисунок 83. Создание направления

В форме доступны следующие поля:

Поле	Значение
Имя	Название направления.
Тип	<p>Параметр, описывающий тип балансировки. Предопределены следующие значения:</p> <p>Линейная – маршрут выбирается из доступных с учетом приоритета.</p> <p>Циклическая – маршрут выбирается из доступных в порядке циклического перебора начиная с первого в списке.</p> <p>Распределенная – маршрут выбирается из доступных с учетом приоритета и веса. Первичный выбор маршрута происходит по значению приоритета. При наличии маршрутов с одинаковым приоритетом, нагрузка перераспределяется в % отношении согласно указанному весу маршрута.</p>
Резервный номер	Внутренний номер, на который будет направлен вызов в случае недоступности транков в направлении.
Описание	Описание направления.

После сохранения направления станет доступна для редактирования вкладка **Маршруты** (см. [Рисунок 84](#)).

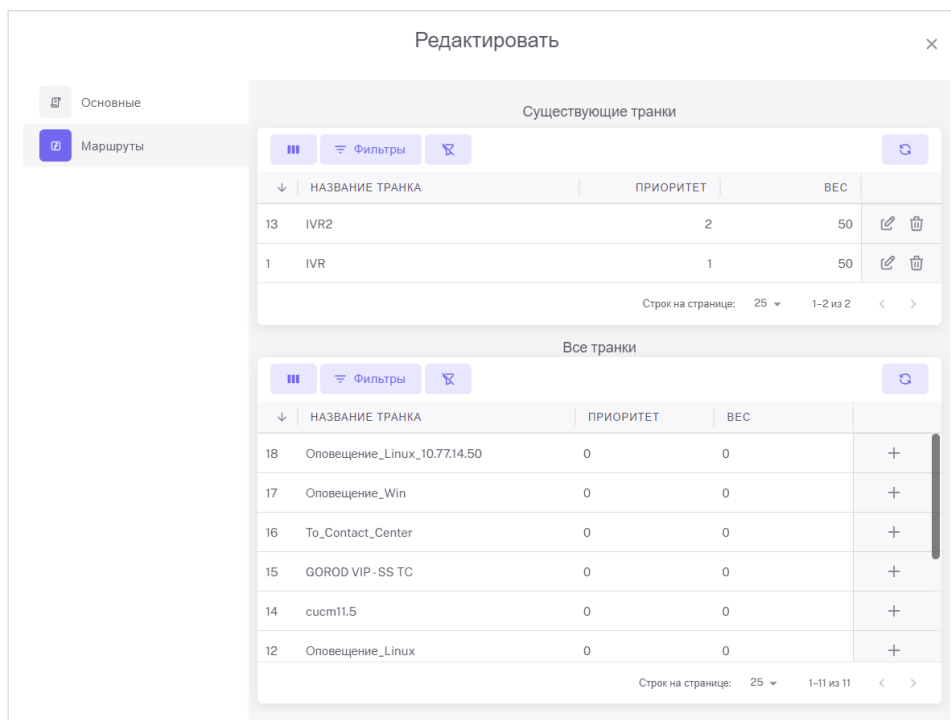


Рисунок 84. Свойства направления, вкладка «Маршруты»

В области формы **Существующие транки** отображается список входящих в маршрут транков, а в области **Все транки** – список транков выбранной зоны, доступных к распределению.

Для включения транка в маршрут нажмите кнопку **+**, укажите значения приоритета и веса, сохраните изменения кнопкой **💾**. Для удаления функции из профиля нажмите кнопку **🗑**.

Для изменения приоритета и веса у включенного в маршрут транка нажмите кнопку **✎**, укажите новые значения и сохраните изменения кнопкой **💾**.

Назначение приоритета и веса:

Поле	Значение
Приоритет	Целочисленное значение приоритета по отношению к другим маршрутам. Чем меньше значение, тем выше приоритет.
Вес	Вес маршрута в % от общей нагрузки. Общий вес маршрутов с одинаковым приоритетом не должен превышать 100%.

10.4.6.3.3. Классификаторы

Для настройки целевой маршрутизации в зависимости от классов сервиса добавлены специальные правила.

Для доступа к их настройкам выберите меню **Зона/Маршрутизация/Целевая/Классификаторы**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 85](#)):

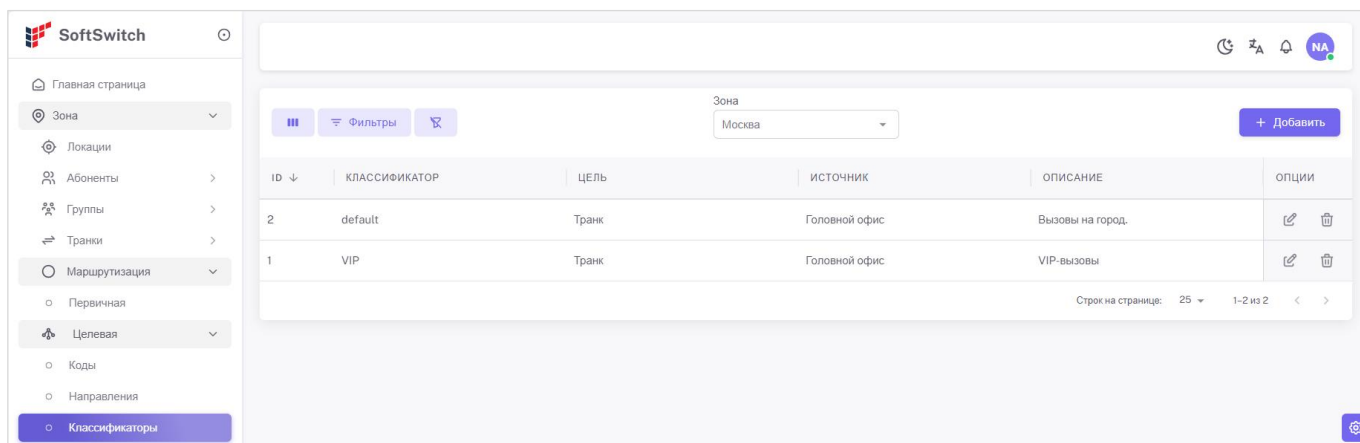


Рисунок 85. Список классификаторов целевой маршрутизации

Для создания нового правила нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 86](#)):

Добавить ×

Название

Зона

Источник

Класс сервиса

Класс трафика

Цель

Параметр

Описание

Рисунок 86. Создание правила целевой маршрутизации по классам

В форме доступны следующие поля:

Поле	Значение
Название	Название правила целевой маршрутизации.
Зона	Указание зоны принадлежности правила.
Источник	Выбор локации источника вызова. Позволяет выбрать любую ранее сконфигурированную локацию текущей зоны. Пустое значение означает «Любая локация».
Класс сервиса	Выбор класса сервиса. Применяется для управления маршрутизацией вызовов в зависимости от класса трафика. Создание классов сервиса см. в главе Классы сервиса .
Класс трафика	Выбор класса трафика.

Поле	Значение
	Определение классов и их назначение см. в разделе Классы трафика .
Цель	Тип цели направления вызова: <ul style="list-style-type: none"> • Внутренний номер. • Транк (см. Транки). • Направление (см. Направления). • Блокировка (вызов блокируется, вызывающему абоненту проигрывается сигнал «занято»). • Расписание (см. По времени).
Параметр	При выборе типа цели Транк , Направление или Расписание форма дополняется полем выбора цели.
Описание	Описание правила.

Применение правил целевой маршрутизации по классам см. в главе [Применение классов сервиса и ограничений](#).

10.4.6.3.4. По времени

Для гибкой настройки перенаправления вызовов с учетом расписания в целевую маршрутизацию добавлены специальные правила.

Для доступа к их настройкам выберите меню **Зона/Маршрутизация/Целевая/По времени**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 87](#)):

ID ↓	НАЗВАНИЕ	ВРЕМЯ НАЧАЛА	ВРЕМЯ ОКОНЧАНИЯ	ТИП ЦЕЛИ	ПАРАМЕТР	ОПИСАНИЕ	ОПЦИИ
2	Нерабочее время	18:01:00	08:59:00	Транк	IVR2		
1	Рабочее время	09:00:00	18:00:00	Транк	IVR		

Рисунок 87. Список правил целевой маршрутизации по времени

Для создания нового правила нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 88](#)):

Рисунок 88. Создание правила целевой маршрутизации по времени

В форме доступны следующие поля:

Поле	Значение
Название	Название правила целевой маршрутизации.
Время	Время начала и окончания действия правила.
Цель	Тип цели направления вызова: <ul style="list-style-type: none"> • Внутренний номер. • Транк. • Направление (см. Направления). • Блокировка (вызов блокируется, вызывающему абоненту проигрывается сигнал «занято»). • Классификатор (см. Классификаторы).
Параметр	При выборе типа цели Транк или Направление форма дополняется полем выбора цели.
Описание	Описание правила.

Рассмотрим пример правила целевой маршрутизации по времени.

Пример 1. Вызов в рабочее время с 09:00 до 18:00 направить на транк с наименованием «IVR» текущей зоны, а в нерабочее время с 18:01 до 08:59 направить на транк с наименованием «IVR2» текущей зоны (см. [Рисунок 89](#)):

ID ↓	НАЗВАНИЕ	ВРЕМЯ НАЧАЛА	ВРЕМЯ ОКОНЧАНИЯ	ТИП ЦЕЛИ	ПАРАМЕТР	ОПИСАНИЕ	ОПЦИИ
2	Нерабочее время	18:01:00	08:59:00	Транк	IVR2		
1	Рабочее время	09:00:00	18:00:00	Транк	IVR		

Рисунок 89. Пример правила целевой маршрутизации по времени

10.4.6.4. Пре-маршрутизация

Для удобства переключения абонентов со старой АТС на новый ФЛАТ SoftSwitch вводится режим пре-маршрутизации, который позволяет направить вызов на абонента минуя маршрутизацию. Пре-маршрутизация для вызовов, поступающих от абонентов локации включается в ее свойствах параметром «Использовать пре-маршрутизацию». Пре-маршрутизация для вызовов, поступающих с транков относящихся к локации, включается в ее свойствах параметром «Использовать пре-маршрутизацию для транков». Включение пре-маршрутизации см. в главе [Вкладка «Параметры локации»](#).

При включенной пре-маршрутизации (от абонентов локации или с транков, относящихся к локации) перед маршрутизацией вызова происходит поиск совпадений в локальной базе абонентов, и при его нахождении вызов переключается на абонента. Если абонент не будет найден в локальной базе данных, тогда вызов направляется на первичную маршрутизацию.

10.4.7. Сервисные коды

Для совершения различных действий с абонентских устройств используются сервисные коды, которые могут влиять на текущее соединение, задавать параметры работы с данным абонентом и пр. Каждый сервисный код состоит из нескольких полей: значения кода, его назначения, принадлежности к определенной Зоне.



Для каждой Зоны создается свой список сервисных кодов.

Для доступа к их настройкам выберите меню **Зона/Сервисные коды**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 90](#)):

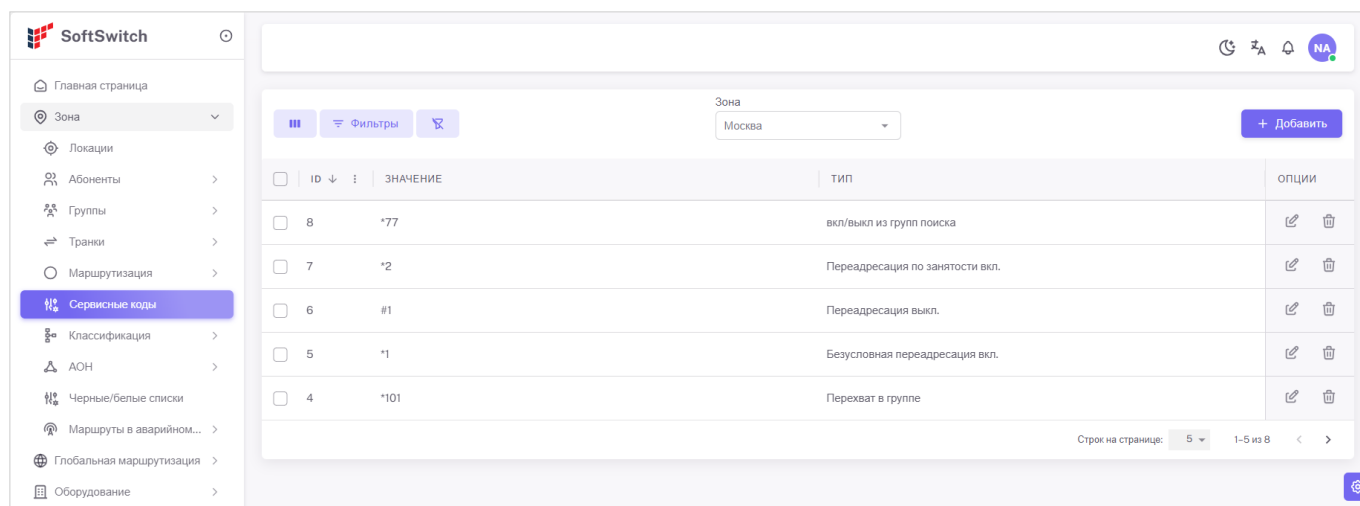


Рисунок 90. Список сервисных кодов зоны Москва

Для создания нового сервисного кода нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 91](#)):

Добавить ×

Зона

Тип

Значение

Рисунок 91. Создание сервисного кода

В форме доступны следующие поля:

Поле	Значение
Зона	Зона принадлежности сервисного кода.

Поле	Значение
Тип	Тип сервисного кода (см. следующую таблицу).
Значение	Сервисный код в установленном формате. Обязательный параметр. Обычно используется значение, состоящее из трех или четырех знаков, состоящее из цифр и знаков *, #.

Типы сервисных кодов:

№	Параметр	Значение
1	Безусловная переадресация вкл.	Включение перевода всех входящих вызовов на указанный номер.
2	Вкл./выкл. из групп поиска	Временное включение/выключение абонента из группы поиска. Фактически абонент остается в группе, но не участвует в перенаправлении вызова.
3	Конференция	Сбор новой конференции или подключение к текущему разговору нового участника.
4	Обратный вызов вкл.	Включение функционала обратного вызова. См. Функция «Обратный вызов» .
5	Обратный вызов выкл.	Выключение функционала обратного вызова.
6	Переадресация выкл.	Выключение любой переадресации.
7	Переадресация по занятости вкл.	Включение перевода входящих вызовов на указанный номер при занятости абонента.
8	Переадресация по неответу вкл.	Включение перевода входящих вызовов на указанный номер при неответе абонента.
9	Перехват в группе	Перехват входящего вызова, предназначенного другому абоненту, участником одной группы перехвата.
10	Вкл./выкл. альтернативный номер	Включение/выключение альтернативного номера.
11	Парковка вызова	Парковка вызова в одном из трех выделенных под каждого абонента слотов, с возможностью с любого ТА введя свой номер и номер слота забрать запаркованный вызов. На ТА Cisco настраивается отображение номера слота с запаркованным вызовом. Ответная часть настроек выполняется в ФЛАТ Device Manager (см. соответствующий документ).

Типы сервисных кодов с №2 по №4 гарантированно поддерживают клиентские устройства следующих производителей: Unify, Atcom, Yealink, Cisco, в конфигурации которых этот функционал необходимо активировать². В остальных устройствах функция сбора конференции и включения обратного вызова с телефонного аппарата может быть не доступна.

Рассмотрим пример сервисного кода.

Пример 1. Установлен сервисный код «*1» для включения безусловной переадресации. Чтобы включить переадресацию с телефонного аппарата на внутренний номер 1111 требуется набрать «*1*1111» и нажать «вызов» (см. [Рисунок 92](#)):

² Для централизованного управления IP-телефонами различных производителей предназначен продукт ФЛАТ Device Manager.

Рисунок 92. Пример сервисного кода безусловной переадресации

10.4.8. Классификация

В системе ФЛАТ SoftSwitch классификация используется для создания правил выбора маршрута при совершении исходящих вызовов или запрета вызовов на заданные направления.

10.4.8.1. Классы трафика

Для удобства управления вызовами вводится понятие класс трафика. Позволяет в рамках глобальной и первичной маршрутизации ограничивать правила обработки голосовых вызовов.

Для каждого вида маршрутизации создаются свои классы трафика – для глобальной маршрутизации классы трафика имеют принадлежность «Глобальная» (см. [Классы трафика](#) в разделе [Маршрутизация глобальная](#)), для первичной маршрутизации – принадлежность «Зона».

Для доступа к списку классов трафика выберите меню **Зона/Классификация/Классы трафика**. После чего в окне отобразится список созданных сущностей с указанием названия, комментария и принадлежности (см. [Рисунок 93](#)). Видны будут все классы трафика – и с глобальной, и зональной принадлежностью, но для редактирования доступны только с принадлежностью «Зона».

ID	НАЗВАНИЕ	КОММЕНТАРИЙ	ПРИНАДЛЕЖНОСТЬ	ОПЦИИ
18	8-МГ-Глобальный	Междугородний	Глобальная	
16	89-МОБ	Город	Зона	
15	8800-Г	Город	Зона	
14	8496-Г	Город	Зона	
13	8499-Г	Город	Зона	

Рисунок 93. Классы трафика

Для создания нового класса трафика нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите название и комментарий (см. [Рисунок 94](#)):

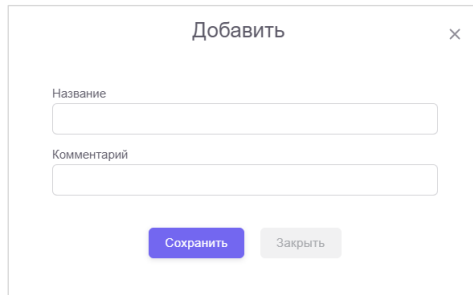


Рисунок 94. Создание класса трафика

После сохранения классу трафика будет присвоена принадлежность «Зона».

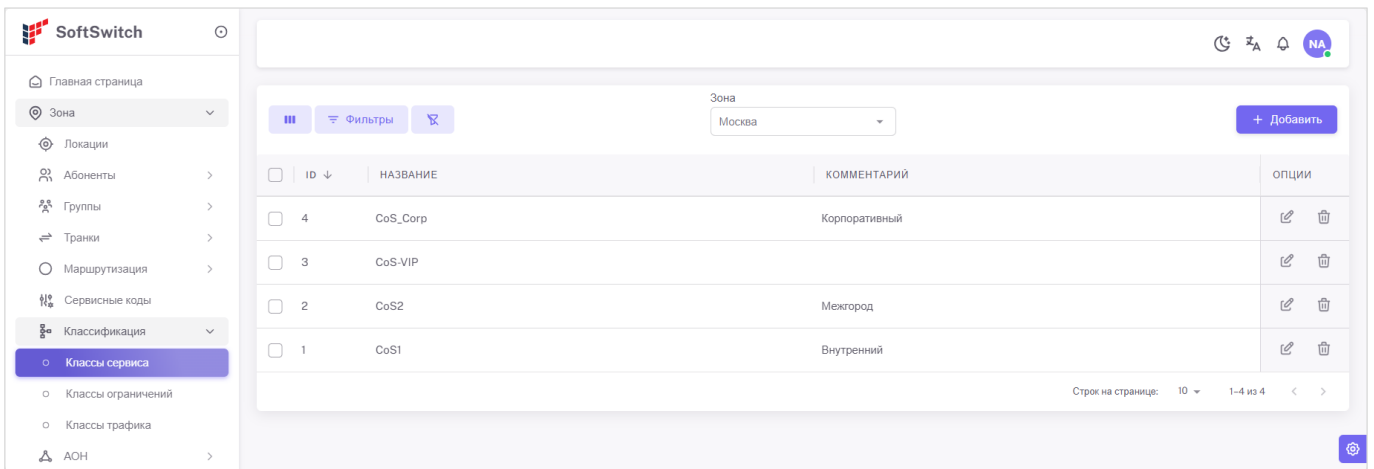
В системе ФЛАТ SoftSwitch predetermined классов трафика нет.

Взаимосвязь классов трафика с другими параметрами системы ФЛАТ SoftSwitch показана на примерах конфигурирования глобальной и первичной маршрутизации (см. [Применение классов сервиса и ограничений](#)).

10.4.8.2. Классы сервиса

Классы сервиса (Class of Service) – набор классов трафика для управления маршрутизацией при совершении исходящих вызовов.

Для доступа к списку классов сервиса выберите горизонтальное меню **Зона/Классификация/Классы сервиса**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 95](#)):



ID	НАЗВАНИЕ	КОММЕНТАРИЙ	опции
4	CoS_Corp	Корпоративный	
3	CoS-VIP		
2	CoS2	Межгород	
1	CoS1	Внутренний	

Рисунок 95. Список классов сервиса

Для создания нового класса сервиса нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите его название и описание (см. [Рисунок 96](#)):

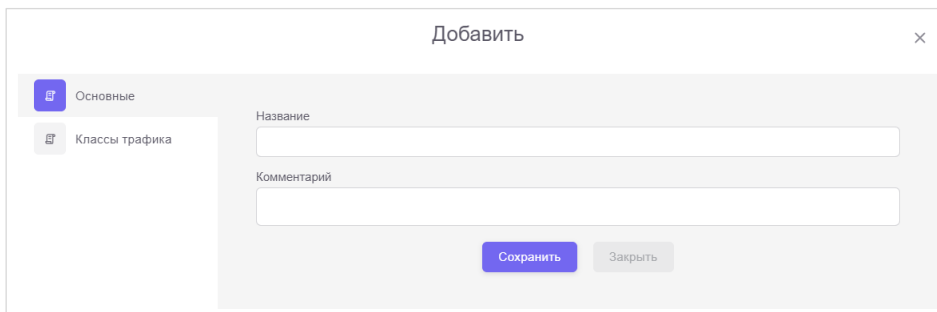


Рисунок 96. Создание класса сервиса

После сохранения класса сервиса станет доступна для редактирования вкладка **Классы трафика**. (см. [Рисунок 97](#)):

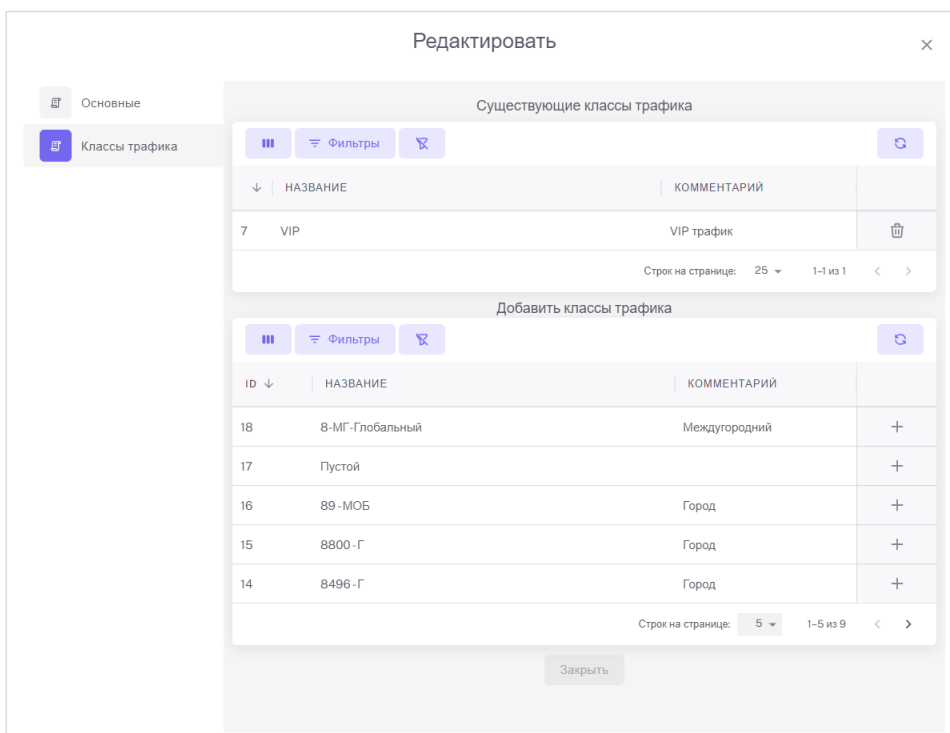


Рисунок 97. Класс сервиса, вкладка "Классы трафика"

В области формы **Существующие классы трафика** отображается список сущностей, входящих в класс сервиса, а в области **Добавить классы трафика** – список сущностей, доступных к распределению.

Для включения класса трафика в класс сервиса нажмите кнопку **+**, а для удаления – кнопку **🗑**. Сохранение изменений состава набора происходит автоматически.

10.4.8.3. Классы ограничений

Классы ограничений (Class of Restrictions) – набор классов трафика для управления маршрутизацией при необходимости запрета вызовов на заданные направления.

Для доступа к списку классов ограничений выберите горизонтальное меню **Зона/Классификация/Классы ограничений**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 98](#)):

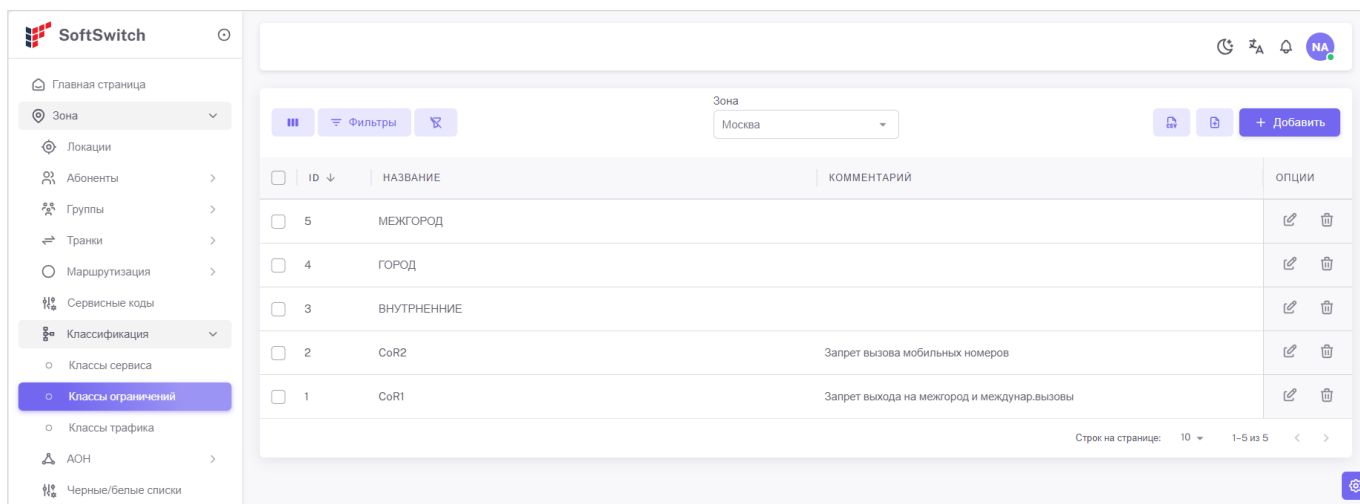


Рисунок 98. Список классов ограничений

Для создания нового класса ограничений нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите его название и описание (см. [Рисунок 99](#)):

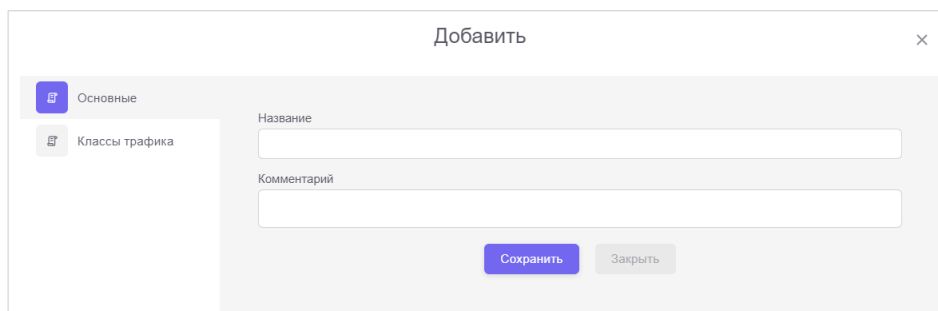


Рисунок 99. Создание класса ограничений

После сохранения класса сервиса станет доступна для редактирования вкладка **Классы трафика**. (см. [Рисунок 100](#)):

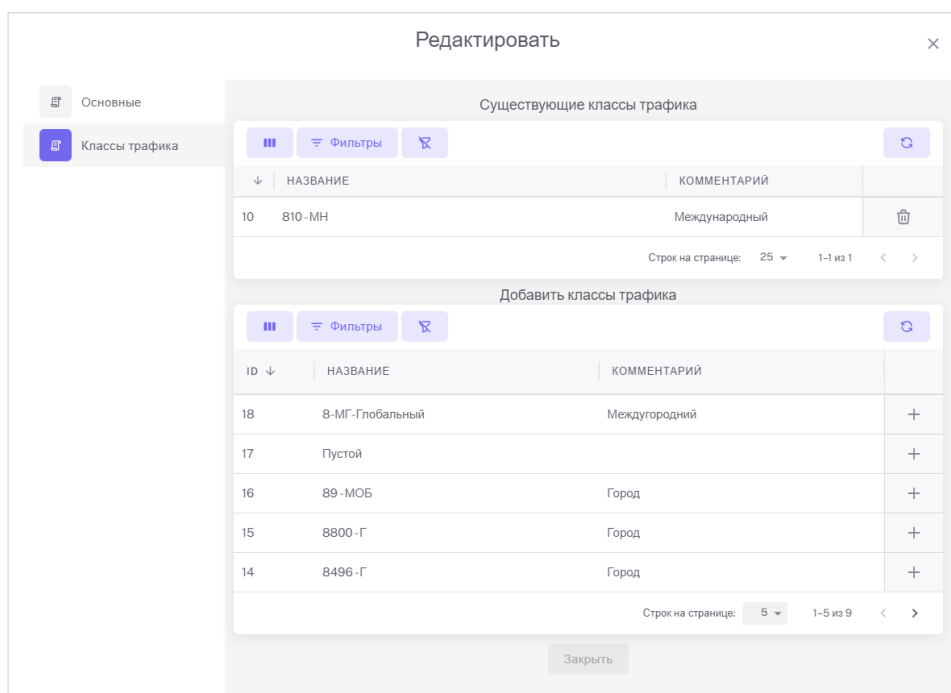


Рисунок 100. Класс ограничений, вкладка "Классы трафика"

В области формы **Существующие классы трафика** отображается список сущностей, входящих в класс сервиса, а в области **Добавить классы трафика** – список сущностей, доступных к распределению.

Для включения класса трафика в класс сервиса нажмите кнопку **+**, а для удаления – кнопку **🗑**. Сохранение изменений состава набора происходит автоматически.

10.4.9. АОН

Для изменения выдаваемых АОН цифр абонентского номера применяются модификаторы, которые для удобства могут быть объединены в группы. Группы модификаторов удобно использовать, назначая заранее сформированные наборы правил для однотипной модификации.

Правила модификации назначаются в свойствах транка (см. [Вкладка «Функции»](#)).

10.4.9.1. Список групп модификаторов

Для доступа к списку групп модификаторов выберите горизонтальное меню **Зона/АОН/Список групп модификаторов**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 101](#)):

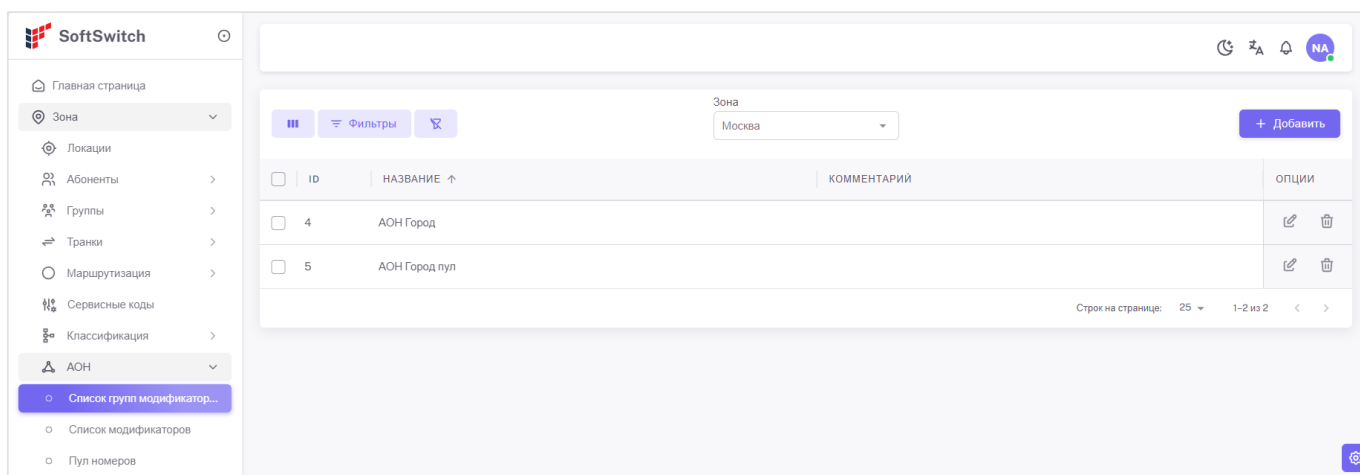


Рисунок 101. Список групп модификаторов АОН

Для создания новой группы модификаторов нажмите кнопку **Добавить**, а для изменения ранее созданной – значок редактирования **✎**. После чего в поля открывшейся формы внесите ее название и описание (см. [Рисунок 102](#)):

Добавить ✕

Название

Комментарий

Сохранить
Заккрыть

Рисунок 102. Создание новой группы модификаторов АОН

10.4.9.2. Список модификаторов

Для доступа к списку модификаторов выберите меню **Зона/АОН/Список модификаторов**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 103](#)):

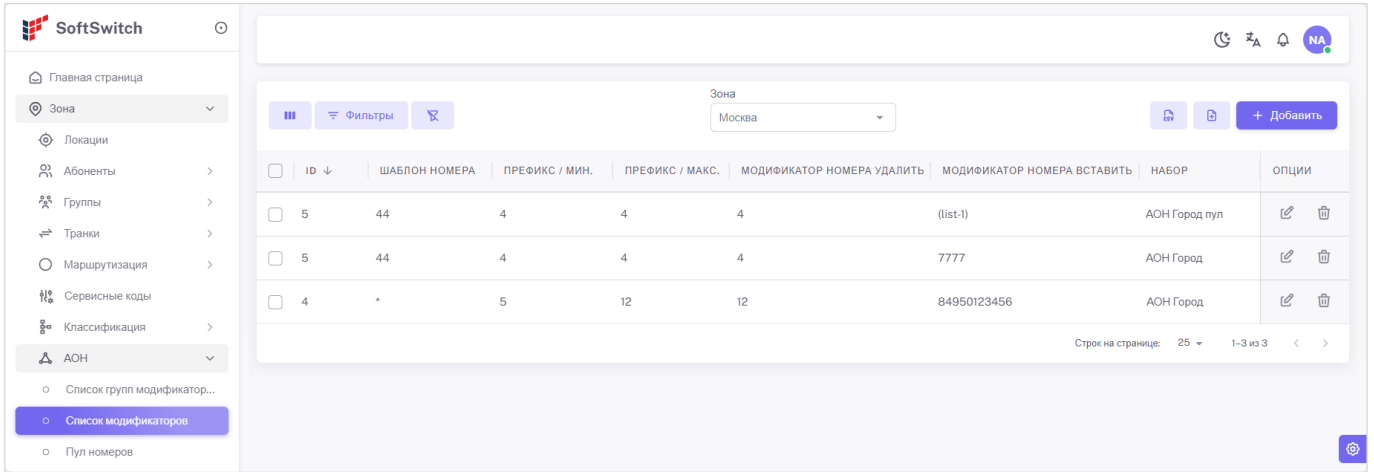


Рисунок 103. Список модификаторов АОН



Перед созданием модификаторов должна быть создана хотя бы одна группа модификаторов.

Для создания нового класса трафика нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 104](#)):

Рисунок 104. Создание модификатора АОН


В форме доступны следующие поля:

Поле	Значение
Шаблон номера Префикс / Мин. Префикс / Макс.	Описание шаблона номера состоит из трех полей: Шаблон номера – шаблон номера, подпадающего под модификацию. Допустимо использование символа «*» для обозначения любого номера. Префикс / Мин. и Префикс / Макс. – минимальное и максимальное количество знаков, ограничивающее диапазон подпадающих под модификацию номеров.
Модификатор номера удалить	Количество удаляемых знаков номера начиная с первого.
Модификатор номера вставить	Символы, вставляемые перед модифицируемым номером. В случае если второе поле содержит строку (list-1) , подставляться будут номера из сформированного пула (см. Пул номеров).
Набор	Выбор группы модификаторов.

При наличии в списке модификаторов нескольких правил, под которые подпадает обрабатываемый номер, выбирается правило наибольшего совпадения.

Предусмотрен импорт и экспорт модификаторов АОН в файл формата CSV.

Для экспорта всех модификаторов АОН ФЛАТ SoftSwitch нажмите кнопку , после чего будет сформировано соответствующее задание, результат выполнения которого отразится в разделе [Задачи](#).

Для загрузки в систему модификаторов нажмите кнопку , отметьте подготовленный файл и подтвердите выбор. После чего будет сформировано соответствующее задание, результат выполнения которого отразится в разделе [Задачи](#). В качестве шаблона удобно использовать ранее выгруженный список.



Рекомендуется использовать кодировку Unicode UTF-8 и разделитель значений колонок – символ запятой.

При некорректном содержимом импортируемого файла на экран будет выведено сообщение об ошибке.

10.4.9.2.1. Примеры модификации АОН

Рассмотрим несколько примеров модификации АОН.

Пример 1. Модификации подлежит номер, соответствующий шаблону «11117» (минимальное и максимальное количество знаков совпадает с длиной шаблона). При модификации будет удален первый символ номера, а перед оставшимися знаками номера будет добавлена строка «7495123». В результате АОН будет выдан номер «74951231117» (см. [Рисунок 105](#)):

Рисунок 105. Пример модификатора АОН по шаблону

Пример 2. В организации принята пятизначная нумерация внутренних номеров. Абонент «А» вызывает абонента «В», у которого настроена переадресация на внешний номер. При модификации будут удалены все цифры номера вызывающего абонента, а в АОН будет выдан номер организации «84950123456» (см. [Рисунок 106](#)):

Рисунок 106. Пример модификатора АОН с подстановкой номера организации

Для завершения настройки в свойствах транка укажите группу модификаторов «АОН Город» (см. [Вкладка «Функции»](#)).

Пример 3. Модификации подлежат четырехзначные номера, начинающиеся с «44». При модификации будут удалены все цифры номера, а в АОН будет выдан в случайном порядке выбранный номер из пула номеров (см. [Рисунок 107](#)):

Рисунок 107. Пример модификатора АОН с подстановкой из пула номеров

10.4.9.3. Пул номеров

В системе ФЛАТ SoftSwitch предусмотрена возможность формирования пула номеров для выдачи АОН случайного номера из выделенной последовательности.

Для доступа к пулу номеров выберите меню **Зона/АОН/Пул номеров**, после чего в окне отобразится сформированный список с указанием номера, названия группы модификаторов и описания (см. [Рисунок 108](#)):

ID	НОМЕР	НАБОР	КОММЕНТАРИЙ	ОПЦИИ
7	74950000001	АОН Город пул		
8	74950000002	АОН Город пул		
9	74950000003	АОН Город пул		
10	74950000004	АОН Город пул		
11	74950000005	АОН Город пул		

Рисунок 108. Сформированный пул номеров

Для пополнения пула номеров нажмите кнопку **Добавить**, а для добавления диапазона номеров – кнопку **Добавить диапазон номеров**. После чего в открывшейся форме укажите принадлежность к группе модификаторов и внесите требуемый номер, или укажите начало и конец диапазона добавляемых номеров (см. [Рисунок 109](#)):

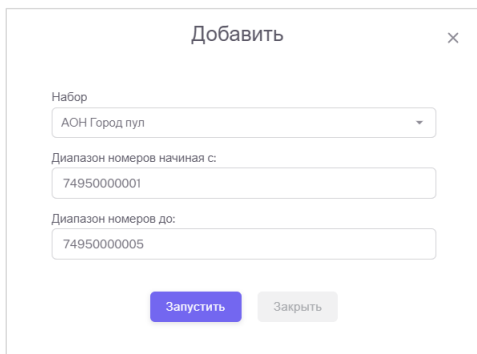


Рисунок 109. Добавление диапазона номеров в пул номеров

В форме доступны следующие поля:

Поле	Значение
Набор	Выбор набора модификаторов. Обязательный параметр.
Номер телефона Диапазон номеров	Добавление номера в пул возможно как по одному, так и диапазоном.

10.4.10. Черные/Белые списки на уровне зон

Функционал черных и белых списков позволяет ограничить входящие телефонные вызовы в зависимости от того, в какой список попадает вызывающий номер.

Черный список позволяет блокировать вызовы, поступающие с определённых номеров. Звонки от таких абонентов будут отклонены при попытке установить соединение.

Белый список позволяет блокировать все входящие вызовы, кроме вызовов абонентов, внесённых в список разрешённых.

Списки действуют на уровне той зоны, в которой были созданы.

10.4.10.1. Создание списков

Для управления списками выберите меню **Зона/Черные/белые списки**, после чего в окне отобразится список созданных сущностей с указанием их параметров (см. [Рисунок 110](#)):

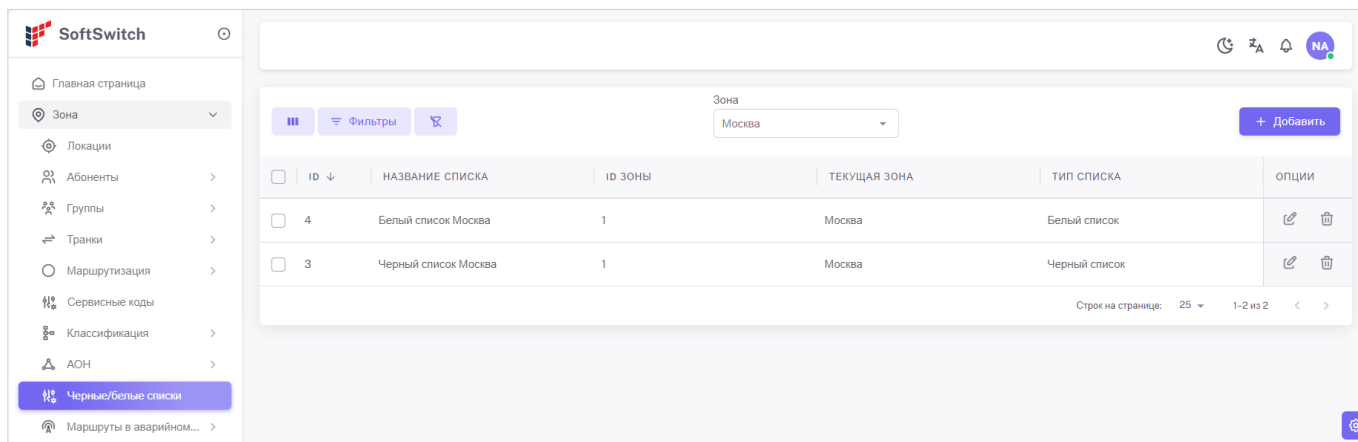



Рисунок 110. Перечень черных/белых списков

Для создания нового списка нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите название и укажите его тип (см. [Рисунок 111](#)):

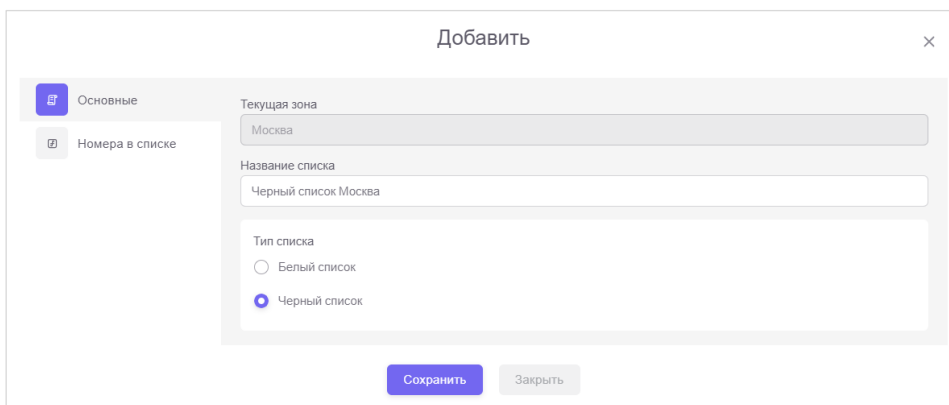


Рисунок 111. Создание черного/белого списка

После сохранения списка станет доступна для редактирования вкладка **Номера в списке** (см. [Рисунок 112](#)):

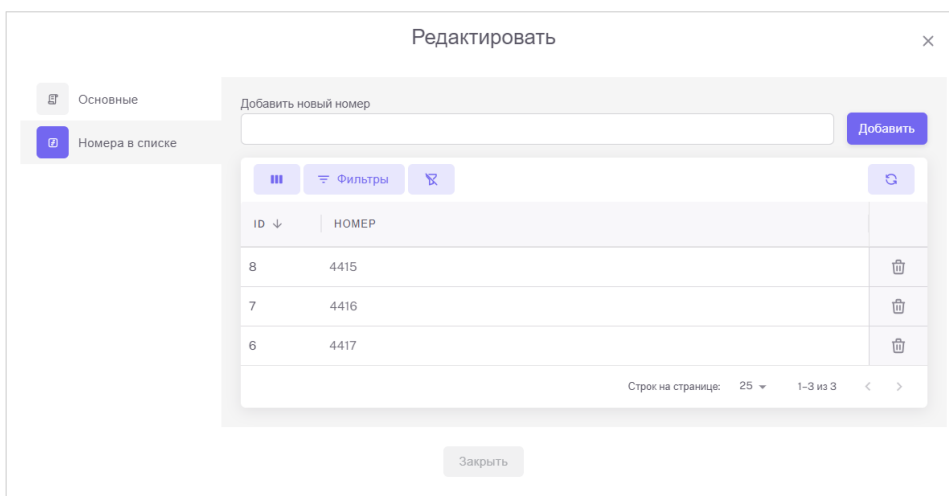


Рисунок 112. Добавление номеров в черный/белый список

10.4.10.2. Работа с черными/белыми списками

Механизм проверки черных/белых списков реализован на двух уровнях:

1. На уровне абонента, персональные черные/белые списки:
 - Формирование – в свойствах абонента (см. [Вкладка «Черные/Белые списки»](#));
 - Дополнительных настроек не требуется.
2. На уровне назначаемого абоненту профиля, групповые черные/белые списки:
 - Формирование – пункт [Создание списков](#);
 - Настройка:
 - Добавление функции «ЧБ список» и присвоение ей статуса «Активно» выполняется в профиле абонента (см. [Профиль абонента](#)).
 - Назначение абоненту профиля с включенной функцией «ЧБ список» выполняется в его свойствах (см. [Вкладка «Профили абонента»](#)).

При одновременном включении у абонента персональных черных/белых списков и применении профиля с подключенной функцией «ЧБ список» выполняются обе проверки. Для черных списков применяется логический оператор «ИЛИ» (номер блокируется при его наличии в любом из списков), для белых списков применяется логический оператор «И» (номер не блокируется при его наличии в обоих списках).

Рассмотрим несколько примеров использования черных/белых списков.

Пример 1. Организация группы шеф-секретарь. В свойствах абонента (руководителя) в **белый** список добавлен только номер секретаря. В этом случае руководитель сможет вызвать любого абонента, но будет ограничен в приеме звонков от всех кроме секретаря. Перевод вызовов от секретаря будет работать.

Пример 2. Настройки абонента: в персональный **черный** список добавлен номер 1111, в профиле добавлены и активированы функции «Входящие вызовы» и «ЧБ список», в **черный** список профиля добавлен номер 2222. Оба номера (1111 и 2222) не смогут дозвониться до абонента.

Пример 3. Настройки абонента: в персональный **белый** список добавлен номер 1111, в профиле добавлены и активированы функции «Входящие вызовы» и «ЧБ список», в **белый** список профиля добавлен номер 2222. До абонента никто не сможет дозвониться.

Пример 4. Настройки абонента: в персональный **белый** список добавлен номер 1111, в профиле добавлены и активированы функции «Входящие вызовы» и «ЧБ список», в **черный** список профиля добавлен этот же номер 1111. Вызов абоненту с номера 1111 проходит.

10.4.11. Маршруты в аварийном режиме

При наличии в системе компоненты ФЛАТ Живучий Офис, необходимо настроить схему первичной и целевой маршрутизации вызовов в аварийном режиме для локации отказоустойчивого офиса.

Параметры правил первичной и целевой маршрутизации в обычном и аварийном режимах совпадают. Создание правил смотрите в разделах [Маршрутизация первичная](#) и [Маршрутизация целевая](#).

10.5. Глобальная маршрутизация

10.5.1. Зоны

При выборе меню **Глобальная маршрутизация/Зоны** в окне отобразится список зон организации (см. [Рисунок 113](#)):


ID ↓	НАЗВАНИЕ	ДОМЕННОЕ ИМЯ	ОПЦИИ
2	Орел		
1	Москва		

Строк на странице: 25 1-2 из 2

Рисунок 113. Список зон



При установке системы автоматически создается зона с названием «По умолчанию». Переименуйте ее при необходимости.

Для создания новой зоны нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего в поля открывшейся формы внесите название и доменное имя зоны (см. [Рисунок 114](#)).

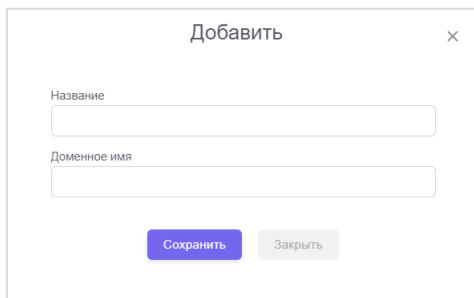


Рисунок 114. Добавление новой зоны

В форме доступны следующие поля:

Поле	Значение
Название	Название зоны.
Доменное имя	Полное имя домена (FQDN). Применяется при необходимости использования одинакового плана нумерации в разных зонах.

10.5.2. Глобальные области

В организациях с большим количеством абонентов, либо разделенных территориально на множество обособленных филиалов, может возникнуть необходимость объединения зон в глобальные области. При этом, в таблицах маршрутизации можно указывать источником звонка не конкретную зону, а их группу (см. [Глобальные маршруты](#) в разделе [Маршрутизация глобальная](#)).

Создание зон см. в главе [Создание зон](#).

Для объединения зон в глобальные области выберите меню **Глобальная маршрутизация/Глобальные области**, после чего в окне отобразится список ранее созданных глобальных областей (см. [Рисунок 115](#)):

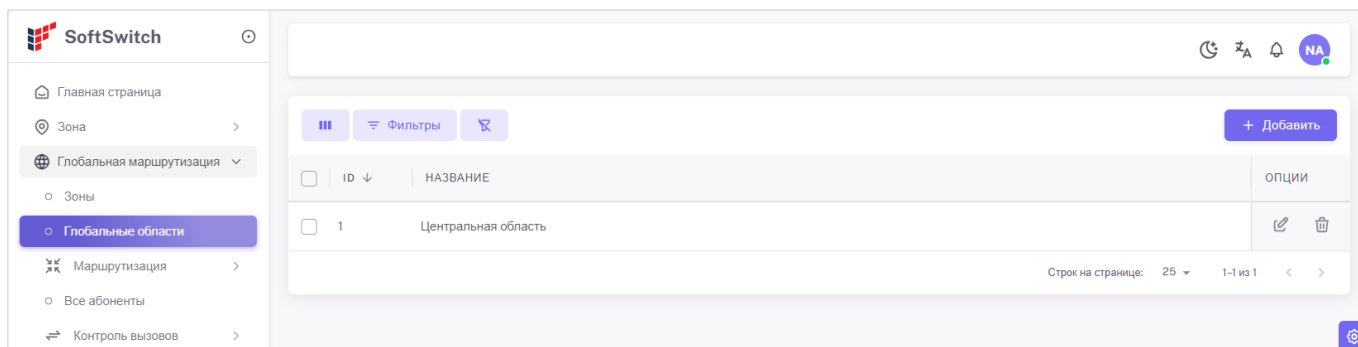



Рисунок 115. Список глобальных областей

Для создания новой глобальной области нажмите кнопку **Добавить**, а для редактирования параметров ранее созданной – значок редактирования . После чего в поле открывшейся формы внесите ее название (см. [Рисунок 116](#)):

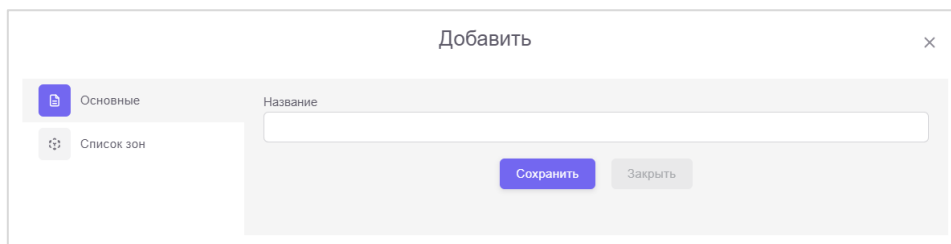


Рисунок 116. Создание глобальной области

После сохранения глобальной области станет доступна для редактирования вкладка **Список зон** (см. [Рисунок 117](#)).

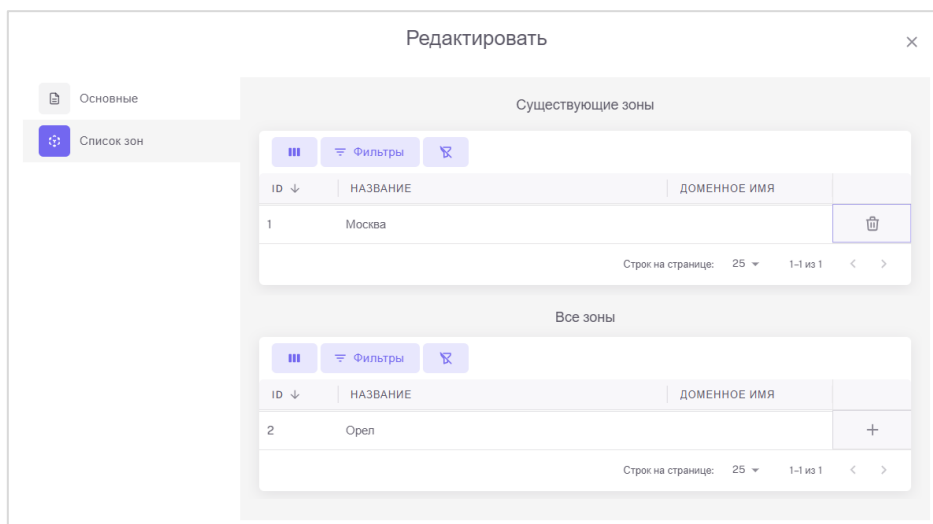


Рисунок 117. Включение зон в глобальную область

В области формы **Существующие зоны** отображается список зон, входящих в глобальную область, а в области **Все зоны** – список зон, доступных к распределению.

Для включения зоны в глобальную область нажмите кнопку **+**, а для удаления – кнопку **🗑**.

10.5.3. Маршрутизация глобальная

Глобальная маршрутизация обрабатывает вызовы, поступающие из входящих в систему зон, производит их обработку и перенаправляет согласно сконфигурированным маршрутам (см. схему [Глобальная маршрутизация](#)).

10.5.3.1. Глобальные маршруты

Для доступа к настройкам межзоновой маршрутизации выберите меню **Глобальная маршрутизация/Маршрутизация/Глобальные маршруты**. После чего в окне отобразится список созданных сущностей с указанием их характеристик (см. [Рисунок 118](#)):

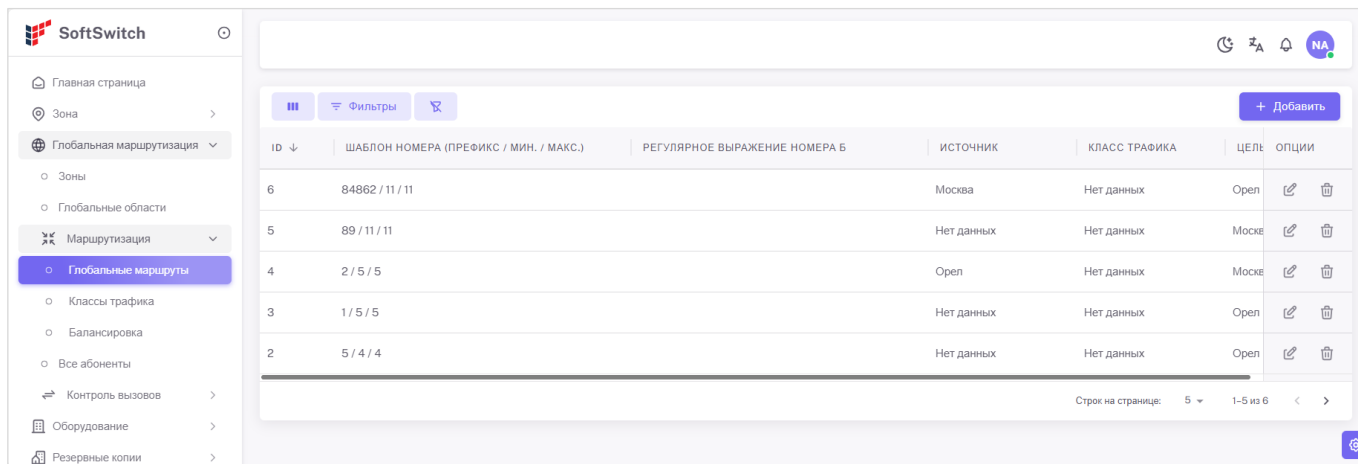


Рисунок 118. Список сохраненных глобальных маршрутов



Рекомендуется при создании правил маршрутизации использовать только один метод обработки номеров – либо с использованием шаблонов, либо с использованием регулярных выражений. Смешение методов может привести к сложно интерпретируемой маршрутизации вызовов.

Для создания нового глобального маршрута нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . В открывшейся форме выберите вариант обработки – с использованием шаблонов ([Рисунок 119](#)), или с использованием регулярных выражений (см. [Рисунок 120](#)).

Добавить ×

Использовать шаблоны
 Использовать регулярные выражения

Шаблон номера (Префикс / Мин. / Макс.)

Тип источника

Зона

Класс трафика

Транк

Цель

Рисунок 119. Создание глобального маршрута с использованием шаблонов

В форме доступны следующие поля:

Поле	Значение
Шаблон номера (Префикс / Мин. / Макс.)	Описание шаблона номера состоит из трех полей: Первое поле – префикс номера, проходящего обработку. Второе и третье поле – минимальное и максимальное количество знаков, ограничивающее диапазон проходящих обработку номеров.
Тип источника	Параметр, описывающий тип источника вызова. Предопределены следующие значения:

Поле	Значение
	<p>Все зоны – все источники вызова.</p> <p>Зона – источником вызова является конкретная зона.</p> <p>Глобальные области – источником вызова являются зоны, объединенные в <i>Глобальные области</i>.</p> <p>При выборе значения Зона или Глобальные области форма дополнится полем выбора источника вызова.</p>
Класс трафика	Выбор класса трафика. Определение классов и их назначение см. в главе <i>Классы трафика</i> .
Транк	<p>Выбор типа транка. Предопределены следующие значения:</p> <p>Зоны – направлением вызова являются зоны.</p> <p>Правила назначения – направлением вызова является балансировщик нагрузки (см. <i>Балансировка</i>).</p> <p>Нет – направление вызова заблокировано.</p> <p>При выборе значения Зоны или Правила назначения форма дополнится полем выбора соответствующей цели.</p>

Рисунок 120. Создание глобального маршрута с использованием регулярных выражений

В форме доступны следующие поля:

Поле	Значение
Блок проверки регулярного выражения	<p>Для проверки совпадения регулярного выражения с номером введите в следующие поля:</p> <p>Номер – обрабатываемый номер.</p> <p>Регулярное выражение – проверяемое регулярное выражение.</p> <p>После нажатия кнопки Тест на экран будет выведено сообщение о результате проверки.</p>
Регулярное выражение номера Б	<p>Регулярное выражение для обработки номера получателя вызова (см. <i>Регулярные выражения при проверке номера</i>).</p> <p>Допустимые символы: <code>[^0123456789-+?!X*#</code></p>
Тип источника	<p>Параметр, описывающий тип источника вызова.</p> <p>Предопределены следующие значения:</p>

Поле	Значение
	<p>Все зоны – все источники вызова.</p> <p>Зона – источником вызова является конкретная зона.</p> <p>Глобальные области – источником вызова являются зоны, объединенные в <i>Глобальные области</i>.</p> <p>При выборе значения Зона или Глобальные области форма дополнится полем выбора источника вызова.</p>
Класс трафика	Выбор класса трафика. Определение классов и их назначение см. в главе <i>Классы трафика</i> .
Транк	<p>Выбор типа транка. Предопределены следующие значения:</p> <p>Зоны – направлением вызова являются зоны.</p> <p>Правила назначения – направлением вызова является балансировщик нагрузки (см. <i>Балансировка</i>).</p> <p>Нет – направление вызова заблокировано.</p> <p>При выборе значения Зоны или Правила назначения форма дополнится полем выбора соответствующей цели.</p>

Рассмотрим несколько примеров правил глобальной маршрутизации.

Пример 1. Вызов на 11-значный номер, начинающийся с «89», пришедший с любого источника и имеющий класс трафика «Международный», направлять в область целевой маршрутизации зоны «Москва» (см. *Рисунок 121*):

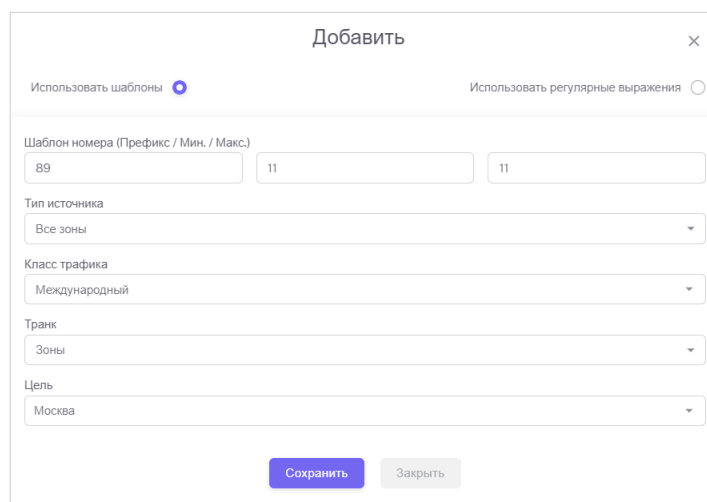


Рисунок 121. Глобальный маршрут - международный в зону Москва

Пример 2. Вызов на 11-значный номер, начинающийся с «84862», приходящий из зоны «Москва» и имеющий класс трафика «Междугородний», направлять в область целевой маршрутизации зоны «Орел» (см. *Рисунок 122*):

Рисунок 122. Глобальный маршрут – междугородний Москва - Орел

10.5.3.2. Классы трафика

Для удобства управления вызовами вводится понятие класс трафика. Позволяет в рамках глобальной и первичной маршрутизации ограничивать правила обработки голосовых вызовов.

Для каждого вида маршрутизации создаются свои классы трафика – для глобальной маршрутизации классы трафика имеют принадлежность «Глобальная», для первичной маршрутизации – принадлежность «Зона» (см. [Классы трафика](#)).

Для доступа к списку классов трафика глобальной маршрутизации выберите меню **Глобальная маршрутизация/Маршрутизация/Классы трафика**. После чего в окне отобразится список созданных сущностей с указанием названия и описания (см. [Рисунок 123](#)):

Рисунок 123. Список классов трафика глобальной маршрутизации

Для создания нового класса трафика нажмите кнопку **Добавить**, а для изменения ранее созданного – значок редактирования . После чего в поля открывшейся формы внесите название и описание (см. [Рисунок 124](#)):

Рисунок 124. Создание класса трафика глобальной маршрутизации

В системе ФЛАТ SoftSwitch predefined классов трафика нет.

Взаимосвязь классов трафика с другими параметрами системы ФЛАТ SoftSwitch показана на примерах конфигурирования глобальной и первичной маршрутизации (см. [Применение классов сервиса и ограничений](#)).

10.5.3.3. Балансировка

В системе ФЛАТ SoftSwitch реализована балансировка нагрузки по различным критериям. На глобальном уровне происходит балансировка нагрузки между различными зонами.

Для доступа к настройкам выберите меню **Глобальная маршрутизация/Маршрутизация/Балансировка**. После чего в окне отобразится список созданных сущностей с указанием названия, типа и описания (см. [Рисунок 125](#)):

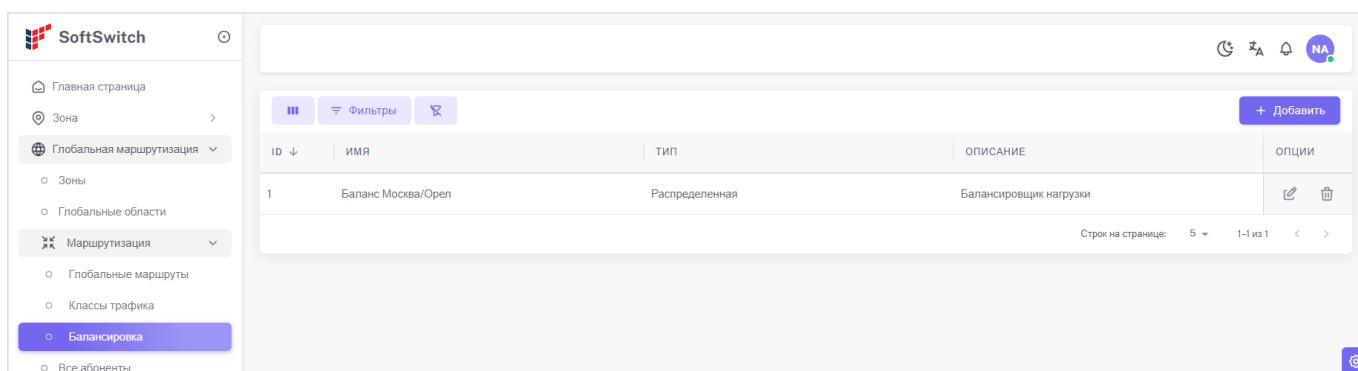


Рисунок 125. Список балансировок глобальной маршрутизации

Для создания новой балансировки нажмите кнопку **Добавить**, а для редактирования параметров ранее созданной – значок редактирования . После чего в поля открывшейся формы внесите ее параметры (см. [Рисунок 126](#)).

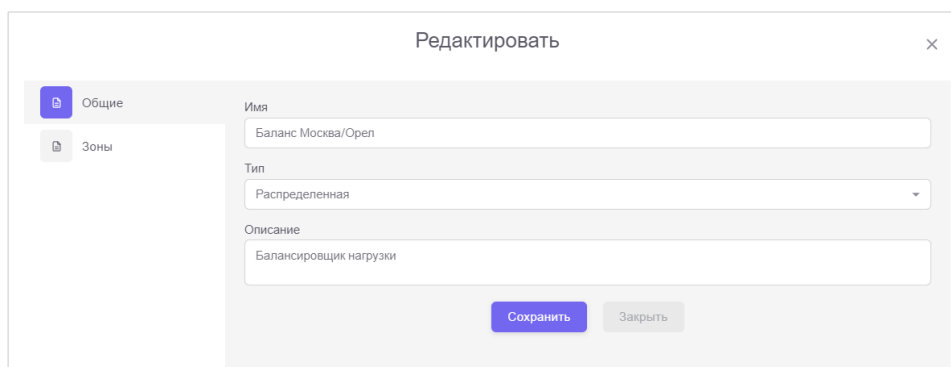


Рисунок 126. Создание балансировки

В форме доступны следующие поля:

Поле	Значение
Имя	Название балансировки.
Тип	Тип балансировки. Предопределены следующие значения: Линейная – маршрут выбирается из доступных с учетом приоритета. Циклическая – маршрут выбирается из доступных в порядке циклического перебора начиная с первого в списке. Распределенная – маршрут выбирается из доступных с учетом приоритета и веса. Первичный выбор маршрута происходит по

Поле	Значение
	значению приоритета. При наличии маршрутов с одинаковым приоритетом, нагрузка перераспределяется в % отношении согласно указанному весу маршрута.
Описание	Описание балансировки.

После сохранения балансировки станет доступна для редактирования вкладка **Зоны** (см. [Рисунок 127](#)).

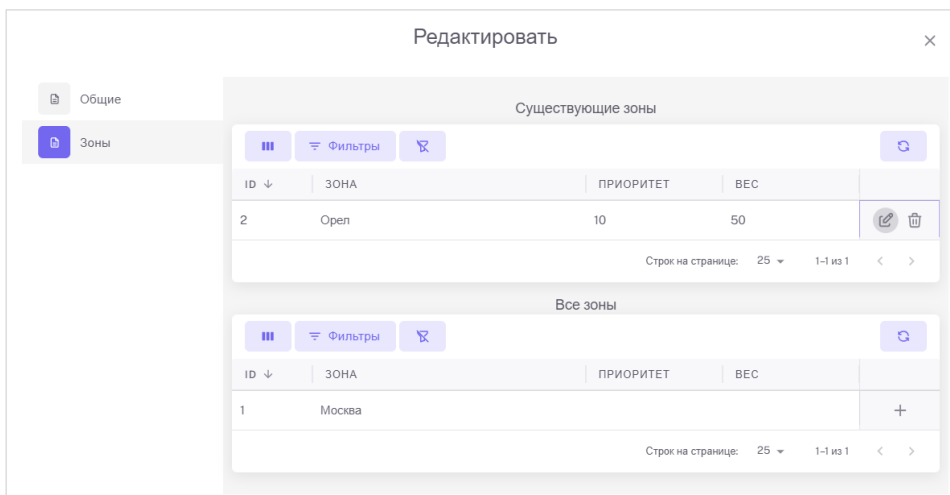







Рисунок 127. Параметры балансировки, вкладка «Зоны»

В области формы **Существующие зоны** отображается список входящих в балансировку зон, а в области **Все зоны** – список зон, доступных к распределению.

Для включения зоны в балансировку нажмите кнопку , укажите приоритет и вес, сохраните кнопкой . Для удаления зоны из балансировки нажмите кнопку .

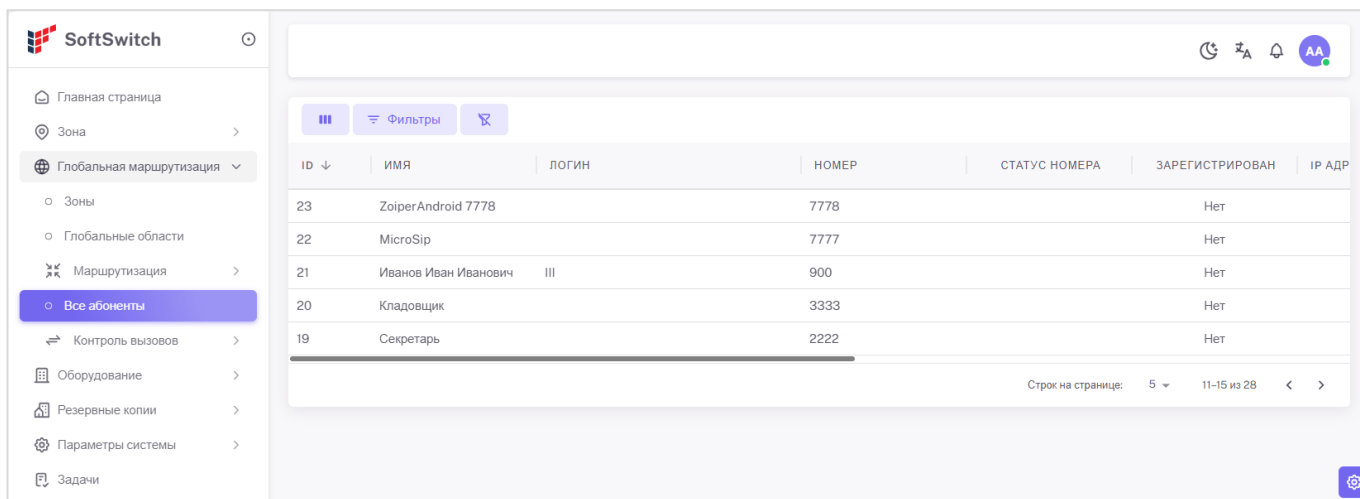
Для изменения параметров включенной в балансировку зоны нажмите кнопку , укажите новые значения и сохраните кнопкой .

Значения параметров балансировки:

Поле	Значение
Приоритет	Целочисленное значение приоритета по отношению к другим маршрутам. Чем меньше значение, тем выше приоритет.
Вес	Вес маршрута в % от общей нагрузки. Общий вес маршрутов с одинаковым приоритетом не должен превышать 100%.

10.5.4. Все абоненты

Для поиска абонентов в глобальном списке выберите меню **Глобальная маршрутизация/Все абоненты**, после чего в окне отобразится список всех абонентов системы с указанием учетных данных и параметров регистрации (см. [Рисунок 128](#)).



The screenshot displays the SoftSwitch administration interface. On the left is a navigation menu with the following items: Главная страница, Зона, Глобальная маршрутизация (expanded), Зоны, Глобальные области, Маршрутизация, Все абоненты (highlighted), Контроль вызовов, Оборудование, Резервные копии, Параметры системы, and Задачи. The main content area shows a table of subscribers with columns: ID, ИМЯ, ЛОГИН, НОМЕР, СТАТУС НОМЕРА, ЗАРЕГИСТРИРОВАН, and IP АДР. The table contains five rows of data. Below the table, there is a pagination control showing 'Строк на странице: 5' and '11-15 из 28'.

ID ↓	ИМЯ	ЛОГИН	НОМЕР	СТАТУС НОМЕРА	ЗАРЕГИСТРИРОВАН	IP АДР
23	ZoiperAndroid 7778		7778		Нет	
22	MicroSip		7777		Нет	
21	Иванов Иван Иванович	III	900		Нет	
20	Кладовщик		3333		Нет	
19	Секретарь		2222		Нет	

Рисунок 128. Поиск абонентов в глобальном списке

10.5.5. Контроль вызовов

Использование механизма Call Admission Control (CAC) для регулирования трафика в голосовой связи и обеспечения высокого качества обслуживания пользователей находится в стадии разработки.

10.6. Оборудование

В данном меню WEB-интерфейса системы ФЛАТ SoftSwitch настраивается конфигурация отказоустойчивого кластера, задаются параметры доступных медиаресурсов и выполняется настройка Живучего Офиса.

10.6.1. Кластер

Кластер ФЛАТ SoftSwitch – объединение двух узлов, работающих в режиме Active-Active, устанавливаемых на различные серверы, часто разнесенных территориально. Возможен только один кластер серверов на систему.

При создании кластера необходимо в WEB-интерфейсе двух узлов перекрестно внести параметры второго узла. После чего автоматически произойдет синхронизация, а в поле «Статус» отразится текущее состояние узла.

Для доступа к параметрам созданного кластера выберите меню **Оборудование/Кластер**, после чего в окне отобразятся его настройки, с указанием названия, IP-адреса хоста, используемого порта и статуса (см. [Рисунок 129](#)):

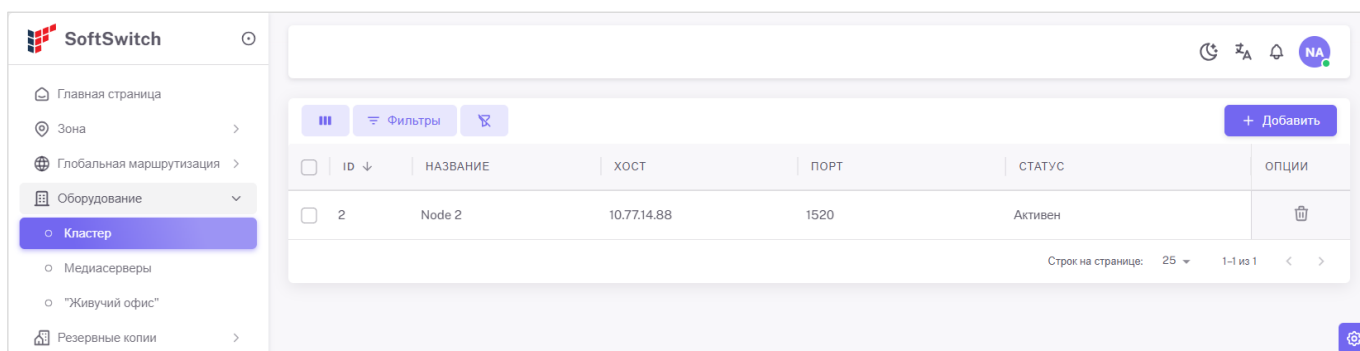


Рисунок 129. Настройки кластера

Для создания записи о втором узле кластера нажмите кнопку **Добавить**. После чего в поля открывшейся формы внесите его параметры (см. [Рисунок 130](#)):

Добавить ×

Название

Хост

Порт

Рисунок 130. Создание кластера

В форме доступны следующие поля:

Поле	Значение
Название	Название второго узла.
Хост	IP-адрес второго узла.
Порт	Порт взаимодействия. Значение по умолчанию «1520».

В WEB-интерфейсе корректность адреса хоста и номера порта не проверяется. Возможные ошибки сохраняются в лог-файлах.



После создания кластера необходимо поочередно перезагрузить оба узла.

10.6.2. Медиасерверы

Функционально Медиасервер представляет собой два отдельных сервиса, отвечающих за разные направления обработки:

- **Mediasrv** – за обработку медиа потоков, музыку на удержании, уведомления голосом и создание конференций;
- **SRClient** – за проксирование RTP и запись SIPREC.

В рамках концепции построения системы ФЛАТ SoftSwitch в данном руководстве Медиасервер рассматривается как единый модуль, лишь по мере необходимости отмечается разделение на отдельные сервисы.

Количество подключаемых в системе модулей Медиасервера не ограничивается и определяется нагрузкой, целесообразностью и топологией сети.

Для управления настройками медиаресурсов выберите меню **Оборудование/Медиасерверы**, после чего в окне отобразится список ранее сохраненных Медиасерверов с указанием адреса хоста, номера используемого порта и выполняемых функций (см. [Рисунок 131](#)):

ID	ХОСТ	ПОРТ	ФУНКЦИИ	ОПЦИИ
15	10.77.14.49	2429	Запись разговоров	
13	10.77.14.88	2429	Запись разговоров	
12	10.77.14.88	2427	Конференции, Проигрывание звуковых файлов	
11	10.77.13.34	2429	Запись разговоров	
10	10.77.13.34	2427	Конференции, Проигрывание звуковых файлов	

Рисунок 131. Список Медиасерверов

Для создания нового Медиасервера нажмите кнопку **Добавить**, после чего в поля открывшейся формы внесите его параметры (см [Рисунок 132](#)):

Рисунок 132. Создание Медиа сервера

В форме доступны следующие поля:

Поле	Значение
Хост	IP-адрес хоста Медиа сервера.
Порт	Для сервиса Mediasrv (проигрывание звуковых файлов и организация конференций) используется порт 2427. Для сервиса SRClient (запись разговоров) используется порт 2429.
Функции	Укажите выполняемые Медиа сервером функции: <ul style="list-style-type: none"> • Проигрывание звуковых файлов. • Конференции. • Запись разговоров. • Прокси. Включение возможности проксирования RTP-трафика. Само проксирование настраивается в свойствах локации (см. Вкладка «Параметры локации»).

В системе ФЛАТ SoftSwitch допустимо вместо стандартных звуковых оповещений использовать свои звуковые файлы. Формат пользовательского звукового файла – расширение WAV, кодек G.711 A-law (PCMA), частота дискретизации 8 кГц, битрейт 64 кбит/с. Примеры конвертации см. [Формат аудиофайлов](#).

Загрузите пользовательские звуковые файлы по адресу `/opt/flat/fss-mediasrv/` соответствующего Медиа сервера. Переименование звуковых файлов вместо стандартных см. в главе [Вкладка «Медиа серверы»](#).

10.6.3. Живучий Офис

Живучий Офис (branch office) – специально сконфигурированное ядро SoftSwitch с функционалом локальной выживаемости и дополнительным медиа сервером для работы с RTP локально на площадке.



Живучий Офис имеет стандартный WEB-интерфейс управления, но его **создание и конфигурирование выполняется на основном узле ФЛАТ SoftSwitch**. В локальном WEB-интерфейсе Живучего Офиса указывается только адрес основного узла.

10.6.3.1. Настройки в WEB-интерфейсе основного узла

На основном узле ФЛАТ SoftSwitch для формирования Живучего Офиса необходимо создать две сущности – отдельную локацию выбранной зоны, в настройках которой выполняется его конфигурирование, и связанную с локацией запись, в которой указываются параметры подключения.

10.6.3.1.1. Создание и настройка локации Живучего Офиса

Для создания локации Живучего Офиса перейдите в меню **Зона/Локации**, в раскрывающемся списке выберите зону принадлежности Живучего Офиса и нажмите кнопку **Добавить**. После чего в поля открывшейся формы внесите название и краткое описание локации Живучего Офиса (см. [Рисунок 133](#)):

Рисунок 133. Создание локации Живучего Офиса

Запомните значение ID созданной локации, которое понадобится для дальнейших настроек. В нашем случае это «6» (см. [Рисунок 134](#)):

ID	ID ЗОНЫ	НАЗВАНИЕ	ЗОНА	КОММЕНТАРИЙ	ОПЦИИ
6	1	Branch	Москва	Живучий Офис в зоне Москва	[Edit] [Delete]
2	1	Дополнительный офис	Москва		[Edit] [Delete]
1	1	Головной офис	Москва		[Edit] [Delete]

Рисунок 134. ID созданной локации

10.6.3.1.2. Регистрационная запись Живучего Офиса

Для доступа к списку созданных сущностей выберите меню **Оборудование/Живучий офис**, после чего в окне отобразится список регистрационных записей, с указанием названия, IP-адреса хоста, номера используемого порта, статуса активности, родительской зоны и связанной с ним локации (см. [Рисунок 135](#)):

ID	НАЗВАНИЕ	ХОСТ	ПОРТ	СТАТУС	ЗОНА	ЛОКАЦИЯ	ОПЦИИ
3	Удаленный офис	10.77.1.79	1540	Активен	Москва	Branch	[Delete]

Рисунок 135. Список подключенных Живучих Офисов

Для создания новой регистрационной записи Живучего Офиса нажмите кнопку **Добавить**. После чего в поля открывшейся формы внесите его параметры (см. [Рисунок 136](#)):

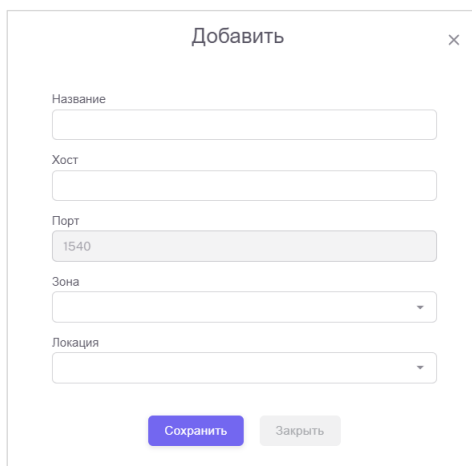


Рисунок 136. Добавление Живучего Офиса

В форме доступны следующие поля:

Поле	Значение
Название	Название Живучего Офиса.
Хост	IP-адрес хоста Живучего Офиса.
Порт	Порт взаимодействия. Значение по умолчанию «1540».
Зона	Выбор зоны принадлежности Живучего Офиса.
Локация	Привязка Живучего Офиса к определенной локации, в настройках которой выполняется его конфигурирование.

Сохраните изменения.

При доступности узла Живучего Офиса его статус примет значение «Активен».

10.6.3.1.3. Создание абонентов Живучего Офиса

Абоненты Живучего Офиса создаются в связанной с ним локации (см. [Абоненты](#)).

10.6.3.1.4. Создание транков

Транки Живучего Офиса создаются в связанной с ним локации (см. [Транки](#)).

10.6.3.1.5. Маршрутизация вне аварийного режима

Создание правил маршрутизации вне аварийного режима рассматривается в главах [Маршрутизация первичная](#) и [Маршрутизация целевая](#).

10.6.3.1.6. Маршрутизация в аварийном режиме

В случае разрыва связи с основным узлом Живучий Офис берет на себя обработку правил маршрутизации вызовов. Для автономного режима работы может быть настроена специальная схема первичной и целевой маршрутизации.

Создание правил первичной и целевой маршрутизации в аварийном режиме см. в разделе [Маршруты в аварийном режиме](#).

10.6.3.1.7. Медиасерверы Живучего Офиса

Создание медиаресурсов рассмотрено в главе [Медиасерверы](#).

Привязка медиаресурсов к Живучему Офису выполняется в свойствах связанной с ним локации (см. [Вкладка «Медиасерверы»](#)).

10.6.3.2. Настройки на стороне узла Живучего Офиса:

В адресной строке браузера укажите IP-адрес хоста Живучего Офиса и в открывшейся форме авторизуйтесь с учетной записью администратора.

На стороне узла Живучего Офиса необходимо выполнить следующие настройки:

10.6.3.2.1. Привязка Живучего Офиса к основному серверу

Выберите меню **Оборудование/Кластер** и нажмите кнопку **Добавить**. В поля открывшейся формы внесите параметры основного сервера (см. [Рисунок 137](#)):

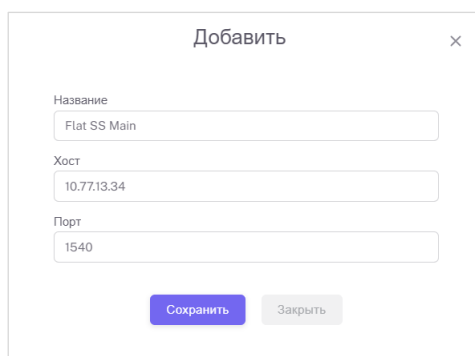


Рисунок 137. Привязка Живучего Офиса к основному серверу

В форме доступны следующие поля:

Поле	Значение
Название	Название основного сервера.
Хост	IP-адрес основного сервера.
Порт	Порт взаимодействия. Значение по умолчанию «1540».

10.6.3.2.2. Привязка Живучего Офиса к выделенной локации

Для привязки Живучего Офиса к локации, в настройках которой выполняется его конфигурирование, необходимо внести изменения в конфигурационный файл. Для этого подключитесь к узлу Живучего Офиса по SSH и откройте на редактирование файл `/opt/flat/fss-server/settings.ini`.

В разделе **[General]** укажите следующий параметр:

LocationID=6 – ID локации Живучего Офиса, в нашем примере это значение «6» (см. [ID созданной локации](#)).

Сохраните изменения и перезагрузите сервис командой:

```
service flat_ss restart
```

10.6.3.2.3. Проверка привязки к основному серверу

Проконтролируйте статус привязки к основному серверу в WEB-интерфейсе узла Живучего Офиса. Выберите меню **Оборудование/Кластер** – статус должен быть «Активен» (см. [Рисунок 138](#)):

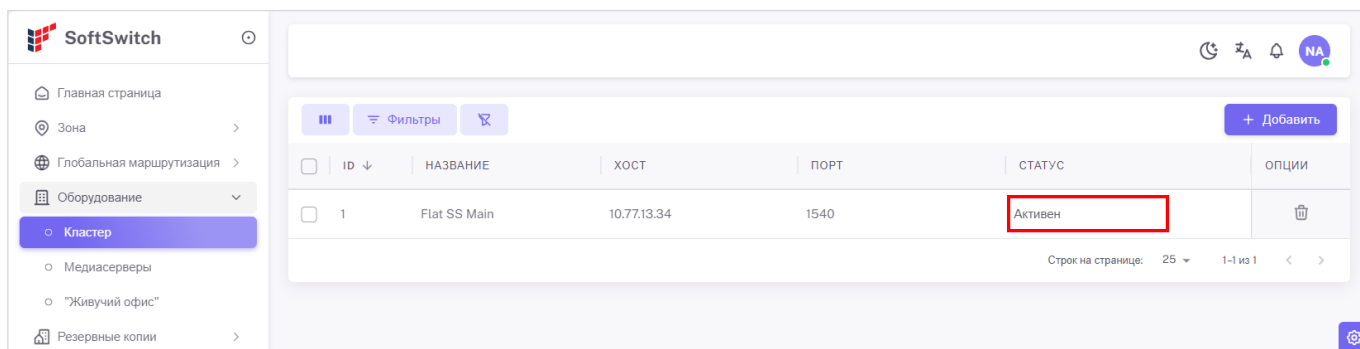


Рисунок 138. Статус привязки к основному серверу

10.6.3.3. Настройка IP-телефонов абонентов Живучего Офиса

В случае потери связи с основным узлом ФЛАТ SoftSwitch, телефоны Живучего Офиса должны переключиться на локальный узел и продолжить работать в автономном режиме. Для этого в их настройках необходимо ввести адрес как основного, так и резервного сервера. Это удобно сделать для всех аппаратов с помощью ПО ФЛАТ Device Manager (в данном руководстве не рассматривается), либо вручную для каждого телефона по отдельности.

10.7. Резервные копии

Система ФЛАТ SoftSwitch с заданной периодичностью сохраняет копии БД. Возможно создание резервной копии вручную.

Функционал восстановления из резервной копии находится в стадии разработки.

10.7.1. Цели

Вначале необходимо задать способ хранения данных. Предопределены два способа, отличающиеся дополнительными настройками – хранение на **FTP-сервере** и **локально**. При использовании FTP-сервера доступна передача по протоколу SFTP.

10.7.1.1. FTP-серверы

На FTP-сервере сохраняются резервные копии базы данных.

Для управления настройками хранения на **FTP-сервере** выберите меню **Резервные копии/Цели/FTP-серверы**. После чего в окне отобразится список записей с указанием названия, IP-адреса хоста и порта, удаленного пути хранения (см. [Рисунок 139](#)):

ID ↓	ИМЯ	ХОСТ	ПОРТ	УДАЛЕННЫЙ ПУТЬ	ОПЦИИ
2	sftp	10.775.39	22		
1	FTP	172.30.30.108	21		

Рисунок 139. Список записей хранения резервных копий на FTP-сервере

Для создания новой записи нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 140](#)):

Добавить ×

Название

Хост

Порт

Логин

Пароль

Удаленный путь

SFTP

Рисунок 140. Создание пути хранения резервных копий на FTP-сервере

В форме доступны следующие поля:

Поле	Значение
Название	Название ресурса.
Хост	IP-адрес FTP-сервера.
Порт	Порт FTP-сервера.
Логин	Логин учетной записи для доступа к FTP-серверу.
Пароль	Пароль учетной записи для доступа к FTP-серверу.
Удаленный путь	Путь хранения на FTP-сервере. При пустом значении резервные копии сохраняются в корне домашней папки указанного пользователя. Например, для пользователя с логином <i>user_ftp</i> путь хранения будет <i>/home/user_ftp/</i>
SFTP	Отправка по протоколу SFTP.

На этапе конфигурирования не отслеживается корректность пути хранения резервных копий. Возможные ошибки проверяйте в локально сохраняемых логах (см. [Логирование](#)).

10.7.1.2. Локальные пути

Настройки определяют путь хранения резервных копий баз данных, тарификационных записей (CDR-файлов) и позволяют задавать срок хранения.

Для управления настройками хранения **локально** выберите меню **Резервные копии/Цели/Локальные пути**. После чего в окне отобразится список записей с указанием названия, пути и срока хранения (см. [Рисунок 141](#)).

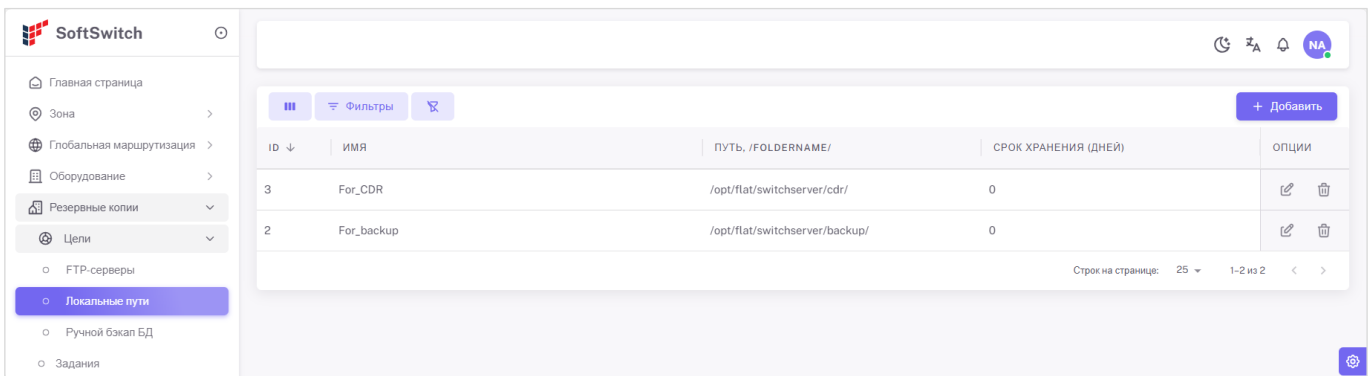


Рисунок 141. Список записей локального хранения

Для создания новой записи нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 142](#)):

Редактировать ×

Название

Путь, /folderName/

Использовать срок хранения

Срок хранения (дней)

Рисунок 142. Редактирование записи локального хранения

В форме доступны следующие поля:

Поле	Значение
Название	Название ресурса.
Путь, /folderName/	Путь хранения.
Использовать срок хранения	Задание срока хранения в днях.

На этапе конфигурирования не отслеживается корректность пути хранения резервных копий. Возможные ошибки проверяйте в локально сохраняемых логах (см. [Логирование](#)).



В системе предусмотрены следующие локальные пути хранения, укажите их:

- резервных копий базы данных **/opt/flat/fss-server/backup/**;
- тарификационных записей (CDR-файлов) **/opt/flat/fss-server/cdr/**.

10.7.1.3. Ручной бэкап БД

Для просмотра списка ранее созданных копий БД и CDR-файлов, хранящихся локально, а также для создания новой ручной копии выберите меню **Резервные копии/Цели/Ручной бэкап БД**. После чего в окне отобразится список сущностей, с указанием пути хранения файла, его названия, размера и времени создания (см. [Рисунок 143](#)):

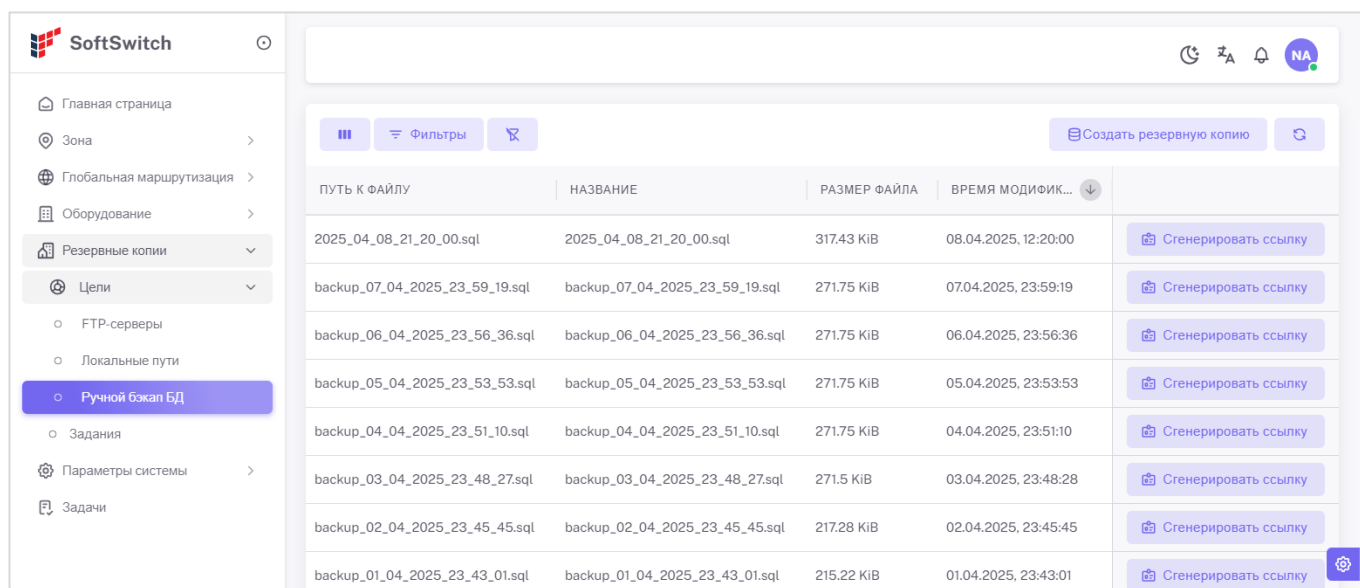
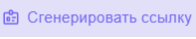



Рисунок 143. Список резервных копий БД

Для обновления списка нажмите кнопку , а для создания новой копии – кнопку .

Для скачивания копии БД вначале нажмите кнопку , а затем кнопку , после чего файл резервной копии будет загружен в папку по умолчанию ПК текущего пользователя.



Если во время создания резервной копии или восстановлении из нее возникают ошибки, необходимо дать права на чтение и запись на каталог, указанный в параметре **backup_dir** конфигурационного файла бэкенда **/usr/lib/flatSoftSwitchBackend/config.yml**.

Пример команды:

```
# chmod 777 /opt/flat/fss-server/backup/
```

10.7.2. Задания

10.7.2.1. Настройка расписания резервного копирования

Для управления заданиями резервного копирования БД выберите меню **Резервные копии/Задания**. После чего в окне отобразится список записей с указанием типа и названия цели хранения, периодичности и времени начала копирования, даты и времени последнего выполнения задания (см. [Рисунок 144](#)):

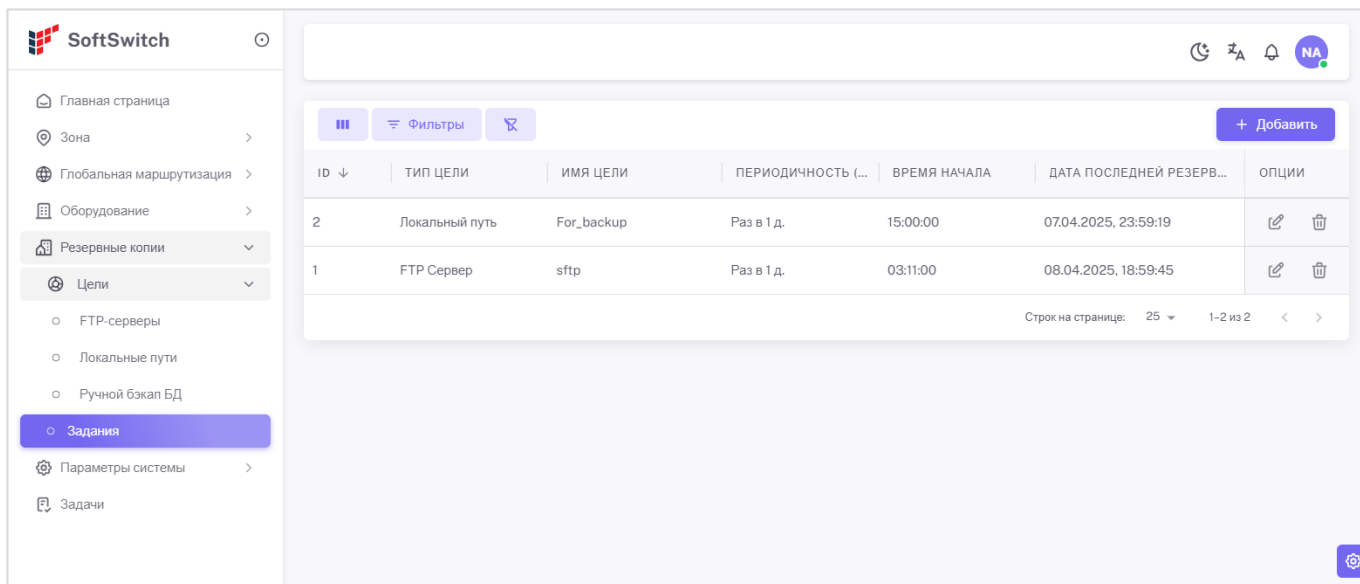


Рисунок 144. Расписание резервного копирования

Для создания новой записи нажмите кнопку **Добавить**, а для редактирования существующей – значок редактирования . После чего в поля открывшейся формы внесите необходимые параметры (см. [Рисунок 145](#)):

Добавить ×

Тип цели

Имя локальной цели

Периодичность (раз в X дней)

Время начала задания

Рисунок 145. Создание записи расписания резервного копирования

В форме доступны следующие поля:

Поле	Значение
Тип цели	Выбор типа цели резервного копирования. Предопределены следующие типы: <ul style="list-style-type: none"> • FTP-сервер • Локальный путь
Имя FTP-сервера/Имя локальной цели	Выбор места хранения резервных копий (см. Цели).

Поле	Значение
Периодичность (раз в X дней)	Периодичность создания резервной копии в днях.
Время начала задания	Время начала выполнения задания.

10.8. Задачи

Для просмотра списка задач выберите меню **Задачи**, после чего в окне отобразится список сформированных сущностей с указанием названия, инициатора, статуса выполнения, типа задачи, времени начала и времени завершения (см. [Рисунок 146](#)):

ID	НАЗВАНИЕ	ИНИЦИАТОР	СТАТУС	ТИП	СОЗДАНО	ОБНОВЛЕНО
13	zones/abonents	admin	Выполняется	Экспорт	2025-04-17 22:22:15	2025-04-17 22:23:10
12	zones/abonents	admin	Успешно	Экспорт	2025-04-11 15:55:13	2025-04-11 15:55:23

Рисунок 146. Список задач

Для просмотра подробной информации о задаче раскройте информационное окно кнопкой **+**, расположенной в ее строке (см. [Рисунок 147](#)):

ID	НАЗВАНИЕ	ИНИЦИАТОР	СТАТУС	ТИП	СОЗДАНО	ОБНОВЛЕНО
13	zones/abonents	admin	Выполняется	Экспорт	2025-04-17 22:22:15	2025-04-17 22:23:10
12	zones/abonents	admin	Успешно	Экспорт	2025-04-11 15:55:13	2025-04-11 15:55:23

ID: 12
 Имя: zones/abonents
 Размер файла: 7.2 KiB
 Статус: success
 Создано: 2025-04-11 15:55:13
 Обновлено: 2025-04-11 15:55:23
 Сообщение:
 Количество записей: 28;

Рисунок 147. Подробная информация о задаче

Для скачивания результата выполнения задачи, например, выгрузки списка абонентов, нажмите кнопку **⋮**, в раскрывшемся списке выберите пункт **Сгенерировать ссылку**, а затем **Скачать файл**, после чего файл в формате CSV (Comma-Separated Values) будет загружен в папку по умолчанию ПК текущего пользователя.

При нажатии кнопки **⋮**, так же будут доступны следующие действия:

- остановить задачу;
- повторить задачу;
- удалить задачу.

Приложения

Изменение наименований пакетов

В процессе развития системы ФЛАТ SoftSwitch от версии v.4.1 до версии v.4.2 поэтапно изменяются наименования инсталляционных пакетов, сервисов, каталогов расположения, файлов журналов событий.

Таблица 4. Изменение наименований пакетов

Наименование подсистемы	Старое название пакета	Новое название пакета
Фронтенд WEB-интерфейса ФЛАТ SoftSwitch	softswitch-frontend	fss-frontend
Бэкенд WEB-интерфейса ФЛАТ SoftSwitch	flatsoftswitchbackend	fss-backend
Сервис Mediasrv	mediasrv	fss-mediasrv
Сервис SRClient	srclient	fss-srclient
Ядро ФЛАТ SoftSwitch	fss-server	fss-server
Сервис FlatFileManager	flatFileManager	fss-file
Бэкенд WEB-интерфейса ЛК пользователя	flatSoftSwitchLK	lc-backend
Фронтенд WEB-интерфейса ЛК пользователя	lc-softswitch-frontend	lc-frontend

Одновременно с изменением наименований пакетов меняются названия связанных с ними ресурсов:

- Место расположения всех сервисов /opt/flat/"Название пакета"
- Лог файлы: /var/log/flat/"Название пакета"
- Название сервиса: /usr/lib/systemd/system/"Название пакета".service
- Настройка для logrotation: /etc/logrotate.d/"Название пакета".conf
- Файл nginx: /etc/nginx/sites-available/"Название пакета"

Лицензионное соглашение



ВАЖНО! ПРОЧТИТЕ ВНИМАТЕЛЬНО!

В связи с особенностями лицензирования, стоимость ПО «ФЛАТ» рассчитывается индивидуально, дополнительную информацию можно получить по электронной почте: info@flat-soft.ru. После отправки запроса, наши сотрудники свяжутся с Вами для детальной консультации и предоставления расчёта в соответствии с техническими характеристиками объекта автоматизации.

Данное Лицензионное соглашение с конечным пользователем является юридическим соглашением между вами (физическим или юридическим лицом) и ООО «ФЛАТ» по использованию программного обеспечения, сопровождающего данное Лицензионное соглашение с конечным пользователем. В это программное обеспечение входит само компьютерное программное обеспечение, а также могут входить соответствующие носители, печатные материалы и "онлайновая" или электронная документация («Программное обеспечение»). Программное обеспечение может сопровождаться изменением или дополнением к данному Лицензионному соглашению с конечным пользователем.

ЕСЛИ ВЫ УСТАНОВЛИВАЕТЕ, КОПИРУЕТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ИЛИ ИСПОЛЬЗУЕТЕ ЕГО КАКИМ-ЛИБО ДРУГИМ СПОСОБОМ, ТЕМ САМЫМ ВЫ ПОДТВЕРЖДАЕТЕ СВОЕ СОГЛАСИЕ СОБЛЮДАТЬ УСЛОВИЯ ДАННОГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ. ЕСЛИ ВЫ НЕ СОГЛАСНЫ, НЕ УСТАНОВЛИВАЙТЕ, НЕ КОПИРУЙТЕ И НЕ ИСПОЛЬЗУЙТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. ВЫ МОЖЕТЕ ВЕРНУТЬ ЕГО В МЕСТО ПРИОБРЕТЕНИЯ ДЛЯ ПОЛУЧЕНИЯ ВОЗМЕЩЕНИЯ ЕГО СТОИМОСТИ В ПОЛНОМ ОБЪЕМЕ, ЕСЛИ ЭТО ПРИМЕНИМО.

Предоставление лицензии

ООО «ФЛАТ» предоставляет вам следующие права при условии выполнения вами всех условий данного Лицензионного соглашения с конечным пользователем:

1.1 Установка и использование. Вы можете установить, использовать, осуществлять доступ, отображать и запускать одну копию Программного обеспечения и обращаться к одной копии Программного обеспечения на одном компьютере – рабочей станции, терминале или другом устройстве («Рабочая станция»). В каждый момент времени.

1.2 Хранение/сетевое использование. Вы также можете хранить или установить копию Программного обеспечения на устройстве хранения данных, таком как сетевой сервер, который используется только для установки или запуска Программного обеспечения на других ваших Рабочих станциях через внутреннюю сеть.

Сохранение права собственности и прочих прав

ООО «ФЛАТ» оставляет за собой все права, не предоставленные вам явно данным Лицензионным соглашением с конечным пользователем. Это Программное обеспечение защищено законами и соглашениями об авторском праве и других правах на интеллектуальную собственность. ООО «ФЛАТ» и его поставщикам принадлежат право собственности, авторских правах и прочие права на интеллектуальную собственность в отношении данного Программного обеспечения. Программное обеспечение не продается, а предоставляется в пользование по лицензии.

Ограничение на вскрытие технологии, декомпиляцию и деассемблирование

Вы не имеете права на вскрытие технологии, декомпиляцию и деассемблирование Программного обеспечения за исключением случаев и только в той степени, когда это прямо разрешено применимым законодательством, несмотря на данное ограничение.

Запрет на передачу во временное пользование и коммерческое использование

Запрещается предоставлять это Программное обеспечение в прокат, в аренду и во временное пользование, а также использовать его для оказания сетевых услуг третьим лицам на коммерческой основе.

Дополнительное программное обеспечение и службы

Данное Лицензионное соглашение с конечным пользователем распространяется на обновления, дополнения, добавляемые компоненты, службы поддержки продукта или компоненты служб Интернета, которые относятся к Программному обеспечению и могут быть получены вами от ООО «ФЛАТ» после получения вами начальной копии Программного обеспечения, если вышеуказанное не поставляется с измененными условиями или не регулируется другим соглашением. ООО «ФЛАТ» оставляет за собой право прекратить оказание услуг Интернета, которые предоставлялись вам или были доступны через Программное обеспечение.

Программное обеспечение, не предназначенное для перепродажи

Если указано, что Программное обеспечение не предназначено для перепродажи («Not For Resale», «NFR»), его не разрешается продавать или передавать кому-либо иным способом с целью получения прибыли. Такое Программное обеспечение может использоваться только для демонстрации, тестирования или оценки.

Прекращение действия соглашения

Без ущерба для каких-либо других прав ООО «ФЛАТ» может прекратить действие данного Лицензионного соглашения с конечным пользователем в случае нарушения вами его условий. В таком случае вы обязаны уничтожить все копии Программного обеспечения и всех его компонентов.

Полнота соглашения и ограничение недействительности

Данное Лицензионное соглашение с конечным пользователем (включая все дополнения и изменения к нему, поставляемые с Программным обеспечением) является полным соглашением между вами и ООО «ФЛАТ» относительно Программного обеспечения и услуг по поддержке (если они есть) и заменяет собой все предыдущие и текущие устные и письменные сообщения, предложения и заявления по Программному обеспечению или любому другому вопросу, являющемуся предметом данного Лицензионного соглашения с конечным пользователем. В той мере, в которой условия каких-либо правил или программ ООО «ФЛАТ» в отношении услуг по поддержке противоречат условиям данного Лицензионного соглашения с конечным пользователем, условия данного Лицензионного соглашения с конечным пользователем имеют преимущественную силу. Если какое-либо из положений данного Лицензионного соглашения с конечным пользователем становится недействительным, ничтожным или неисполнимым, остальные положения остаются в силе.

Взаимодействие с пользовательским интерфейсом

Взаимодействие с программными продуктами семейства ФЛАТ происходит с помощью WEB-интерфейса, для подключения к которому в адресной строке браузера введите IP-адрес. При корректном вводе адреса в окне браузера отобразится форма авторизации:

Рисунок 148. Форма авторизации

Для авторизации введите *Логин* и *Пароль* пользователя и выберите в раскрывающемся списке IP-адрес администрируемой системы.



Выбор IP-адреса в форме авторизации позволяет управлять несколькими системами из одного интерфейса (см. [Список администрируемых систем в форме авторизации](#)).

В дополнение к механизму авторизации по логину и паролю могут применяться способы аутентификации с использованием Active Directory и технологии единого входа. В первом случае после ввода логина и пароля отметьте чек-бокс **Доменная авторизация**, а в случае аутентификации с использованием SSO нажмите кнопку **SSO**.

После успешной авторизации откроется главная страница пользовательского интерфейса (см. [Рисунок 149](#)):

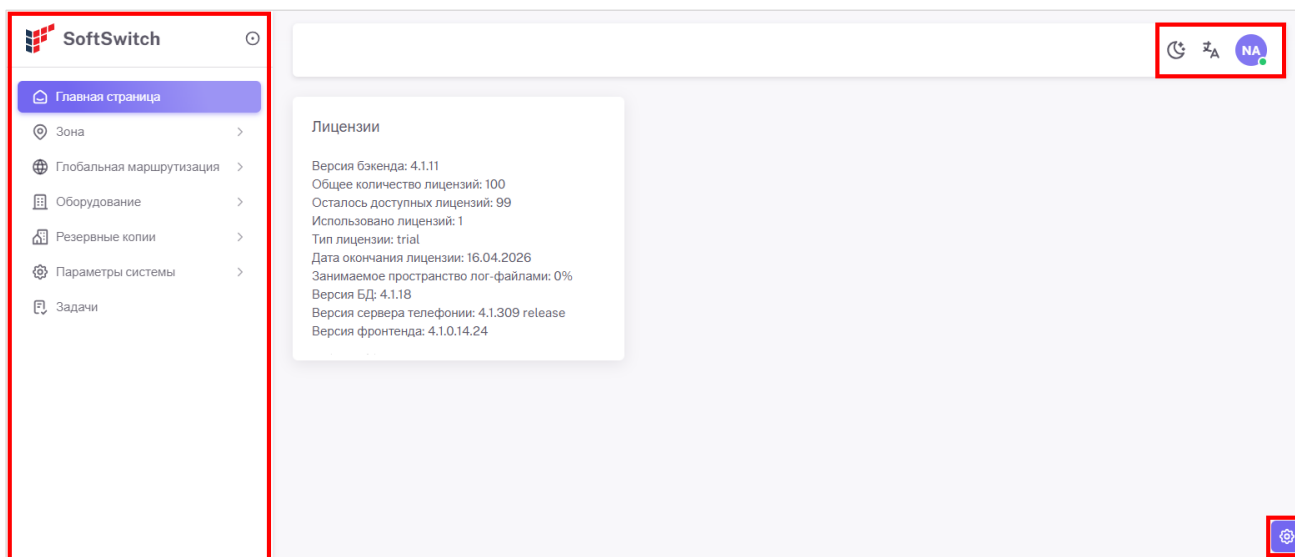








Рисунок 149. Основные элементы WEB-интерфейса

Таблица 5. Назначение основных элементов WEB-интерфейса

Элемент	Описание
<p>Меню системы</p>	<p>Меню системы. Может располагаться как вертикально в левой части окна, так и горизонтально в верхней части окна. Переключение производится в настройках WEB-интерфейса (кнопка ).</p>
<p></p>	<p>Закрепление/открепление вертикального меню.</p>
<p></p>	<p>Переключение цветового режима WEB-интерфейса – светлый/темный.</p>
<p></p>	<p>Переключение языка WEB-интерфейса.</p>
<p></p>	<p>Меню пользователя:</p> <ul style="list-style-type: none"> • Имя текущего пользователя; • Сбросить настройки – сброс настроек WEB-интерфейса текущего пользователя на значения по умолчанию; • Выйти из учетной записи.
<p></p>	<p>Настройки оформления WEB-интерфейса текущего пользователя:</p> <ul style="list-style-type: none"> • Структура – настройка оформления элементов интерфейса: <ul style="list-style-type: none"> • С тенью; • С рамками. • Режим – цветовой режим оформления элементов интерфейса: <ul style="list-style-type: none"> • Светлый; • Темный; • Полутемный. • Основной цвет – выбор основного цвета элементов оформления интерфейса; • Ширина контента – ширина табличной части интерфейса: <ul style="list-style-type: none"> • На всю ширину; • С отступами. • Позиционирование верхней панели: <ul style="list-style-type: none"> • Зафиксировать – фиксация сверху страницы, прокручивается вместе с содержимым окна; • Статический – фиксация над страницей, постоянная видимость при прокрутке окна; • Скрыть – полоса скрыта. • Панель прозрачная – включение видимости страницы над верхней панелью; • Позиция меню – настройка расположения меню: <ul style="list-style-type: none"> • Вертикальное; • Горизонтальное. • Навигация – настройка сворачивания меню: <ul style="list-style-type: none"> • Аккордеон – сворачивание текущего меню при выборе другого пункта меню; • Складная панель – состоянием меню управляет пользователь. • Свернуть меню; • Скрыть меню.

При выборе пунктов меню соответствующая им информация выводится в основном окне в табличном виде (см. [Рисунок 150](#)):

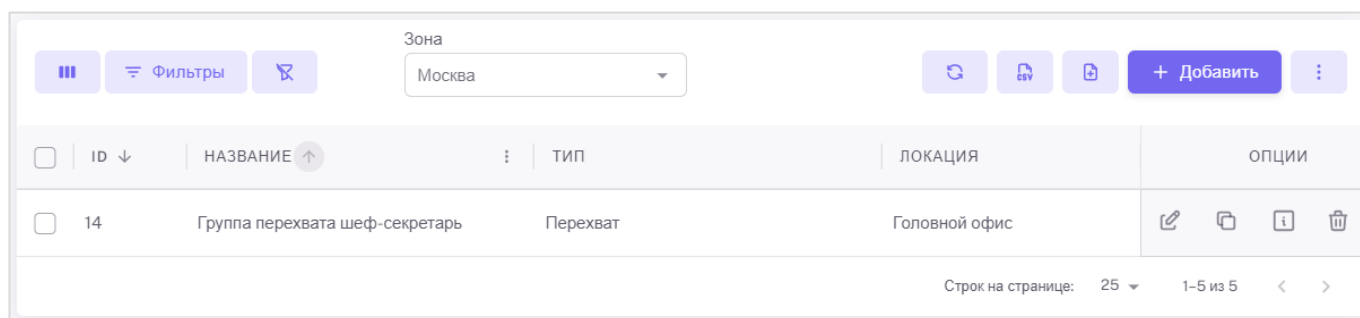


Рисунок 150. Элементы табличной части WEB-интерфейса

Таблица 6. Назначение элементов табличной части WEB-интерфейса

Элемент	Описание
	Настройка видимости столбцов таблицы. В раскрывающемся списке отметьте необходимые для отображения столбцы. Серым цветом отмечаются имена закрепленных столбцов недоступных для скрытия.
	Фильтрация выводимой информации с помощью набора условий, связанных между собой логическими операторами. Возможно сохранение и использование ранее созданных фильтров. Удаление фильтров см. в разделе Фильтры .
	Очистка фильтров.
	Выбор в раскрывающемся списке элементов, связанных с текущим представлением информации на странице.
	Обновление выводимой на странице информации.
	Сохранения информации в файл формата CSV.
	Импорт информации из файла формата CSV.
	Создание резервной копии.
	Кнопка в названии столбца – сортировка записей по текущему столбцу по возрастанию/убыванию.
	Кнопка в названии столбца – раскрывает меню: <ul style="list-style-type: none"> • Сортировка записей по текущему столбцу по возрастанию/убыванию. • Закрепление текущего столбца слева или справа таблицы. • Настройка фильтра по значению текущего столбца. • Настройки отображения текущего столбца. • Управление колонками – настройка видимости столбцов таблицы.
	Изменение текущей записи таблицы.
	Клонирование текущей записи таблицы.
	Подробная информация по текущей записи таблицы.
	Удаление текущей записи таблицы.
	Настройка количества выводимых строк на странице.
	Кнопки навигации по страницам.

Лицензирование

Система ФЛАТ SoftSwitch лицензируется на временной или постоянной основе только по количеству абонентов и варианту развертывания (дублирование, Живучий Офис). Абонентские лицензии расходуются при регистрации абонентского устройства и высвобождаются при его отключении. Множественная регистрация нескольких абонентских устройств на один номер не требует дополнительной лицензии.

На главной странице интерфейса приводится полная информация о лицензиях – общее количество, доступное количество, сколько лицензий использовано, тип выданной лицензии и дата окончания срока действия (см. [Рисунок 151](#)):

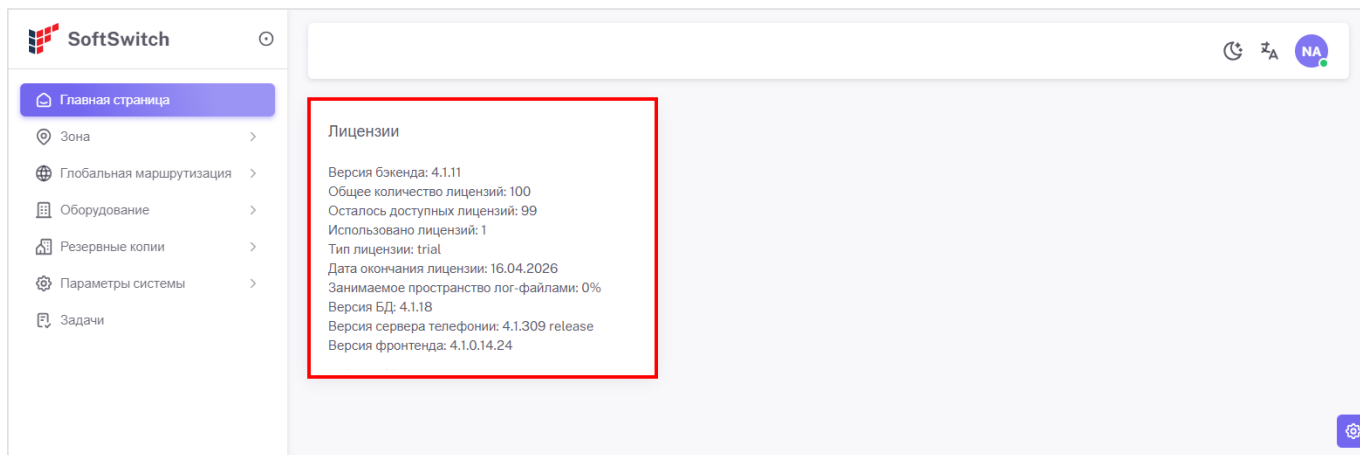


Рисунок 151. Информация о лицензиях

Лицензия предоставляется в цифровом виде, наличие физического носителя не требуется.

Лицензионный ключ для ядра системы ФЛАТ SoftSwitch (или для каждого узла при организации кластера), а также для отказоустойчивого выноса (Живучего Офиса), вводится на стадии установки системы.

Полная информация по установке системы приведена в документе «ФЛАТ SoftSwitch. Руководство по установке» (ссылку на документ см. в разделе [Связанные документы](#)).

После обновления ключей (при замене временной лицензии на постоянную, либо при расширении системы) необходимо поочередно перезапустить сервисы на основном и дублирующем узле командой:

```
service flat_ss restart
```



Временная лицензия после окончания своего срока продолжает действовать до перезагрузки (для версий ФЛАТ SoftSwitch до v.2.4).

Список администрируемых систем в форме авторизации

Для настройки списка администрируемых систем, доступных в форме авторизации фронтенда ФЛАТ SoftSwitch, внесите изменения в файл `/opt/flat/fss-frontend/apps/softswitch/public/config.json`.

В параметре **addresses** конфигурационного файла должен быть указан IP-адрес (или FQDN) и порт взаимодействия бэкенда ФЛАТ SoftSwitch.

При указании через запятую нескольких адресов форма авторизации будет дополнена полем выбора администрируемой системы, при указании одного адреса (по умолчанию) поле выбора отображаться не будет.

Пример конфигурационного файла:

```
/opt/flat/fss-frontend/apps/softswitch/public/config.json
{
  "addresses": ["10.77.13.11:443", "10.77.15.194:443"]
  "isDomainAuthEnable": true,
  "isSSOEnable": true
}
```

Включение в форму авторизации фронтенда ФЛАТ SoftSwitch элементов дополнительных способов аутентификации см. [Аутентификация пользователей с использованием AD и SSO](#).

Установка ФЛАТ SoftSwitch и внесение изменений в конфигурационные файлы входящих в систему сервисов, рассматриваются в документе «ФЛАТ SoftSwitch. Руководство по установке» (ссылку на документ см. в разделе [Связанные документы](#)).

Матрица портов и разрешённых соединений

Для сетевого взаимодействия используются следующие порты (см. [Таблица 7. Порты внешних взаимодействий](#)):

Таблица 7. Порты внешних взаимодействий

№	Точка А	Порт	Точка Б	Порт	Сетевой протокол	Описание
1	ФЛАТ Softswitch. Ядро 1	1520/1540 (Proprietary)	ФЛАТ Softswitch. Ядро 2	1520/1540 (Proprietary)	TCP	Обмен служебной информацией. Взаимодействие узлов.
2	ФЛАТ Softswitch. Ядро	1540	Бэкенд ФЛАТ Softswitch	1540	TCP	Обмен служебной информацией.
3	ФЛАТ Softswitch. Ядро	1540	Бэкенд ЛК ФЛАТ Softswitch	1540	TCP	Обмен служебной информацией.
4	ФЛАТ Softswitch. Ядро	3306	БД	3306	TCP	Взаимодействие с реляционной базой данных
5	ФЛАТ Softswitch. Ядро	2429	SRClient	2429	MGCP UDP	Управление модулем записи и проксирования
6	ФЛАТ Softswitch. Ядро	5060 (SIP)	Абоненты/транки	5060 (SIP)	UDP/TCP	SIP-сигнализация
7	ФЛАТ Softswitch. Ядро	5061 (SIP)	Абоненты/транки	5061 (SIP)	TLS	SIP-сигнализация
8	ФЛАТ Softswitch. Ядро	2427	Mediasrv	2427	MGCP UDP	Управление модулем медиаресурсов
9	ФЛАТ Softswitch. Ядро	1541	REST API	1541	TCP	Интерфейс REST API
10	ФЛАТ Softswitch. Ядро	1540	XML API	1540	TCP	Интерфейс XML API
11	ФЛАТ Softswitch. Ядро	1040 (CSTA)	ФЛАТ Контакт	1040 (CSTA)	TCP	Обмен служебной информацией. Протокол CSTA
12	ФЛАТ Softswitch. Ядро	5060 (SIP)	ФЛАТ Контакт	5060 (SIP)	UDP/TCP	SIP-сигнализация
13	ФЛАТ Softswitch. Ядро	5061 (SIP)	ФЛАТ Контакт	5061 (SIP)	TLS	SIP-сигнализация
14	Mediasrv	5000-8000 (RTP)	Абоненты	порт абонентского устройства	UDP	Передача медиаресурсов
15	СХД	22 (SFTP)	ФЛАТ Тарификатор	22 (SFTP)	TCP	Передача тарификационных данных
16	SRClient	5000-8000 (RTP)	Абоненты/транки	порт абонентского устройства	UDP	Передача медиатрафика
17	SRClient	5000-8000 (RTP)	ФЛАТ Запись	29100-32100 (RTP)	UDP	Передача медиатрафика
18	SRClient	5062 (SIPREC)	ФЛАТ Запись	5060 (SIPREC)	UDP/TCP	Передача медиатрафика
19	Бэкенд ФЛАТ Softswitch	389 (LDAP)	AD	389 (LDAP)	TCP	Взаимодействие с Active Directory
20	Бэкенд ФЛАТ Softswitch	636 (LDAPS)	AD	636 (LDAPS)	TCP	Взаимодействие с Active Directory

№	Точка А	Порт	Точка Б	Порт	Сетевой протокол	Описание
21	Бэкенд ФЛАТ Softswitch	3306	БД MySQL	3306	TCP	Взаимодействие с реляционной базой данных MySQL
22	Фронтенд ФЛАТ Softswitch	80 (HTTP)	Администратор	80 (HTTP)	TCP	Интерфейс управления. WEB
23	Фронтенд ФЛАТ Softswitch	443 (HTTPS)	Администратор	443 (HTTPS)	TCP	Интерфейс управления. WEB
24	Бэкенд ЛК ФЛАТ Softswitch	389 (LDAP)	AD	389 (LDAP)	TCP	Взаимодействие с Active Directory
25	Бэкенд ЛК ФЛАТ Softswitch	636 (LDAPS)	AD	636 (LDAPS)	TCP	Взаимодействие с Active Directory
26	Бэкенд ЛК ФЛАТ Softswitch	3306	БД MySQL	3306	TCP	Взаимодействие с реляционной базой данных
27	Бэкенд ЛК ФЛАТ Softswitch	443	ФЛАТ DM	443	TCP	Обмен служебной информацией.
28	Фронтенд ЛК ФЛАТ Softswitch	80 (HTTP)	Пользователь	80 (HTTP)	TCP	Интерфейс управления. WEB
29	Фронтенд ЛК ФЛАТ Softswitch	8443 (HTTPS)	Пользователь	8443 (HTTPS)	TCP	Интерфейс управления. WEB
30	LDAPSynchronizer	389 (LDAP)	AD	389 (LDAP)	TCP	Взаимодействие с Active Directory
31	LDAPSynchronizer	636 (LDAPS)	AD	636 (LDAPS)	TCP	Взаимодействие с Active Directory
32	FlatFileManager	8053	Бэкенд ФЛАТ Softswitch	8053	TCP	Обмен служебной информацией.
33	Управление (Putty, WinSCP)	22 (SSH)	ОС	22 (SSH)	TCP	Интерфейс управления. Консоль

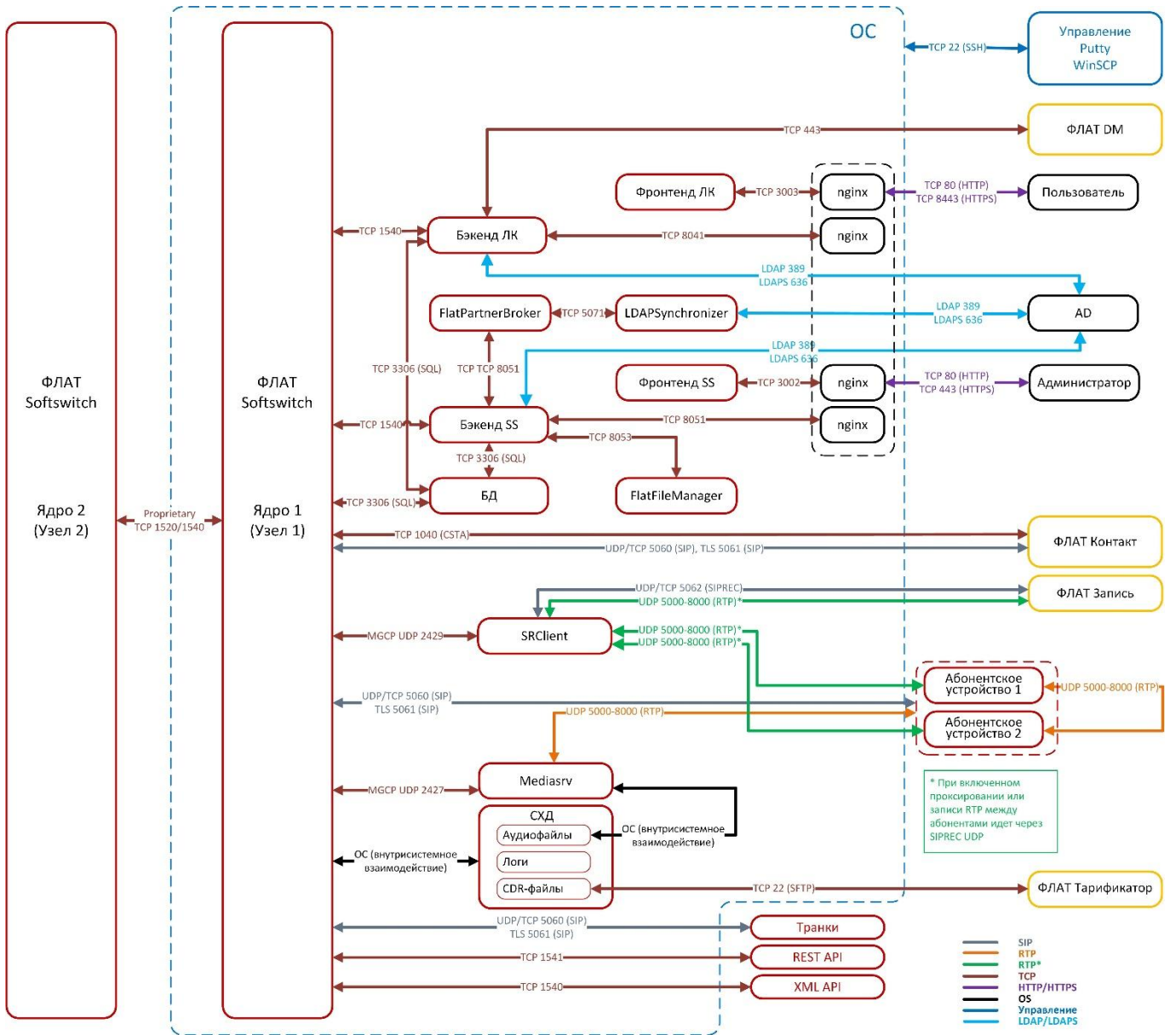


Рисунок 152. Схема соединений, портов и протоколов

Аутентификация пользователей с использованием AD и SSO

В системе ФЛАТ SoftSwitch в дополнение к встроенному механизму авторизации по логину и паролю могут применяться следующие способы аутентификации пользователей:

- С использованием Active Directory (см. [Рисунок 153](#)).
- С использованием SSO (см. [Рисунок 154](#)).

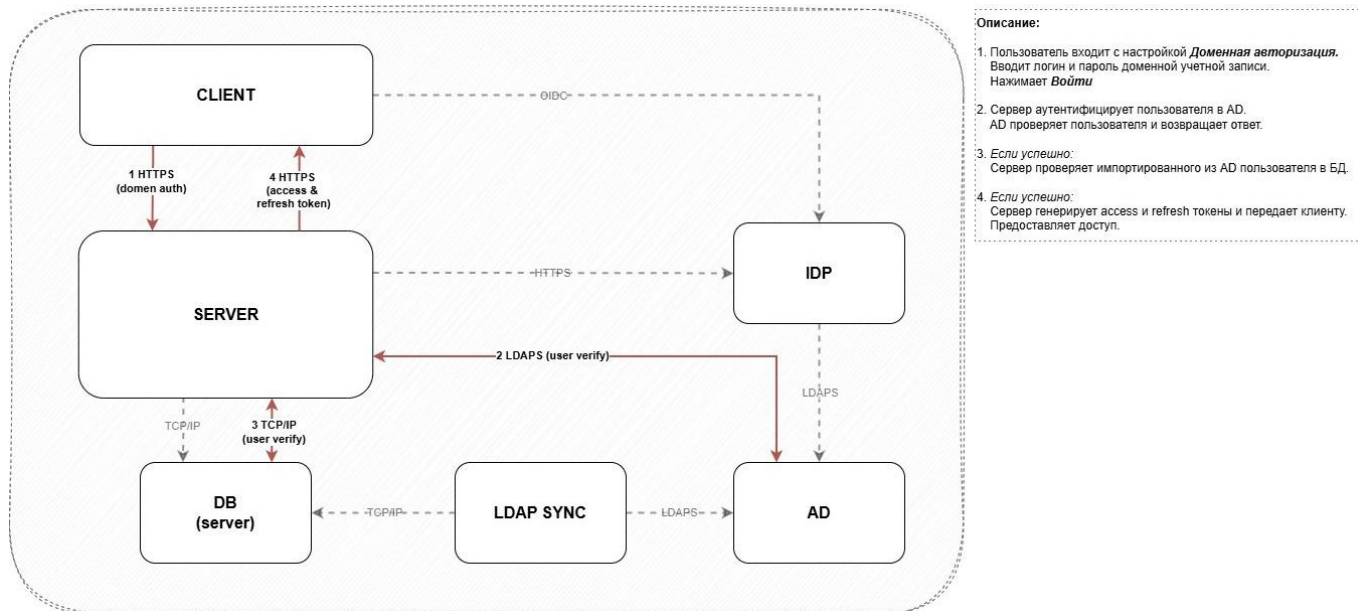


Рисунок 153. Доменная авторизация

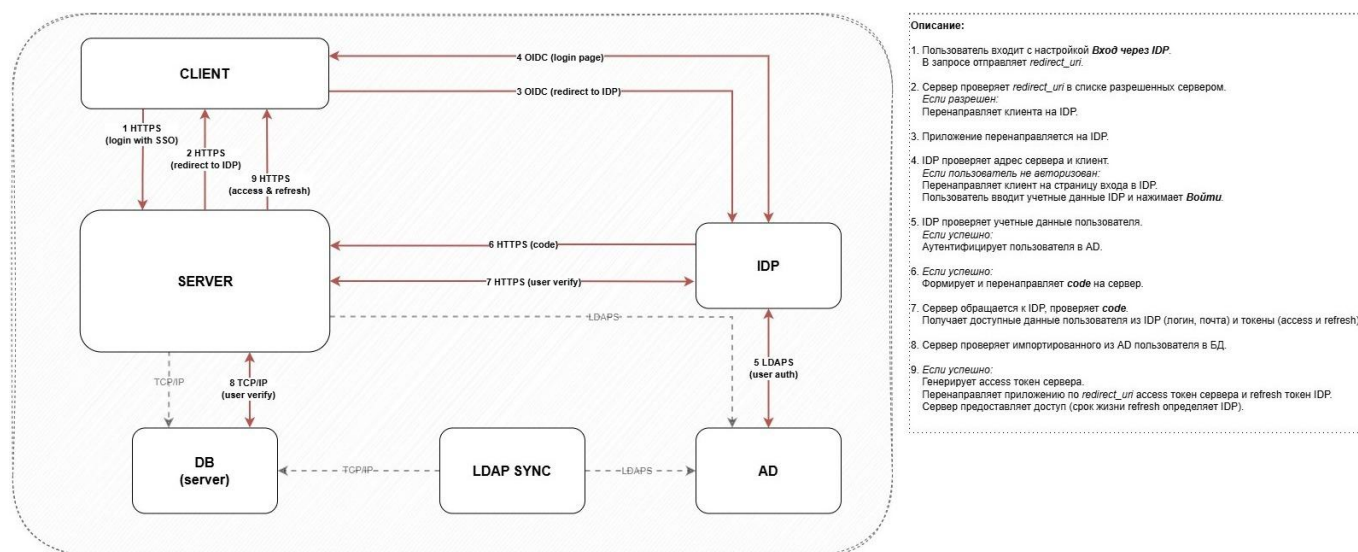


Рисунок 154. Единый вход (SSO)

Для корректной работы указанных способов аутентификации важно, чтобы логин пользователя системы ФЛАТ SoftSwitch совпадал с учетными данными пользователя корпоративного домена Active Directory.

Для аутентификации с использованием AD и SSO понадобятся сервисы **LDAPSynchronizer** и **FlatPartnerBroker**, которые необходимо установить дополнительно. Указанные сервисы предназначены для импорта данных пользователей из корпоративного каталога по протоколу LDAP (LDAPS) в программные продукты ФЛАТ, используя механизм брокера. При работе сервисов измененные, удаленные или созданные в AD учетные данные синхронизируются с системой ФЛАТ SoftSwitch.

Установка и конфигурирование сервисов рассматривается в документе «ФЛАТ Software. Дополнительные компоненты» (ссылку на документ см. в разделе [Связанные документы](#)).

Настройка бэкенда ФЛАТ SoftSwitch

Выполните в конфигурационном файле `/usr/lib/flatSoftSwitchBackend/config.yml` настройки аутентификации через AD или SSO, указав необходимые параметры.

Для аутентификации с использованием SSO оставьте включенным один из протоколов проверки подлинности OIDC или SAML, указав в параметре **enabled** каждой секции значение **false** или **true**. В настройках остальных параметров укажите требуемые значения.

Пример:

```
/usr/lib/flatSoftSwitchBackend/config.yml
# Настройки аутентификации
auth:

# Время жизни access токена в минутах. По умолчанию 15 минут.
# Для SSO время жизни токена согласно настройкам IDP
access_token_ttl: 30

# Ключ шифрования access токена.
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
# ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
key: lkIUHVKJhobfwkbe1wouwebvkwkeJKIUUYUyf67u

# Настройки аутентификации через Active Directory.
ldap:

# Адрес AD
# ldap://example.com:389
# ldaps://example.com:636
addr: ldap://10.77.13.11:389

# BaseDN пользователей
# Если включена синхронизация через LDAPsynchronizer, рекомендуется
# скопировать base_dn из config.json.
base_dn: OU=OrganizationalUnit,DC=example,DC=com

# Фильтрация пользователей.
# Если нужно разрешить доступ только пользователям из определенной группы
# или по другому признаку.
# Оставьте пустым, если хотите разрешить доступ всем пользователям
# из BaseDN.
base_filter: (objectClass=Person)

# Домен AD.
# Требуется для авторизации пользователей - login_attr + @ + example.com
domain: example.com

# Укажите true для включения
enabled: false

# Из какого параметра извлекать Логин. Принимает одно значение.
# Если включена синхронизация через LDAPsynchronizer, рекомендуется
# скопировать data.login из config.json.
# Обычно sAMAccountName или cn
login_attr: sAMAccountName

# Время жизни refresh токена в минутах. По умолчанию 540 минут - 8 часов.
```

```

refresh_token_ttl: 540

# Настройки SSO
sso:

  # Настройки OIDC
  oidc:

    # ID клиента
    client_id:

    # Секретный ключ
    # ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
    # ./flatsoftswitchbackend_1.0.0 encrypt --text='....'
    client_secret:

    # Укажите адрес для извлечения конфигурации провайдера
    # Отправится запрос по адресу
    # config_url + /.well-known/openid-configuration
    config_url: http://10.77.13.11/oauth2/token

    # Укажите true для включения
    enabled: true

    # Из какого параметра извлекать Логин
    # По умолчанию sub
    login_attr: sub

    # Адрес данного сервиса.
    # Если настроен nginx, домен и порт должны совпадать с настройками nginx
    # Для HTTP укажите порт 8051, для HTTPS 8050
    root_url: http://10.77.13.11:8051

    # Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
    # Принимает массив (несколько адресов)
    # Удалите все адреса, чтобы снять ограничение (не рекомендуется)
    valid_redirect_urls:
      - http://10.77.13.11:3000

  # Настройки SAML
  saml:

    # Самоподписанный сертификат
    # openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out
myservice.cert -days 365 -nodes -subj "/CN=myservice.example.com"
    cert_file:

    # Укажите true для включения
    enabled: false

    # Самоподписанный ключ
    # openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out
myservice.cert -days 365 -nodes -subj "/CN=myservice.example.com"
    key_file:

    # Из какого параметра извлекать Логин
    # По умолчанию http://wso2.org/claims/username

```

```

login_attr: http://wso2.org/claims/username

# Если файл xml расположен на сервере, укажите полный путь к нему
# У текущего пользователя должны быть права на чтение
meta_data_path: /etc/metadata.xml

# Если xml расположен на сервере IDP, укажите его адрес
# https://example.com:8443/realms/master/protocol/saml/descriptor
meta_data_url:

# Адрес данного сервиса.
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
# Для HTTP укажите порт 8051, для HTTPS 8050
root_url: http://10.77.13.11:8051

# Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
# Принимает массив (несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:
  - http://10.77.13.11:3000

```

После изменения конфигурационного файла перезапустите сервис:

```
service flatsoftswitchbackend restart
```

Проверьте успешность запуска сервиса:

```
systemctl status flatsoftswitchbackend.service
```

Статус сервиса должен быть: **active (running)**.

Настройка фронтенда ФЛАТ SoftSwitch

Для включения в форму авторизации ФЛАТ SoftSwitch элементов дополнительных способов аутентификации внесите изменения в файл `/opt/flat/fss-frontend/apps/softswitch/public/config.json`. В следующих параметрах должно быть указано:

addresses – IP-адрес бэкенда администрируемой системы ФЛАТ SoftSwitch (порт должен быть указан 443).

isDomainAuthEnable – укажите **true** при аутентификации с использованием AD, или **false** без использования.

isSSOEnable – укажите **true** при аутентификации с использованием SSO, или **false** без использования.

Пример конфигурационного файла:

```

/opt/flat/fss-frontend/apps/softswitch/public/config.json
{
  "addresses": ["10.77.13.11:443"],
  "isDomainAuthEnable": true,
  "isSSOEnable": true
}

```

После изменения конфигурационного файла перезапустите сервис:

```
systemctl restart fss-frontend.service
```

Проверьте успешность запуска сервиса:

```
systemctl status fss-frontend.service
```

Статус сервиса должен быть: **active (running)**.

Сценарии использования

Применение ролей пользователей

Пример 1. Необходимо создать роль с правами просмотра только «Журнала безопасности» и «Журнала безопасности абонентов».

Выберите меню **Параметры системы/Администраторы/Роли** и нажмите кнопку **Добавить**. В поля открывшейся формы внесите название роли «Аудитор ИБ». Прокрутив список отметьте права на чтение у разрешения «История запросов абонентов – abonents-query-history (ID: 20)» и «История запросов – query-history (ID: 36)» (см. [Рисунок 155](#)). Сохраните изменения.

Рисунок 155. Создание роли «Аудитор ИБ»

Создайте пользователя с ролью «Аудитор ИБ» и авторизуйтесь с его логином и паролем. В результате выполненных настроек указанному пользователю будут доступны только два пункта интерфейса – «Журнал безопасности» и «Журнал безопасности абонента» (см. [Рисунок 156](#)):

id	id пользователя	ФАМИЛИЯ	ИМЯ	ОТЧЕСТВО	IP АДРЕС	МЕТОД	КОД ОТВЕТА	ID ОПЕРАЦИИ	ПУТЬ	ВРЕЯ	ОПЦИИ
1266	3	auditor	auditor		10.77.10.31	GET	200	1744285579689	/api/v1/license	10.04	□
1265	3	auditor	auditor		10.77.10.31	GET	200	1744285579589	/api/v1/license	10.04	□
1264	3	auditor	auditor		10.77.10.31	GET	200	1744285579509	/api/v1/auth/permissions	10.04	□
1263	3	auditor	auditor		10.77.10.31	POST	200	1744285579475	/api/v1/auth/login	10.04	□
1262	1	Admin	Admin		10.77.10.31	POST	200	1744285571162	/api/v1/auth/logout	10.04	□
1261	1	Admin	Admin		10.77.10.31	GET	200	1744285566114	/api/v1/license	10.04	□
1260	1	Admin	Admin		10.77.10.31	GET	200	1744285565836	/api/v1/license	10.04	□
1259	1	Admin	Admin		10.77.10.31	GET	200	1744285565682	/api/v1/auth/permissions	10.04	□
1258	1	Admin	Admin		10.77.10.31	POST	200	1744285565652	/api/v1/auth/login	10.04	□

Рисунок 156. Список разделов, доступный пользователю «Аудитор ИБ»

Применение профиля абонента

Использование профиля абонента покажем на примере реализации функции вторжения в разговор.

Напомним, что при применении профиля активируется модель разрешений, в которой по умолчанию все запрещено. Применение пустого профиля, либо профиля с добавленными, но выключенными функциями, равноценно его отсутствию – абоненту все так же запрещено.

При применении профиля, в который добавлены функции с различными признаками («Вкл.»/«Выкл.»), абоненту будут доступны только включенные функции.

Пример 1. Создан профиль абонента «Default», в который добавлены функции, разрешающие входящие и исходящие вызовы, а также функции «Вторжение» и «Вторжение в режиме конференции» (см. [Рисунок 157](#)):

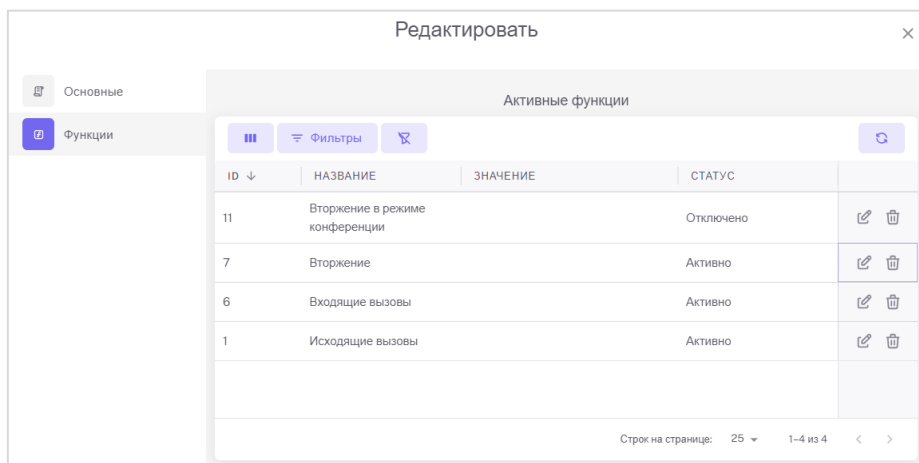


Рисунок 157. Функция «Вторжение» в профиле абонента «Default»

В свойствах абонента «С» применен созданный на предыдущем шаге профиль «Default» (см. [Рисунок 158](#)):

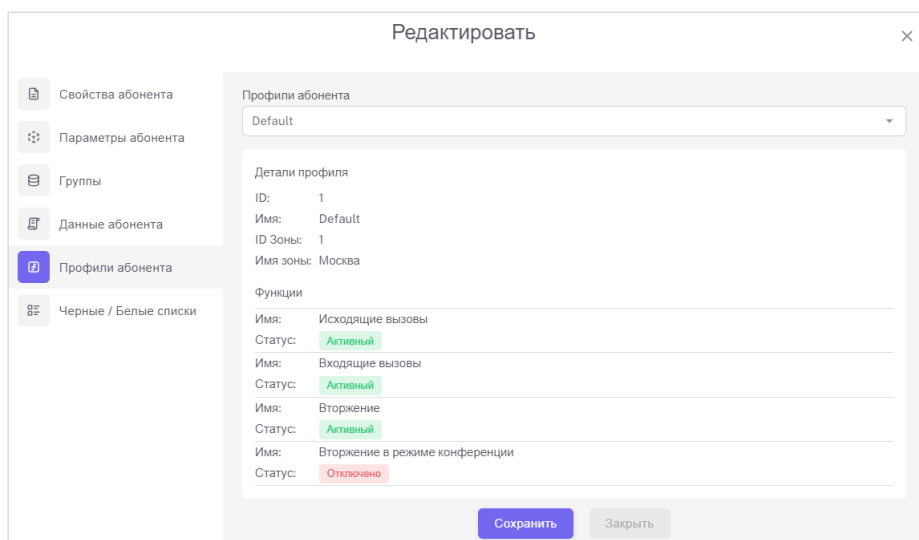


Рисунок 158. Назначение профиля в свойствах абонента

Абонент «А» разговаривает с абонентом «В».

Абонент «С» с правом вторжения и **выключенной** опцией «Вторжение в режиме конференции» вызывает абонента «А», автоматически вторгаясь в разговор. При этом абонент «А» слышит три предупреждающих сигнала, абонент «В» слышит предупреждение о разрыве вызова.

Абонент «С» с правом вторжения и **включенной** опцией «Вторжение в режиме конференции» вызывает абонента «А», автоматически вторгаясь в разговор в режиме конференции. При этом абоненты «А» и «В» слышат три предупреждающих сигнала.

Пример 2. В дополнение к предыдущему примеру создан супер-абонент «D», в профиле которого добавлена функция «Разрешать вторгаться в любой разговор», дающая ему максимальные права вторжения.

С активированной функцией «Разрешать вторгаться в любой разговор», абонент «D» может вызывать как абонента «А», так и абонента «С», ведущих разговор после вторжения. Без этой функции абонент «D» услышит только сигнал «busy».

Применение групп перехвата

Пример 1. Организация группы шеф-секретарь.

Создается группа перехвата, в которую включаются номера руководителя (900) и секретаря (2222) (см. [Рисунок 159](#)):

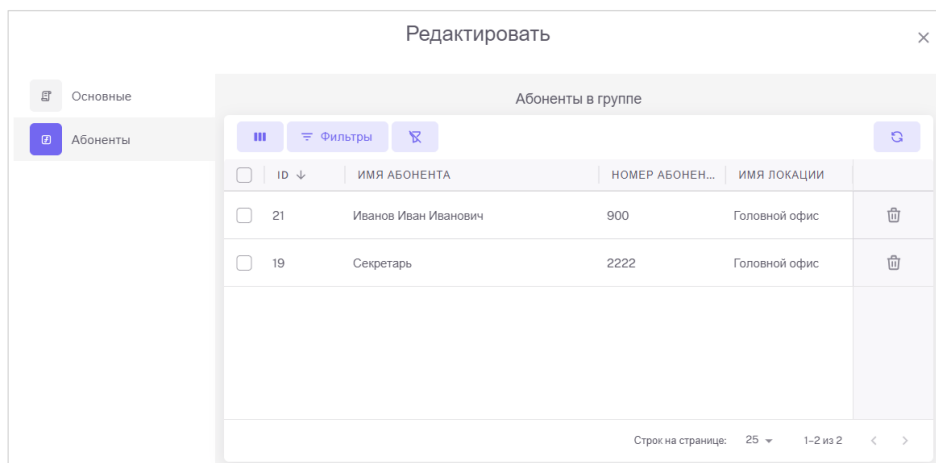


Рисунок 159. Создание группы перехвата шеф-секретарь

В свойствах абонента (руководителя) на вкладке **Черные/Белые списки** отмечается пункт «Только белый список», в который добавляется номер секретаря (2222) (см. [Рисунок 160](#)):

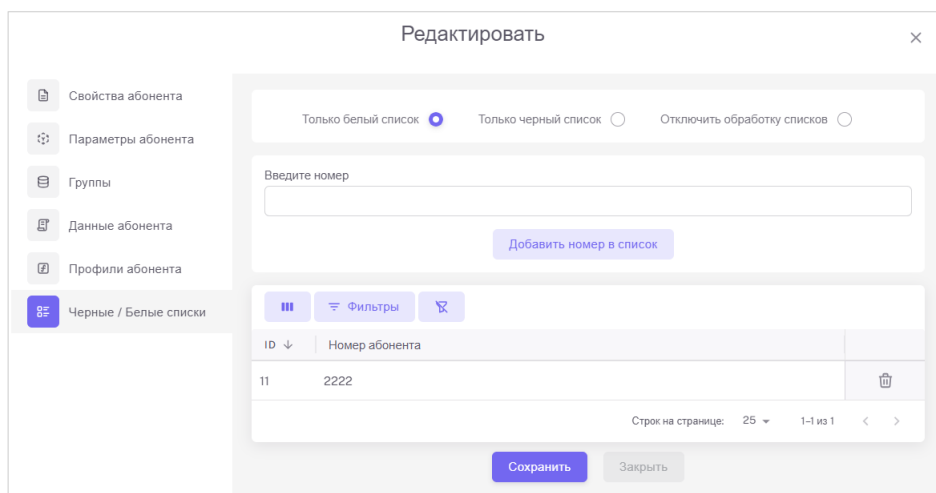


Рисунок 160. Включение номера секретаря в белый список руководителя

В свойствах абонента (руководителя) на вкладке **Параметры абонента** включается опция «Переадресация по Ч/Б списку» и указывается номер секретаря (см. [Рисунок 161](#)):

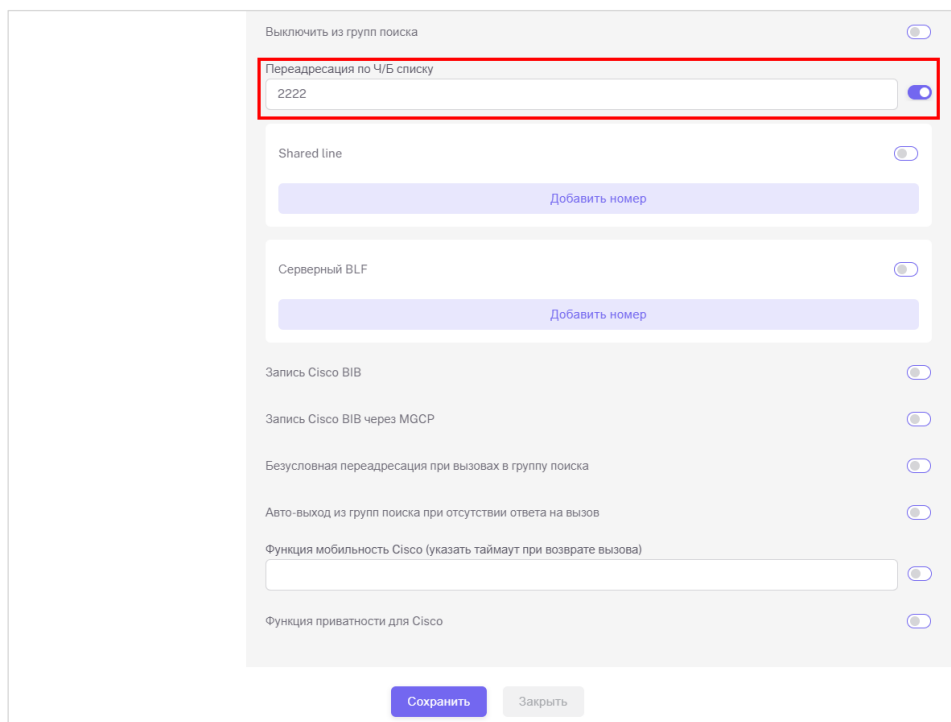


Рисунок 161. Включение опции переадресации по Ч/Б списку

Для перехвата в группе создается сервисный код «*101» (см. [Рисунок 162](#)):

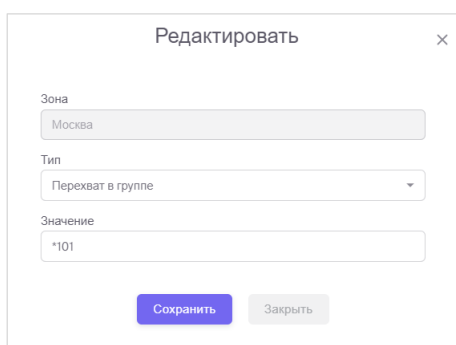


Рисунок 162. Создан код перехвата в группе

В результате применения указанных настроек только секретарь сможет напрямую дозвониться до руководителя или перевести на него вызов. При вызове на номер руководителя произойдет переадресация на номер секретаря, а руководитель сможет перехватить вызов.

Пример 2. Три абонента (4406 – «TA6 Yealink T46S тест», 4401 – «TA1 Cisco CP-8861 тест», 4402 – «TA2 Cisco CP-8861 тест») включены в группу перехвата «Группа Перехват головной офис» (см. [Рисунок 163](#)):

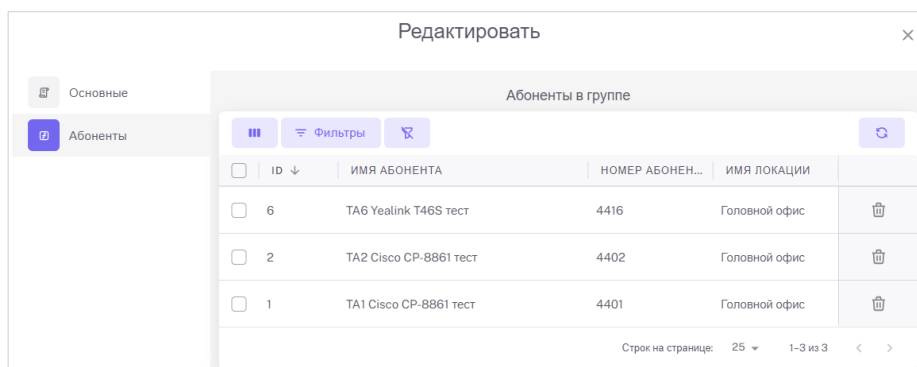


Рисунок 163. ТА объединены в группу перехвата

Создан сервисный код для перехвата вызова в группе с кодом «*101» (см. [Рисунок 164](#)):

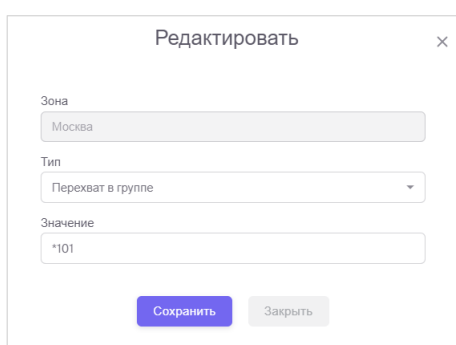


Рисунок 164. Создан код перехвата в группе

Сервисный код присвоен определенным кнопкам на указанных телефонных аппаратах.

При вызове абонентом 4406 «TA6 Yealink T46S тест» абонента 4402 «TA2 Cisco CP-8861 тест» на экране последнего отобразится номер вызываемого абонента, а кнопки под экраном примут значения: «Ответ», «Отклонить», «Игнорировать» (см. [Рисунок 165](#)):



Рисунок 165. Экран 4402 «TA2 Cisco CP-8861 тест» при вызове

На третьем телефонном аппарате, включенном в общую группу перехвата, на экране отобразится информация о вызове, а назначенная кнопка примет значение «Перехват» (см. [Рисунок 166](#)):



Рисунок 166. Экран 4401 «TA1 Cisco CP-8861 тест» при перехвате

При нажатии кнопки «Перехват» произойдет перехват вызова.

Способ оповещения о вызове на экране телефонного аппарата (всплывающее сообщение или моргающая кнопка BLF) зависит от возможностей ТА и его настроек. Например, на экране ТА 4406 «ТА6 Yealink T46S тест» не отображаются всплывающие сообщения, а только моргает назначенная кнопка (см. [Рисунок 167](#)). Так же не предусмотрена индикация о перехвате в мобильной версии программного телефона ФЛАТ Партнер.

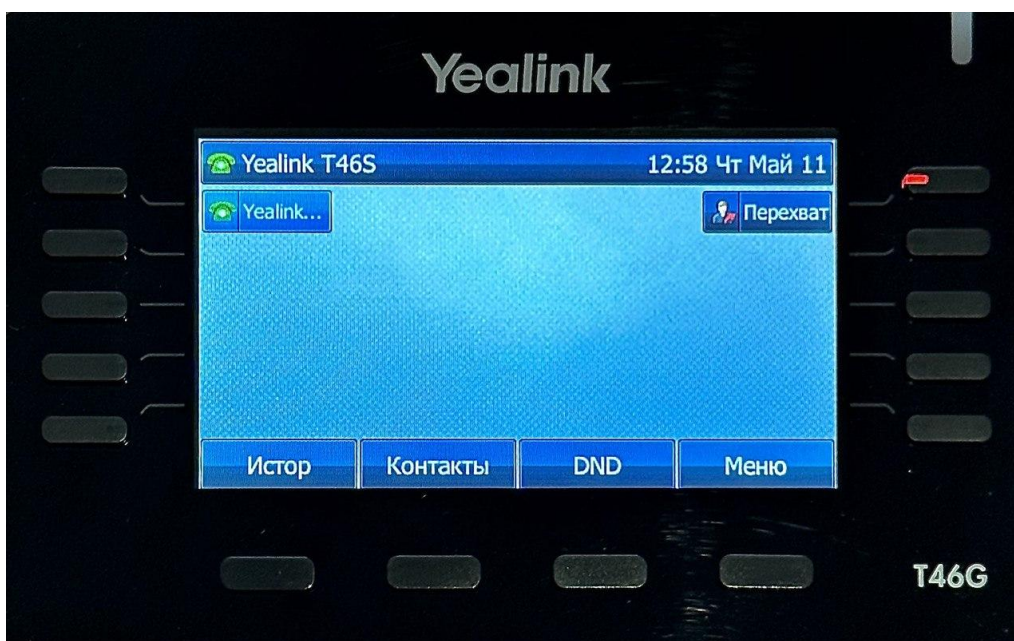


Рисунок 167. Экран 4406 «ТА6 Yealink T46S тест» при перехвате

Применение классов сервиса и ограничений

Применение классов ограничений

Применение классов ограничений покажем на примере организации маршрутизации вызовов в небольшой компании.

Исходные данные. Созданы учетные записи абонентов и один транк для выхода в сеть общего пользования. В организации принята четырехзначная нумерация внутренних номеров. Абоненты делятся на группы со следующими ограничениями:

- Разрешены только внутренние вызовы.
- Разрешены вызовы внутренние и городские.
- Разрешены вызовы внутренние, городские и междугородные.
- Разрешены все вызовы, включая международные.

Решение. Для организации маршрутизации вызовов необходимо выполнить следующие действия:

1. Создать классы трафика;
2. Создать классы ограничений;
3. Назначить абонентам класс ограничений;
4. Создать правила первичной маршрутизации;
5. Создать правила целевой маршрутизации.

1. Создание классов трафика.

В России полный телефонный номер состоит из 11 цифр, в которые входит префикс «8» (1 цифра), зональный код – код региона или оператора мобильной связи (3 цифры, для Москвы это коды 495, 496 и 499, а так же код 800, звонок на который оплачивается вызываемым абонентом) и номер абонента (7 цифр). Для наглядности в названии создаваемых классов трафика будем указывать префикс «8» и цифры, однозначно идентифицирующие направление вызова.

Создаем следующие классы трафика:

Класс трафика	Направление
8495-Г	Городской вызов для Москвы с кодом 495.
8496-Г	Городской вызов для Москвы с кодом 496.
8499-Г	Городской вызов для Москвы с кодом 499.
8800-Г	Городской вызов с кодом 800.
89-МОБ	Мобильный вызов. Мобильные операторы имеют коды в зоне 9xx.
810-МН	Международный вызов. Международный код — «810».
8-МГ	Междугородний вызов. Все остальные вызовы с префиксом «8».

Для внутренних вызовов отдельный класс трафика не создаем.

Созданы следующие классы (см. [Рисунок 168](#)):

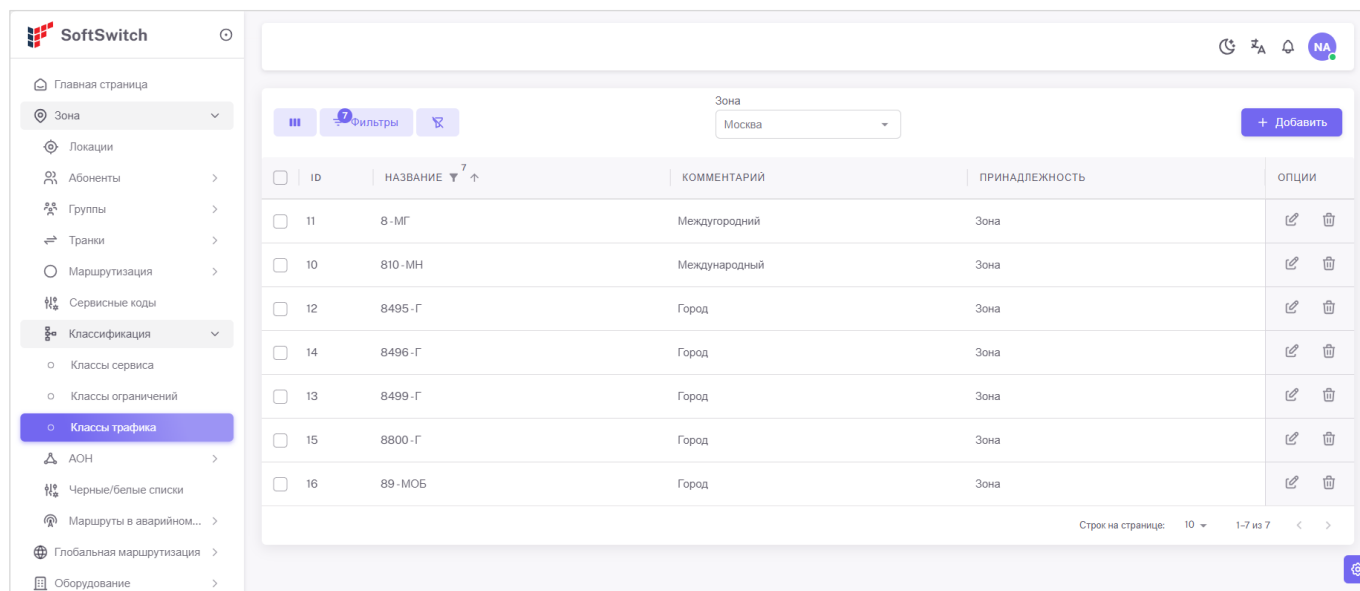


Рисунок 168. Список классов трафика

2. Создание классов ограничений.

В создаваемые классы ограничений вносим те классы трафика, которые должны быть ограничены:

Класс ограничений	Ограничения	Ограничение по классам трафика
ВНУТРЕННИЕ	Разрешены только внутренние вызовы.	<ul style="list-style-type: none"> 8495-Г 8496-Г 8499-Г 8800-Г 89-МОБ 810-МН 8-МГ
ГОРОД	Разрешены внутренние и городские вызовы. Запрещены междугородние и международные вызовы.	<ul style="list-style-type: none"> 810-МН 8-МГ
МЕЖГОРОД	Разрешены внутренние, городские и междугородние вызовы. Запрещены международные вызовы.	<ul style="list-style-type: none"> 810-МН

Для международных вызовов, имеющих максимальные разрешения, класс ограничений не нужен.

Создаем три класса ограничений (см. [Рисунок 169](#), [Рисунок 170](#), [Рисунок 171](#), [Рисунок 172](#)):

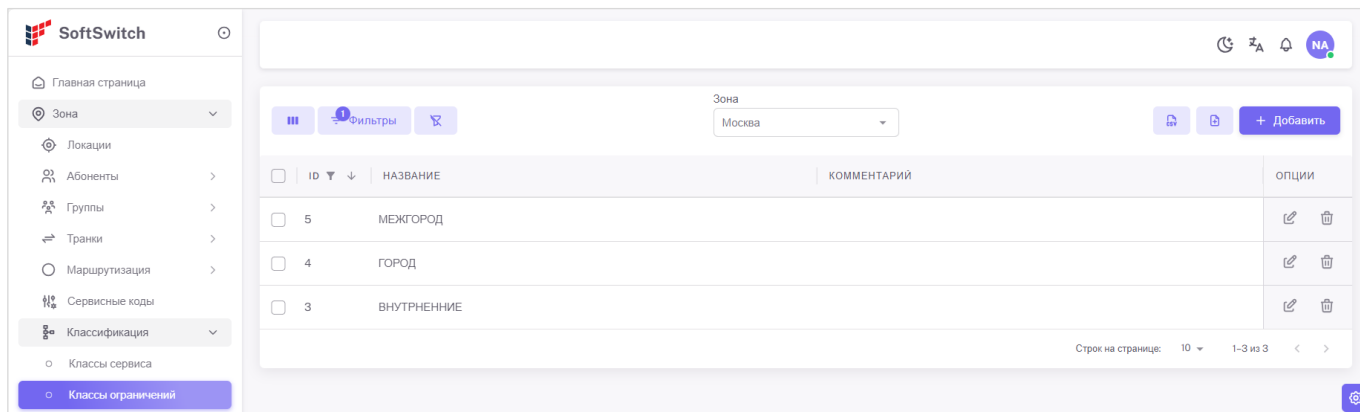


Рисунок 169. Список классов ограничений

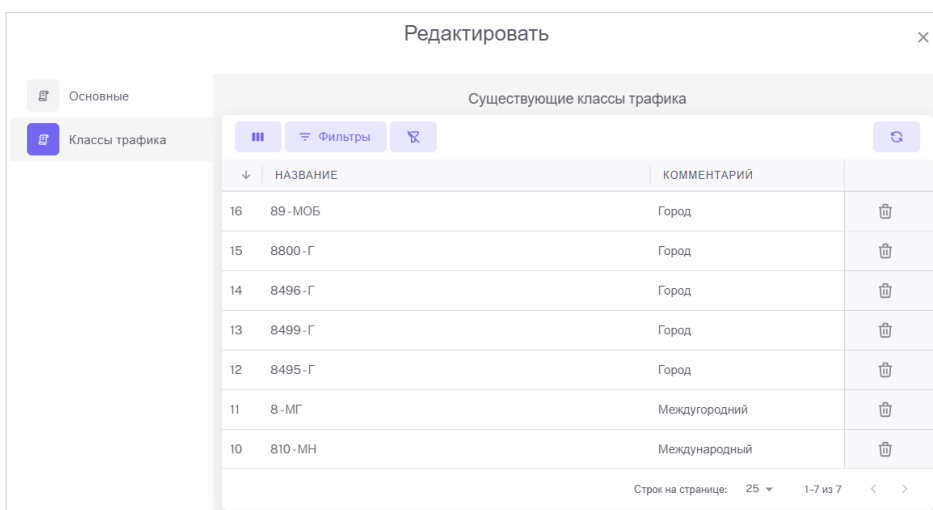


Рисунок 170. Класс ограничений "Внутренние"

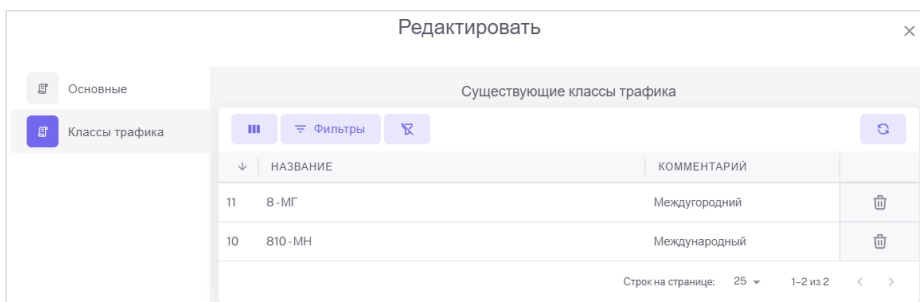


Рисунок 171. Класс ограничений "Город"

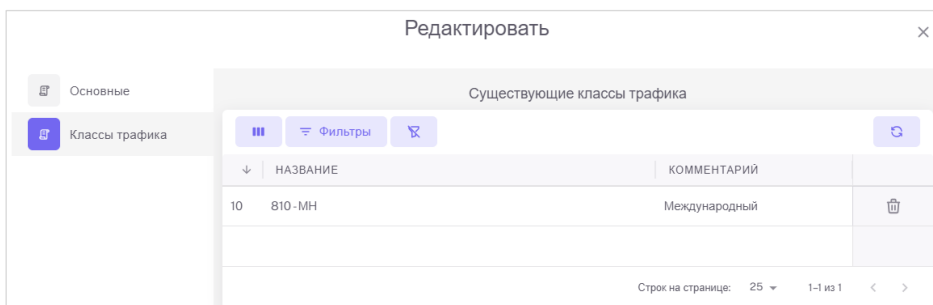


Рисунок 172. Класс ограничений "Межгород"

3. Назначение абонентам класса ограничений.

Четырем абонентам назначаем класс ограничений:

Абонент	Назначаемый класс ограничений	Ограничения
Кладовщик	ВНУТРЕННИЕ	Разрешены только внутренние вызовы.
Менеджер	ГОРОД	Разрешены внутренние и городские вызовы. Запрещены междугородние и международные вызовы.
Руководитель отдела	МЕЖГОРОД	Разрешены внутренние, городские и междугородние вызовы. Запрещены международные вызовы.
Директор		Разрешены все вызовы, включая международные.

Абоненту «Директор» ни один класс ограничений не назначен, ему будут доступны все вызовы, включая международные.

4. Создание правил первичной маршрутизации.

Создаем правила первичной маршрутизации под каждый класс трафика (см. [Рисунок 173](#)):

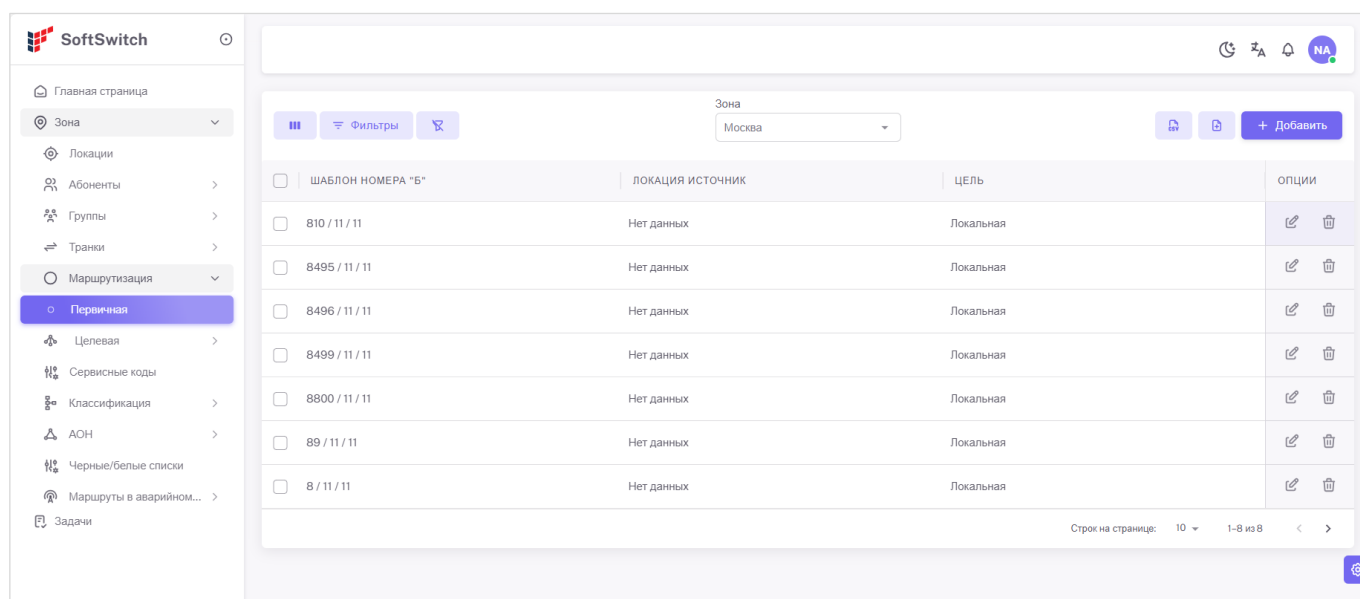


Рисунок 173. Правила первичной маршрутизации

Подробное описание процесса обработки правил первичной маршрутизации рассмотрено в отдельном разделе (см. [Маршрутизация первичная](#)).

5. Создание правила целевой маршрутизации.

Согласно условиям примера, после прохождения первичной маршрутизации вызовы должны направляться в единственный транк для выхода в сеть общего пользования. Для этого создаем правило целевой маршрутизации (см. [Рисунок 174](#)):

Рисунок 174. Правило целевой маршрутизации

При соответствии цифр вызываемого номера *шаблону номера "Б"* правила, а именно, длина номера равна 11 знакам, и номер начинается с цифры 8, происходит направление вызова в указанный транк.

Подробное описание процесса обработки правил целевой маршрутизации рассмотрено в отдельном разделе (см. [Маршрутизация целевая](#)).

Применение классов сервиса

Исходные данные. Для VIP-абонента необходимо организовать маршрутизацию «в город» по выделенному транку.

Сначала необходимо создать соответствующие класс трафика и класс сервиса (см. [Рисунок 175](#) и [Рисунок 176](#), [Рисунок 177](#)):

Рисунок 175. Создаем класс трафика VIP

Рисунок 176. Создаем класс сервиса CoS-VIP

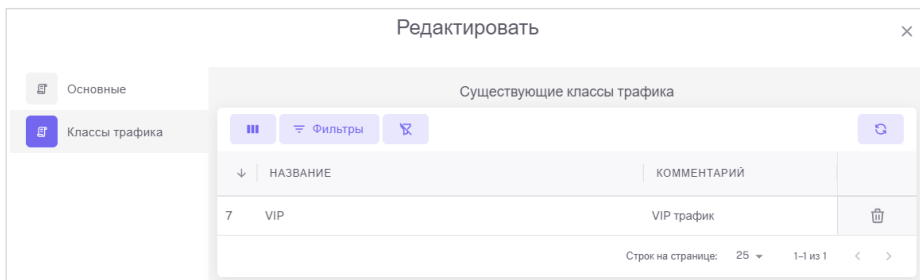


Рисунок 177. Включаем в класс сервиса класс трафика VIP

Далее, VIP-абоненту присваиваем класс сервиса «CoS-VIP» (см. [Рисунок 178](#)):

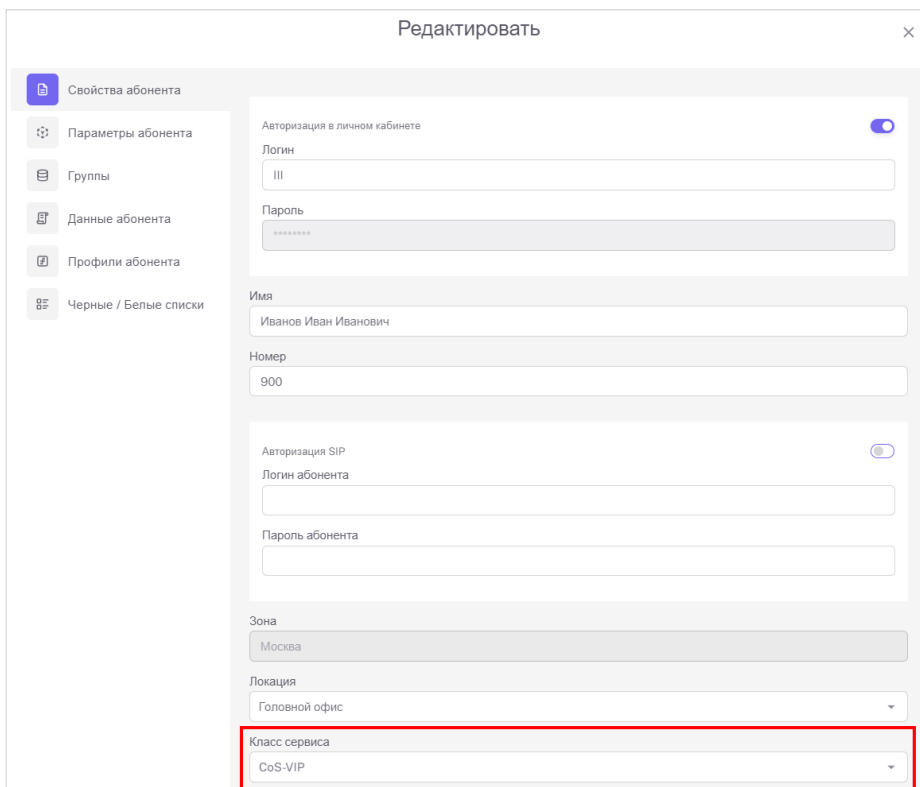


Рисунок 178. VIP-абоненту присваиваем класс сервиса «CoS-VIP»

Создаем правило первичной маршрутизации (см. [Рисунок 179](#)):

Редактировать

Использовать шаблоны Использовать регулярные выражения

Шаблон номера "Б" (Префикс / Мин. / Макс.)

Шаблон номера "А" (Префикс / Мин. / Макс.)

Домен

Модификатор номера Б(удалить / вставить)

Модификатор номера А (удалить / вставить)

Цель
 Локальная

Класс трафика
 Пустой

Зона
 Москва

Источник
 Головной офис

Описание

Сохранить Закрыть

Рисунок 179. Создаем правило первичной маршрутизации

Создаем правило целевой маршрутизации (см. [Рисунок 180](#)):

Редактировать

Использовать шаблоны Использовать регулярные выражения

Шаблон номера "Б" (Префикс / Мин. / Макс.)

Шаблон номера "А" (Префикс / Мин. / Макс.)

Домен

Модификатор номера Б(удалить / вставить)

Цель
 Классификатор

Параметр
 VIP

Описание

Сохранить Закрыть

Рисунок 180. Создаем правило целевой маршрутизации

Создаем классификаторы default и VIP, в которых прописываем разные классы сервиса и разные транки (см. [Рисунок 181](#)):

Редактировать ×

Название

Зона

Источник

Класс сервиса

Класс трафика

Цель

Параметр

Описание

Рисунок 181. Создаем классификатор для VIP-абонентов

Настройка отправки уведомлений о пропущенных вызовах

Для отправки на электронную почту абонентов уведомлений о пропущенных вызовах создайте на локальном почтовом сервере учетную запись, от имени которой будут отправляться письма, и отдельное правило для отправки без авторизации.

Откройте на редактирование файл `/opt/flat/fss-server/settings.ini` и в разделе **[Email]** укажите следующие параметры:

from= – адрес учетной записи, от имени которой будут отправляться уведомления;

fromname= – имя отправителя;

host= – адрес SMTP-сервера.

Сохраните изменения и перезагрузите сервис командой:

```
service flat_ss restart
```

Включите опцию отправки уведомлений в параметрах абонента и в соответствующем поле укажите его электронный адрес (см. [Рисунок 182](#)):

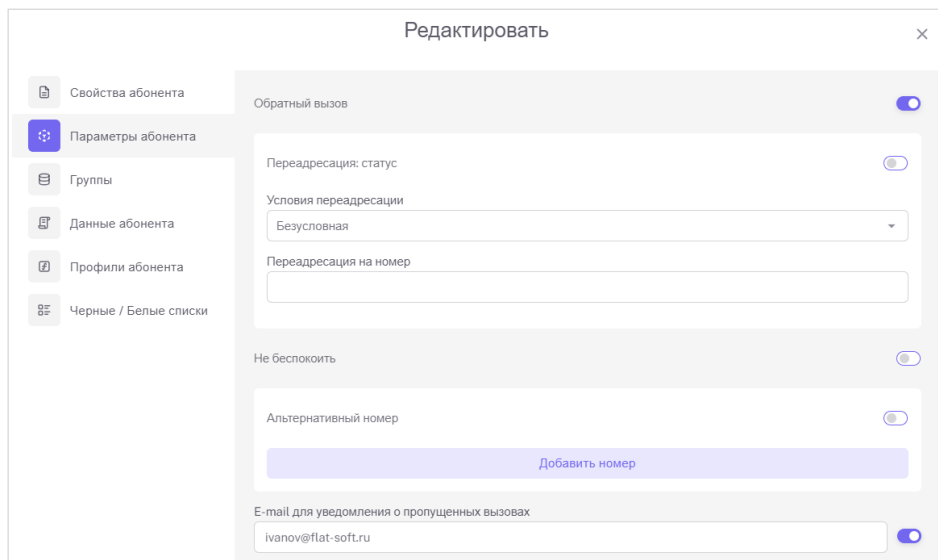


Рисунок 182. E-mail для уведомлений

Функции и возможности системы ФЛАТ SoftSwitch

В разделе представлена справочная информация о функциях и возможностях, влияющих на работу системы ФЛАТ SoftSwitch.

Интервал проверки состояния транка

При указании параметра «Интервал проверки (сек.)» (см. [Вкладка «Общие»](#)) происходит проверка состояния транка с заданной периодичностью посредством отправки запроса OPTIONS.

Таймаут ожидания ответа на вызов

Таймаут ожидания ответа на вызов составляет 120 секунд.

Индикация статусов BLF

BLF (Busy Lamp Field) – это функция SIP-телефонов, которая позволяет отслеживать текущее состояние линий других абонентов ФЛАТ SoftSwitch с помощью светящихся индикаторов на кнопках телефонных аппаратов, а так же пиксельных картинок на ТА, имеющих экраны.

Для телефонных аппаратов, оснащенных цветными экранами цвет пиксельной картинке совпадает с цветом индикатора статуса линии. Для телефонных аппаратов, оснащенных ч/б экраном статус обозначается выводимым пиксельной картинкой изображением.

Предусмотрены следующие статусы:

Состояние индикатора	Цвет пиксельной картинки	Статус контролируемой линии
Выключен	Черный	Абонент не зарегистрирован.
	Зеленый	Линия свободна.
Зеленый	Зеленый	Линия свободна.
Красный	Красный	Линия занята.

Настройка отображаемых статусов телефонных линий выполняется с помощью программного обеспечения ФЛАТ Device Manager (см. документацию по указанному ПО).

Дополнительные виды обслуживания

В разделе представлена справочная информация о ДВО (дополнительных видах обслуживания) системы ФЛАТ SoftSwitch.

Функция «Обратный вызов»

Функция позволяет назначить обратный вызов в случае, когда вызывающий абонент не дожидается ответа. Запрос обратного вызова происходит по вводимому с клавиатуры сервисному коду (см. [Сервисные коды](#)), а для телефонных аппаратов с экранным меню выбором соответствующего пункта. Для телефонных аппаратов с экранным меню необходимо выполнить настройки с помощью программного обеспечения ФЛАТ Device Manager (см. документацию по указанному ПО). Запрос обратного вызова может быть отменен вводом сервисного кода отмены.

Пример для ТА без экранного меню: Абонент «А» вызывает абонента «В», и, не дождавшись ответа, запрашивает обратный вызов с помощью набора сервисного кода на цифровой клавиатуре. При этом, абонент «А» слышит уведомление о запрошенном обратном вызове и завершает звонок. Абонент «В» совершает действие, после которого абоненту «А» поступает обратный вызов от абонента «В».

Пример для ТА с экранным меню: Абонент «А» вызывает абонента «В», и, не дождавшись ответа, запрашивает обратный вызов выбором пункта экранного меню телефонного аппарата. Абонент «В» совершает действие, после которого абонент «А» получает уведомление на экране телефонного аппарата, с помощью экранного меню осуществляет вызов абонента «В».

Функция «Перехват вызова в группе»

Эта функция позволяет перехватывать вызовы, которые приходят на другие телефоны, состоящие в одной группе перехвата.

Множественная регистрация

«Множественная регистрация» – возможность зарегистрировать на один номер несколько телефонных аппаратов. Применяется в случае, когда сотрудникам необходимо зарегистрировать на один номер несколько устройств (в зависимости от выбранной лицензии до 10 регистраций на один номер со стационарных телефонов, либо программных клиентов ФЛАТ Партнер для различных ОС).

Входящий вызов приходит на все зарегистрированные устройства. Исходящие вызовы доступны одновременно для всех зарегистрированных устройств.

Поддержка множественной регистрации включается в свойствах абонента (см. [Вкладка «Свойства абонента»](#)).

Функция «Shared line»

«Shared line» – совместное использование второй линии несколькими телефонными аппаратами Cisco и Yealink с отображением статуса общей линии и номера

Входящий вызов на общий номер приходит на все зарегистрированные ТА. Исходящие вызовы с общей линии доступны одновременно для всех зарегистрированных устройств.

Настройки отображения статуса общей линии на ТА выполняется с помощью программного обеспечения ФЛАТ Device Manager (см. документацию по указанному ПО).

Пример: Телефонным аппаратам Cisco с номерами «1021» и «1022» необходимо подключить общую линию с номером 1030. Для этого создается абонент с номером «1030», в свойствах которого включается опция «Множественная регистрация». В свойствах абонентов «1021» и «1022» включается опция «Shared line» и указывается номер общей линии «1030».



Включение опции «Shared line» для ТА Cisco приводит к отключению стандартного механизма индикации BLF этих аппаратов. Для отображения индикаторов BLF включите опцию «Серверный BLF» (см. [Вкладка «Параметры абонента»](#)).

SNMP мониторинг

SNMP мониторинг доступен для ядра ФЛАТ SoftSwitch и Медиа сервера. Поддерживается реализация SNMPv2.

SNMP мониторинг ядра ФЛАТ SoftSwitch

Для взаимодействия с системой мониторинга необходимо в конфигурационном файле `/opt/flat/fss-server/settings.ini` в разделе `[EventMessenger]` указать следующие параметры:

Enabled=1 – включить SNMP мониторинг;

SNMPHost=10.77.5.25 – указать IP адрес системы мониторинга;

SNMPport=60161 – указать порт, на котором ядро принимает SNMP-запросы.

Перед настройкой SNMP, необходимо отключить системные сервисы мониторинга, использующие порт прослушивания 60161. Проверьте какие процессы используют этот порт командой: **ss -tulpan | grep 60161**.

Для получения информации о состоянии ядра ФЛАТ SoftSwitch по протоколу SNMP укажите в системе мониторинга IP-адрес хоста ядра системы, порт взаимодействия и следующие коды параметров:

Коды OID	Описание
1.3.6.1.2.2.32.10.1.1	Общее количество текущих соединений
1.3.6.1.2.2.32.10.1.2.x	Состояние транка, где x - id транка
1.3.6.1.2.2.32.10.1.3.x	Текущее количество соединений на транке, где x - id транка
1.3.6.1.2.2.32.10.1.4	Uptime
1.3.6.1.2.2.32.10.1.5	Количество зарегистрированных абонентов
1.3.6.1.2.2.32.10.1.6	Количество свободных лицензий
1.3.6.1.2.2.32.10.1.7.x	Состояние Медиа сервера, где x - id Медиа сервера

Метрики функционирования VM (загрузка ЦПУ, оперативной памяти, и т.д.) получают средствами ОС.

SNMP мониторинг Медиа сервера

Для взаимодействия с системой мониторинга необходимо в конфигурационном файле `/opt/flat/fss-mediasrv/config.xml` указать следующие параметры:

<SnmPort>60163</SnmPort> – указать порт, на котором Медиа сервер принимает SNMP-запросы;

<Community>public</Community> – указать слово-пароль «**public**», по которому проверяются сообщения.

Для получения информации о состоянии Медиа сервера по протоколу SNMP укажите в системе мониторинга IP-адрес хоста Медиа сервера, порт взаимодействия и следующие коды параметров:

Коды OID	Описание
1.1.3.6.1.2.2.32.30.1.1	Количество участников конференции.
1.1.3.6.1.2.2.32.30.1.4	Время работы приложения в секундах.

Формат аудиофайлов пользовательских звуковых оповещений

В системе ФЛАТ SoftSwitch допустимо вместо стандартных звуковых оповещений использовать свои звуковые файлы. Формат пользовательского звукового файла – расширение WAV, кодек G.711 A-law (PCMA), частота дискретизации 8 кГц, битрейт 64 кбит/с.

Конвертация аудиофайла (Linux)

Исходный файл может быть в формате MP3 или WAV. Битрейт и прочие параметры не важны.

В примере показана конвертация файла *on_hold.mp3*.

1. Установите приложения SOX и LAME:

```
apt install -y lame sox
```

2. Выполните команду декодирования файла *on_hold.mp3* в *on_hold.wav*:

```
lame --decode on_hold.mp3
```

3. Выполните команду конвертации *on_hold.wav* в файл *on_hold_pcm.wav* формата PCM 8000 Гц 16 бит:

```
sox on_hold.wav -t wav -b 16 -r 8000 -c 1 on_hold_pcm.wav
```

Конвертация аудиофайла на примере приложения Audacity (Windows)

1. Запустите Audacity и откройте исходный аудиофайл.

2. Выполните преобразование из стерео в моно (см. [Рисунок 183](#)):

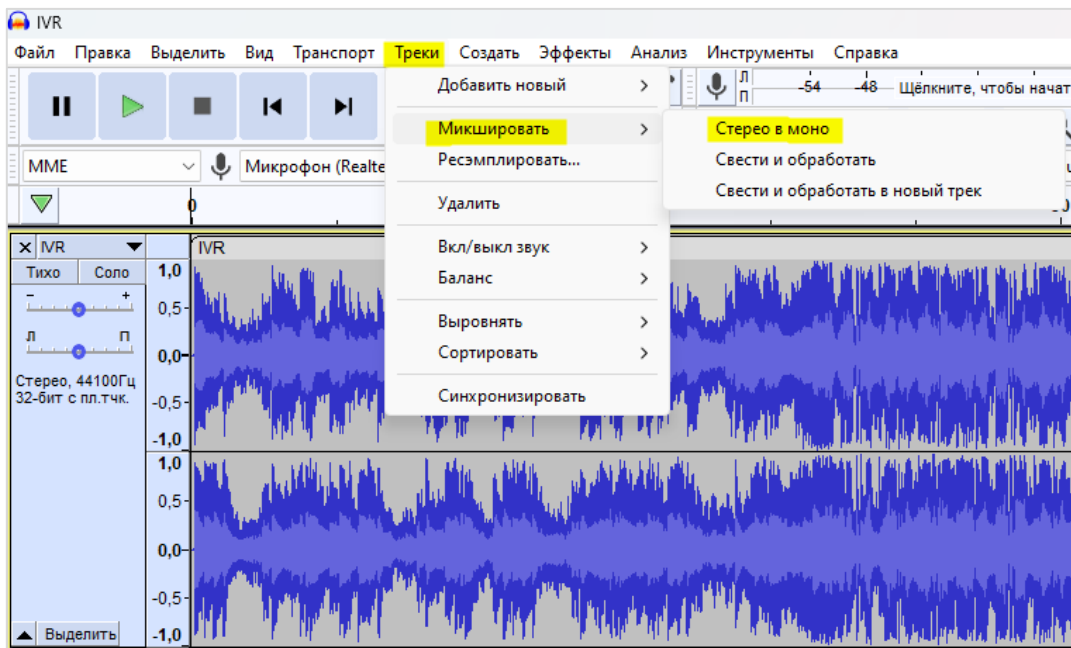


Рисунок 183. Преобразование из стерео в моно

3. Измените частоту проекта на 8 кГц (см. [Рисунок 184](#)):

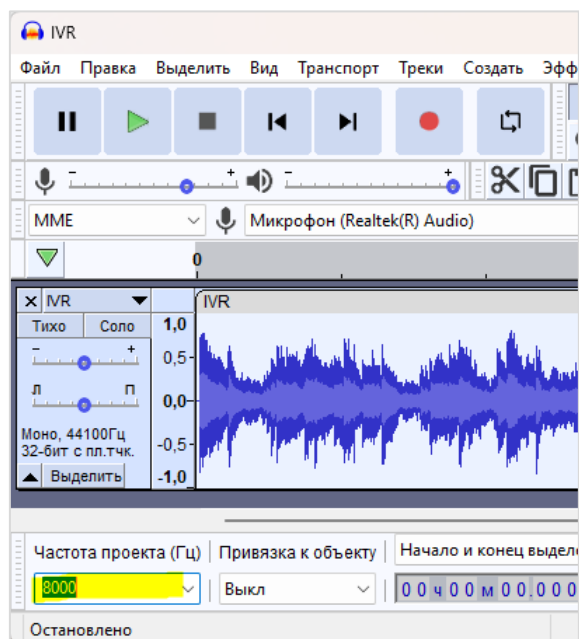


Рисунок 184. Изменение частоты

4. Выберите экспорт проекта в формат WAV (см. [Рисунок 185](#)):

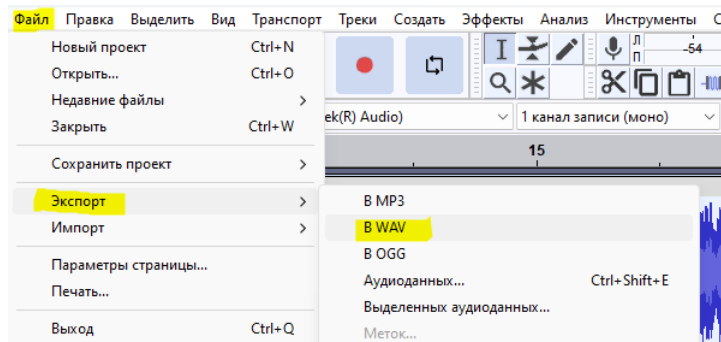


Рисунок 185. Экспорт проекта в формат WAV

5. Выберите кодирование в A-law (см. [Рисунок 186](#)):

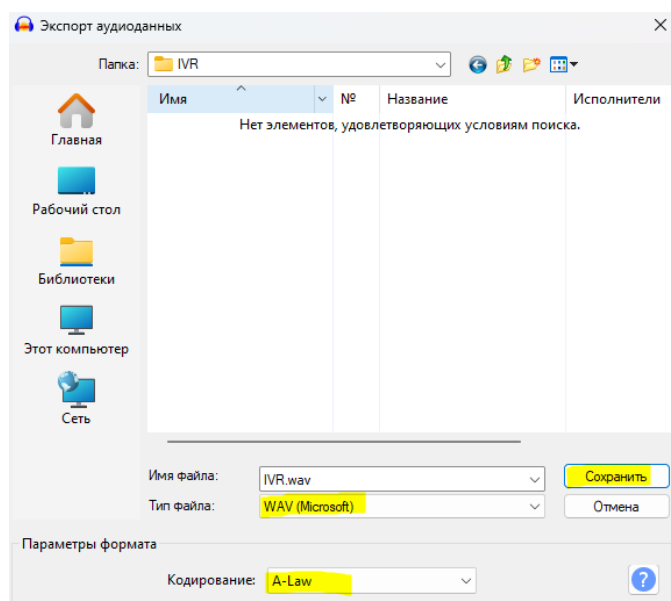


Рисунок 186. Кодирование в A-law

6. Выполните очистку метаданных и сохраните файл (см. [Рисунок 187](#)):

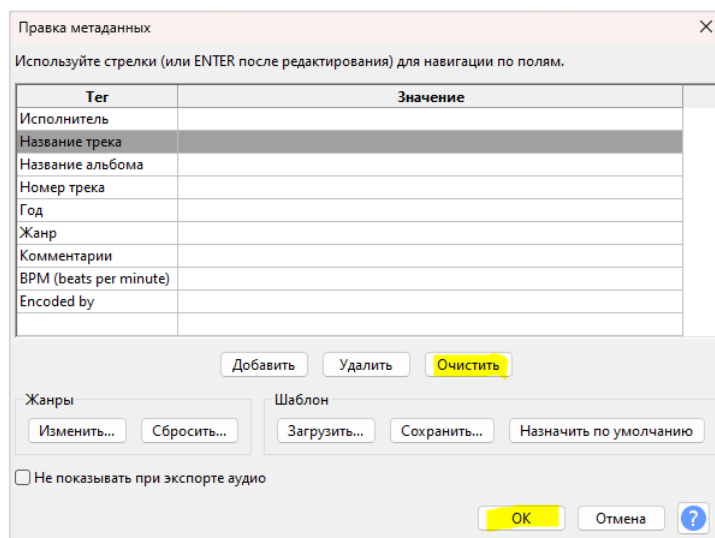


Рисунок 187. Очистка метаданных

7. Проверьте в свойствах полученного аудиофайла соответствие скорости потока параметрам кодека G.711 64 кбит/с (см. [Рисунок 188](#)):

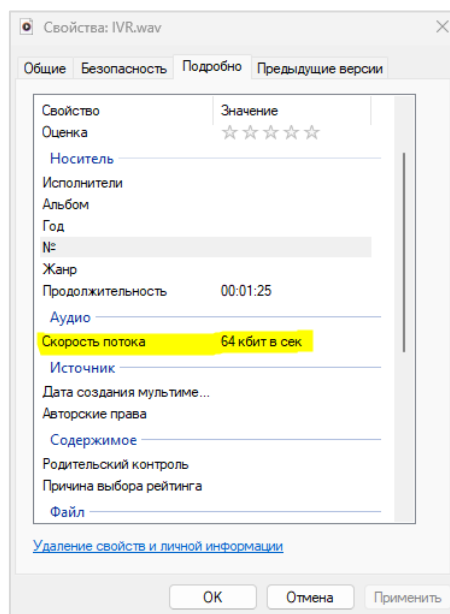


Рисунок 188. Параметры полученного аудиофайла

Описание конфигурационных файлов

Ядро системы

Файл settings.ini содержит в себе параметры необходимые для работы ядра ФЛАТ SoftSwitch.

Расположение файла `/opt/flat/fss-server/settings.ini`

Параметр	Значение по умолчанию	Описание
[General]		
Database	rapidcall	Имя БД.
Server		IP-адрес сервера БД.
UID	rapid	Логин для доступа к БД.
PWD	QwSDv	Пароль для доступа к БД.
License		Лицензионный ключ.
NodeID		Идентификатор ноды.
LocationID		Идентификатор локации, заполняется на сервере Живучего Офиса.
UseMultiTenant	0	Использовать разделение зон по доменным именам для закрытой нумерации.
LicenseServerHost		IP-адрес лицензионного сервера.
LicenseServerPort	1550	Порт лицензионного сервера.
encrypted	0	Использование зашифрованного пароля. 1 – включено, 0 – выключено. Шифрование пароля выполняется бэкендом ФЛАТ SoftSwitch.
[SIP]		
SelfDomain		Доменное имя сервера SoftSwitch.
LogLevel	3	Базовый уровень логирования.
SelfIP		IP-адрес сервера SoftSwitch.
SelfUDPPort	5060	Порт для UDP.
SelfTCPport	5060	Порт для TCP.
SelfTLSport	5061	Порт для TLS.
TLSProto	10	Версия TLS – 10/11/12.
MaxConnections	0	Ограничение количества соединений SoftSwitch (по умолчанию нет ограничений).
RegisterMaxAttempts	0	Ограничение количества попыток неуспешных регистраций абонентский устройств (по умолчанию нет ограничений).
[email]		
Используется для отправки уведомлений о пропущенных вызовах		
from		Адрес FROM.

Параметр	Значение по умолчанию	Описание
fromname		Имя FROM.
host		IP-адрес SMTP-сервера.
[EventMessenger]		
Enabled	0	1 – включить SNMP-мониторинг, 0 – выключить.
Host		Адрес SMTP-сервера
From		Адрес FROM
FromName		Имя FROM
SNMPHost		Адрес SNMP-сервера
SNMPPort		Локальный порт SNMP
SNMPVersion		Версия протокола (1,2,3)
SNMPUser		Логин (для V3)
SNMPPass		Пароль (для V3)
[Log]		
LogSizeLimit	20480M	Ограничение размера папки с логами.
LogPath	/var/log/fss-server/	Путь хранения лог-файлов ядра системы.
SysLogLevel	normal	Уровень логирования. Допустимые значения: critical, error, normal, debug, advanced.
UseUTC		Выводить в лог время в UTC. 1 – включено, 0 – выключено.
[API]		
TokenLifeTime		Время жизни токена (в секундах).
WebPort	1541	Локальный порт для REST API.

Бэкенд WEB-интерфейса ФЛАТ SoftSwitch

Файл config.yml содержит в себе параметры необходимые для работы бэкенда WEB-интерфейса ФЛАТ SoftSwitch.

```
/usr/lib/flatSoftSwitchBackend/config.yml
```

```
# Настройки аутентификации
```

```
auth:
```

```
# Время жизни access токена в минутах. По умолчанию 15 минут.
```

```
# Для SSO время жизни токена согласно настройкам IDP
```

```
access_token_ttl: 30
```

```
# Ключ шифрования access токена.
```

```
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
```

```
# ./flatSoftSwitchBackend_1.0.0 encrypt --text='....'
```

```
key: e519925533aa70b2ec1fff24f19854729eb3e319972aa43ee0901982741e0fe5be8c365934bf9ad2
```

```
# Настройки аутентификации через Active Directory.
```

```
ldap:
```

```
# Адрес AD
```

```
# ldap://example.com:389
```

```
# ldaps://example.com:636
```

```
addr: ldap://10.77.13.11:389
```

```
# BaseDN пользователей
```

```
# Если включена синхронизация через LDAPSynchronizer, рекомендуется скопировать
```

```
# base_dn из config.json.
```

```
base_dn: OU=OrganizationalUnit,DC=example,DC=com
```

```
# Фильтрация пользователей.
```

```
# Если нужно разрешить доступ только пользователям из определенной группы или
```

```
# по другому признаку.
```

```
# Оставьте пустым, если хотите разрешить доступ всем пользователям из BaseDN.
```

```
base_filter: (objectClass=Person)
```

```
# Домен AD.
```

```
# Требуется для авторизации пользователей - login_attr + @ + example.com
```

```
domain: example.com
```

```
# Укажите true для включения
```

```
enabled: false
```

```
# Из какого параметра извлекать Логин. Принимает одно значение.
```

```
# Если включена синхронизация через LDAPSynchronizer, рекомендуется скопировать
```

```
# data.login из config.json.
```

```
# Обычно sAMAccountName или cn
```

```
login_attr: sAMAccountName
```

```
# Время жизни refresh токена в минутах. По умолчанию 540 минут - 8 часов.
```

```
refresh_token_ttl: 540
```

```
# Настройки SSO
```

```
sso:
```

```
# Настройки OIDC
```

```
oidc:
```

```
# ID клиента
```

```
client_id:
```

```

# Секретный ключ
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
# ./flatSoftSwitchBackend_1.0.0 encrypt --text='....'
client_secret:

# Укажите адрес для извлечения конфигурации провайдера
# Отправится запрос по адресу config_url + /.well-known/openid-configuration
config_url: http://10.77.13.11/oauth2/token

# Укажите true для включения
enabled: false

# Из какого параметра извлекать Логин
# По умолчанию sub
login_attr: sub

# Адрес данного сервиса.
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
root_url: http://10.77.13.11:443

# Адреса админ сервисов(frontend), которым разрешена OIDC аутентификация
# Принимает массив (несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:
  - http://10.77.13.11:3000

# Настройки SAML
saml:

# Самоподписанный сертификат
# openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
# -days 365 -nodes -subj "/CN=myservice.example.com"
cert_file:

# Укажите true для включения
enabled: false

# Самоподписанный ключ
# openssl req -x509 -newkey rsa:2048 -keyout myservice.key -out myservice.cert
# -days 365 -nodes -subj "/CN=myservice.example.com"
key_file:

# Из какого параметра извлекать Логин
# По умолчанию http://wso2.org/claims/username
login_attr: http://wso2.org/claims/username

# Если файл xml расположен на сервере, укажите полный путь к нему
# У текущего пользователя должны быть права на чтение
meta_data_path: /etc/metadata.xml

# Если xml расположен на сервере IDP, укажите его адрес
# https://example.com:8443/realms/master/protocol/saml/descriptor
meta_data_url:

# Адрес данного сервиса.
# Если настроен nginx, домен и порт должны совпадать с настройками nginx
root_url: https://10.77.13.11:443

# Адреса админ сервисов (frontend), которым разрешена OIDC аутентификация
# Принимает массив (несколько адресов)
# Удалите все адреса, чтобы снять ограничение (не рекомендуется)
valid_redirect_urls:

```

```
- http://10.77.13.11:3000
```

```
# Настройки БД.
```

```
db:
```

```
# Настройка подключения к MariaDB.
```

```
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
```

```
# ./flatSoftSwitchBackend_1.0.0 encrypt --text='....'
```

```
dsn: fd36914520c259bfc62cc00fddaf6d19cee5a346fe76ff7b93d454d3387d52b2edf6486814b9b0d5
```

```
# Максимальное количество неактивных подключений к базе данных
```

```
max_idle_conn: 10
```

```
# Максимальное количество открытых подключений к базе данных
```

```
max_open_conn: 100
```

```
# Настройки Device Manager
```

```
device_manager:
```

```
# Укажите true для включения
```

```
enabled: false
```

```
# Логин
```

```
# Нужно создать пользователя на DM с логином API
```

```
login: API
```

```
# Пароль
```

```
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
```

```
# ./flatSoftSwitchBackend_1.0.0 encrypt --text=....
```

```
password:
```

```
# Адрес DM
```

```
url: https://10.77.13.20
```

```
# Настройки файлового менеджера FFM
```

```
ffm:
```

```
# Установите FFM на сервере SoftSwitch
```

```
# Добавьте сервис fss-backup в config.yml
```

```
# В настройках укажите папку с бэкапами софт-свитча
```

```
# (/opt/flat/fss-server/backup) и перезапустите сервис
```

```
# Параметр принимает адрес FFM
```

```
fss-backup: http://localhost:8053
```

```
# Установите FFM на сервере SoftSwitch
```

```
# Добавьте сервис fss-logs в config.yml
```

```
# В настройках укажите папку с логами софт-свитча
```

```
# (/var/log/fss-server) и перезапустите сервис
```

```
# Параметр принимает адрес FFM
```

```
fss-logs: http://localhost:8053
```

```
# НЕ РЕДАКТИРОВАТЬ. Всегда должен быть false.
```

```
force: false
```

```
# Настройки FPS
```

```
fps:
```

```
# Укажите true для включения
```

```
enabled: false
```

```
# Адрес
```

```
url: 10.77.13.15:5081
```

```
# Настройка сети
```

```
http:
```

```
# Адрес
# localhost - при настройке nginx(http/https или домен)
# ip адрес - доступ по IP адресу, настройка nginx не требуется
host: localhost

# Порт
# Укажите любой свободный порт
# При настройке nginx укажите этот порт в проху настройках
port: 8051

# Настройка логирования
log:

# Архивация файлов -> max_backups.
# Каждый файл архивируется отдельно
compress: true

# production или development
debug: production

# Путь к папке с логами
# Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
folder: /var/log/flatSoftSwitchBackend

# Максимальное время хранения
max_age: 28

# Максимальное количество файлов
max_backups: 4

# Максимальный размер файла
max_size: 10

# Настройка подключения к REDIS
redis:

# Адреса
address:
  - localhost:6379

# Включить кластер
cluster_mode: false

# Номер БД
db: 0

# Максимальное количество попыток подключения
max_retry: 10

# Пароль. По умолчанию пусто
# ЗАШИФРОВАННАЯ СТРОКА. Шифровать нужно этим же сервисом
# ./flatSoftSwitchBackend_1.0.0 encrypt --text='....'
password:

# Логин. По умолчанию пусто
username:

# Настройки подключения к SoftSwitch
soft_switch:

# Путь хранения бэкапов на сервере софт-свитча
# По умолчанию /opt/flat/fss-server/backup
backup_dir: /opt/flat/fss-server/backup
```

Адрес

url: 10.77.13.34:1540

НЕ РЕДАКТИРОВАТЬ. Версия конфига.

version: 7

Фронтенд WEB-интерфейса ФЛАТ SoftSwitch

Файл `config.json` содержит в себе параметры необходимые для работы фронтенда WEB-интерфейса ФЛАТ SoftSwitch.

В файле `/opt/flat/fss-frontend/apps/softswitch/public/config.json` должны быть указаны параметры:

addresses – IP-адрес (или FQDN) и порт взаимодействия бэкенда ФЛАТ SoftSwitch.

isDomainAuthEnable – укажите **true** при аутентификации с использованием AD, или **false** без использования.

isSSOEnable – укажите **true** при аутентификации с использованием SSO, или **false** без использования.

```
/opt/flat/fss-frontend/apps/softswitch/server.js
```

```
{
  "addresses": [
    "10.77.13.11:443"
  ],
  "isDomainAuthEnable": true,
  "isSSOEnable": true
}
```

FlatFileManager

Файл `config.yml` содержит в себе параметры необходимые для работы модуля FlatFileManager, ответственного за обеспечение взаимодействия между сервисами и файлами ОС.

```
/opt/flat/fss-file/config.yml
```

```
force: false
```

```
# Настройка сети
```

```
http:
```

```
  # Адрес
```

```
  # localhost - при настройке nginx (http/https или домен)
```

```
  # ip адрес - доступ по IP адресу, настройка nginx не требуется
```

```
  host: 10.77.13.34
```

```
  # Порт
```

```
  # Укажите любой свободный порт
```

```
  # При настройке nginx укажите этот порт в проху настройках
```

```
  port: 8053
```

```
# Настройка логирования
```

```
log:
```

```
  # Архивация файлов -> max_backups.
```

```
  # Каждый файл архивируется отдельно
```

```
  compress: false
```

```
  # production или development
```

```
  debug: development
```

```
  # Путь к папке с логами
```

```
  # Убедитесь, что к папке есть доступ для записи/чтения у текущего пользователя
```

```
  dir: /var/log/flat/fss-file
```

```
  # Максимальное время хранения
```

```
  max_age: 28
```

```
  # Максимальное количество файлов
```

```
  max_backups: 10
```

```
# Максимальный размер файла
max_size: 20

services:

contact-scripts:
  # Укажите true для включения
  enable: false
  # Разрешения
  rules:
    # Разрешение создавать каталоги
    create_dir: true
    # Разрешение создавать файлы
    create_file: true
    # Разрешение скачивать
    download: true
    # Разрешение удалять каталоги
    remove_dir: true
    # Разрешение удалять файлы
    remove_file: true
  # Путь хранения скриптов для ФЛАТ Контакт
  workdir: /opt/flat/scripts

# Резервное копирование для ФЛАТ SoftSwitch
fss-backup:
  # Укажите true для включения
  enable: true
  # Разрешения
  rules:
    # Разрешение создавать каталоги
    create_dir: true
    # Разрешение создавать файлы
    create_file: true
    # Разрешение скачивать
    download: true
    # Разрешение удалять каталоги
    remove_dir: true
    # Разрешение удалять файлы
    remove_file: true
  # Путь хранения резервных копий ФЛАТ SoftSwitch
  workdir: /opt/flat/fss-server/backup

# Логирование для ФЛАТ SoftSwitch
fss-logs:
  # Укажите true для включения
  enable: true
  # Разрешения
  rules:
    # Разрешение создавать каталоги
    create_dir: true
    # Разрешение создавать файлы
    create_file: true
    # Разрешение скачивать
    download: true
    # Разрешение удалять каталоги
    remove_dir: true
    # Разрешение удалять файлы
    remove_file: true
  # Путь хранения логов для ФЛАТ SoftSwitch
  workdir: /var/log/fss-server

# НЕ РЕДАКТИРОВАТЬ. Версия конфига.
version: 4
```

Сервис Mediasrv

Файл config.xml содержит в себе параметры необходимые для работы сервиса **Mediasrv**.

Расположение файла `/opt/flat/fss-mediasrv/config.xml`

Параметр	Значение по умолчанию	Описание
LocalIP		IP-адрес медиасервера.
RTPportStart	7000	Диапазон RTP-портов.
RTPportEnd	8000	
MaxParticipants	16	Максимальное количество участников конференции.
MGCPport	2427	MGCP-порт медиасервера.
MediaDir	media	Директория хранения медиафайлов.
SnmpPort	60163	SNMP-порт медиасервера.
Community	public	Тип community.
PlayerTimeout	180	Ограничение длительности сессии.
LogParams	<code>/var/log/flat/fss-mediasrv/mediasrv.log</code>	Путь хранения и имя лог-файлов.

Сервис SRClient

Файл settings.ini содержит в себе параметры необходимые для работы сервиса **SRClient**.

Расположение файла `/etc/flat/fss-srclient/settings.ini`

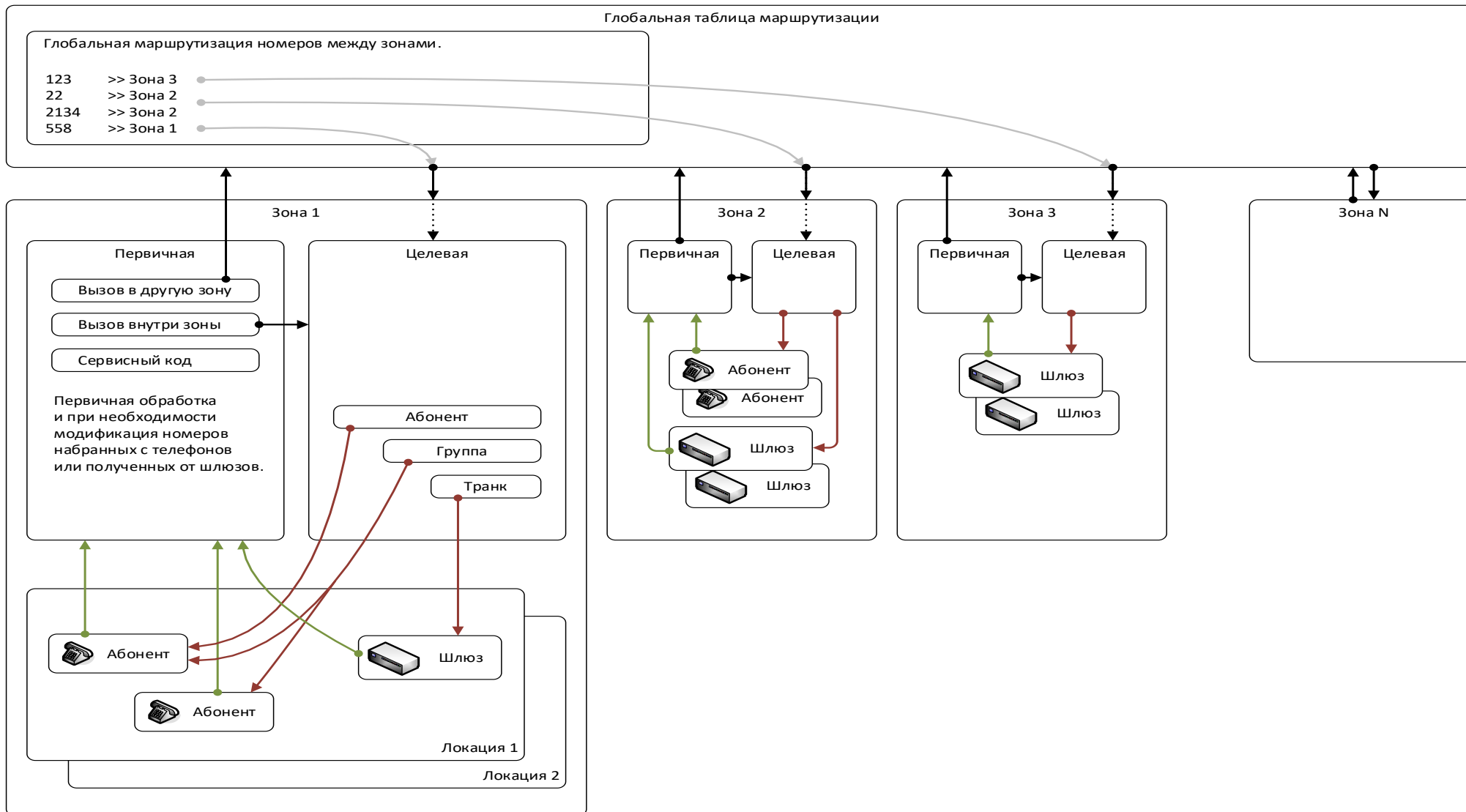
Параметр	Значение по умолчанию	Описание
localIp		IP-адрес SRC-клиента.
mgcpPort	2429	MGCP-порт сервиса SRClient.
sipPort	5062	SIP-порт сервиса SRClient.
startRtpPort	6000	Диапазон RTP-портов.
endRtpPort	7000	
logger_fileName	<code>/var/log/flat/fss-srclient/siprecclient.log</code>	Путь хранения и имя лог-файлов.
logger_fileSize	10000000	Максимальный размер логов в килобайтах.
logger_maxFiles	5	Максимальное количество файлов по 10 МБ, которые хранятся в логах.
logger_level	1	Уровень логирования. По умолчанию – 1.
threadsCount	4	Количество потоков медиасервера.
[SNMP]		
snmpPort	60161	Порт для протокола SNMP.
community	public	Тип community.

Словарь аббревиатур и сокращенных слов

Аббревиатура/сокращение	Значение
ДВО	Дополнительные виды обслуживания.
Кластер ФЛАТ SoftSwitch	Объединение двух узлов, работающих в режиме Active – Active, устанавливаемых на различные серверы.
Живучий Офис	Отказоустойчивый вынос, в виде узла ФЛАТ SoftSwitch, но без своего интерфейса управления. Управляется через настройки Локации в ядре, в котором задается аварийный режим работы узла Живучего Офиса.
Хост	Сервер, подключённый к локальной или глобальной сети.
BLF	Busy Lamp Field – светящаяся кнопка-индикатор на телефонном аппарате.

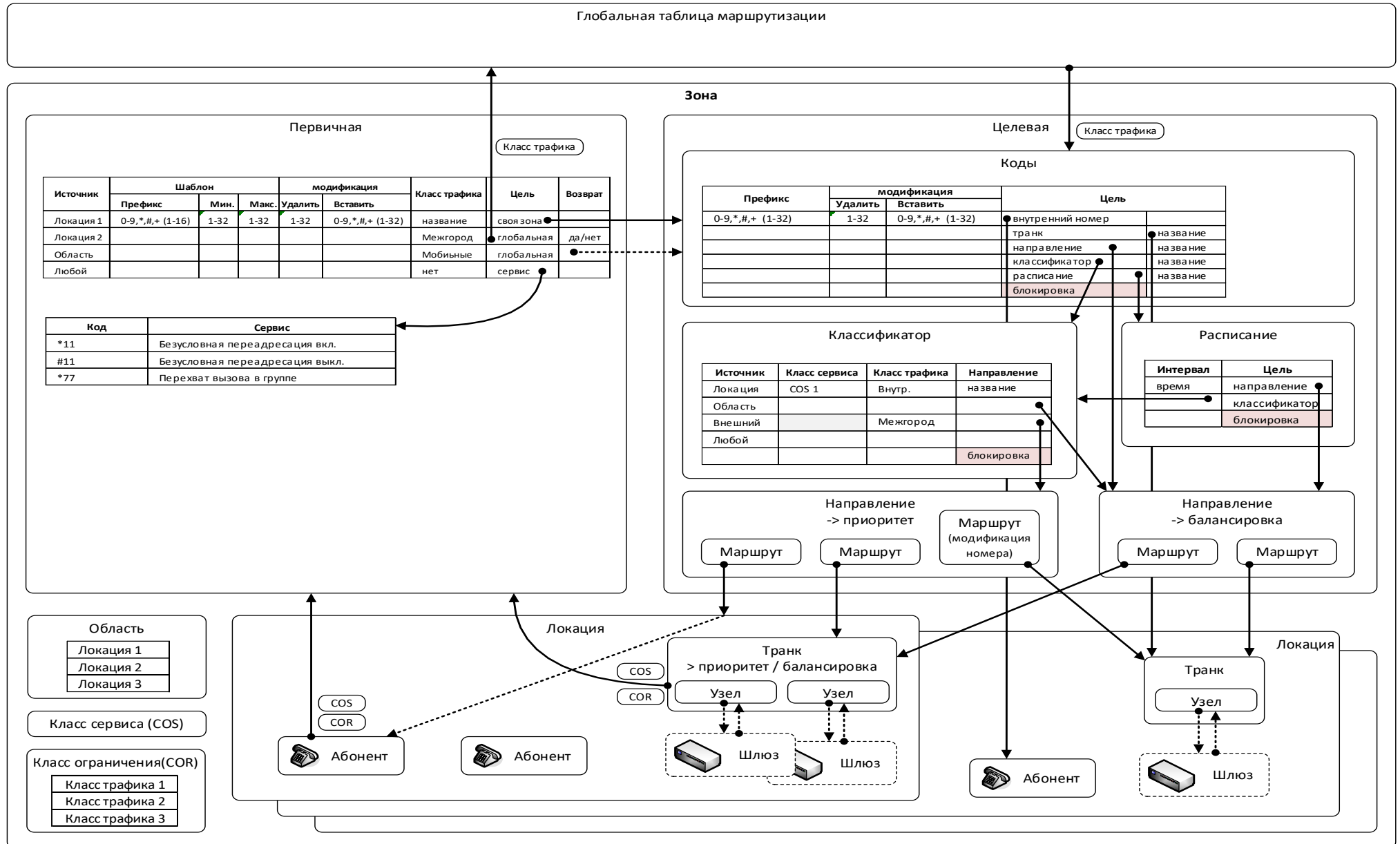
Таблица маршрутизации

Общая схема маршрутизации

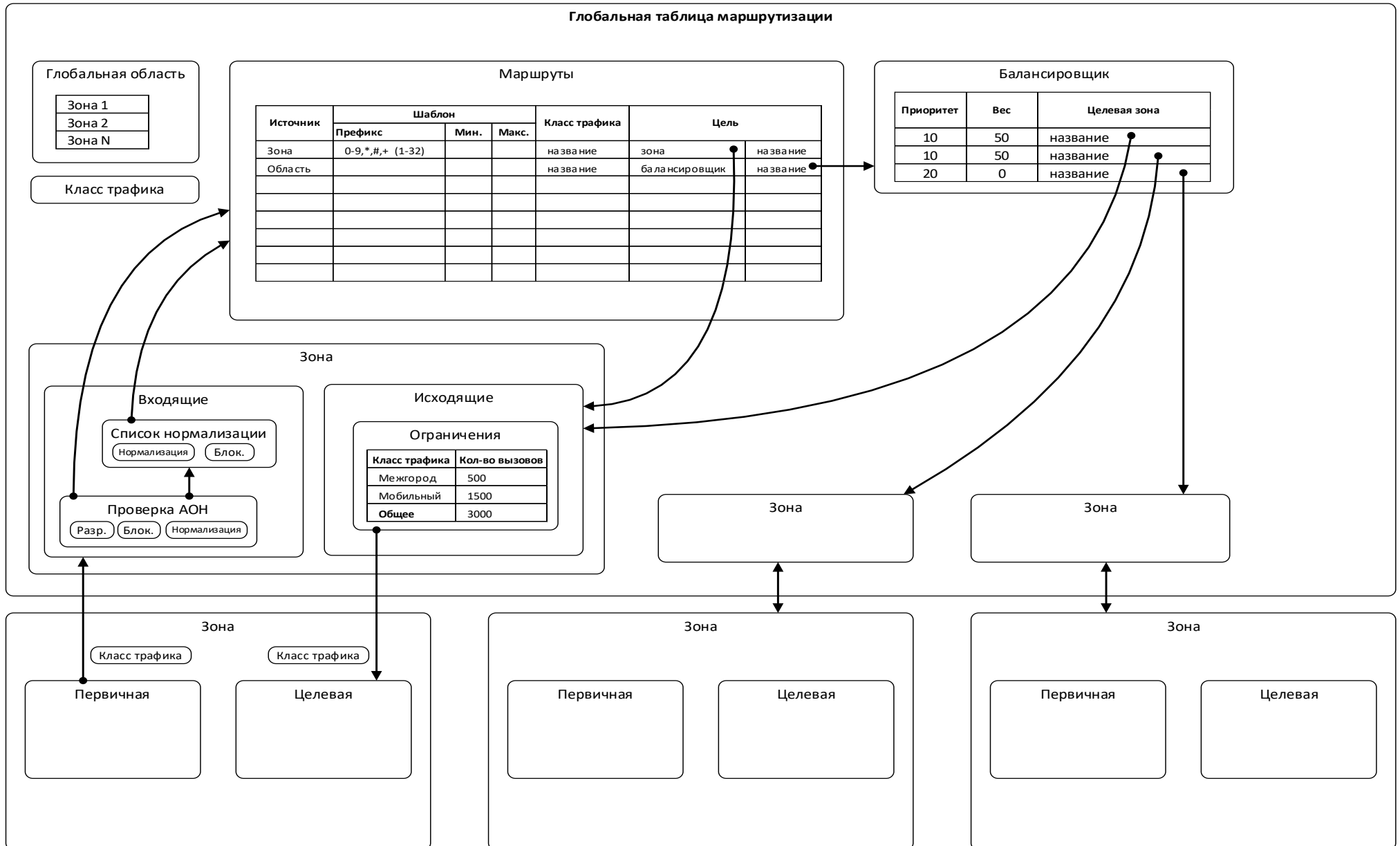


Внутризоновая маршрутизация

Глобальная таблица маршрутизации



Глобальная маршрутизация



Модификация АОН

