Общество с ограниченной ответственностью
«Научно-Технический Центр ПРОТЕЙ»
(ООО «НТЦ ПРОТЕЙ»)

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «ПРОТЕЙ-SBC»

ОПИСАНИЕ ПРОГРАММЫ

RUS.ПАМР.49300-01 13

Листов 37

2021

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата

Литера ___

Аннотация

Настоящий документ «Специальное программное обеспечение «ПРОТЕЙ-SBC». Описание программы» разработан на Специальное программное обеспечение «ПРОТЕЙ-SBC» (далее — ПРОТЕЙ-SBC, SBC) производства Общества с ограниченной ответственностью «Научно-Технический Центр ПРОТЕЙ» (далее — ООО «НТЦ ПРОТЕЙ»). Настоящий документ предназначен для подачи в Минцифры России вместе с заявлением о внесении сведений о программном обеспечении СПО ПРОТЕЙ-SBC в единый реестр российских программ для электронных вычислительных машин и баз данных.

Описание программы содержит следующую информацию:

1. Назначение, свойства и виды деятельности программы.
2. Объекты автоматизации СПО.
3. Функциональное назначение программы.
4. Описание структуры системы.
5. Описание подсистем СПО.

Настоящий документ разработан в соответствии с требованиями ГОСТ 19.402–78 «Единая система программной документации. Описание программы».

СОДЕРЖАНИЕ

1 Термины и сокращения

В таблице 1 приведены используемые в настоящем документе термины и сокращения.

Таблица 1 – Используемые термины и сокращения

Термин	Описание
ALG	Application-Level Gateway — шлюз прикладного уровня
CDR	Call Detail Record — подробная запись о вызове
CLI	Command Line Interface — интерфейс командной строки
DoS	Denial of Service — отказ в обслуживании
DTMF	Dual-Tone Multi-Frequency — двухтональный многочастотный аналоговый сигнал
FTP	File Transfer Protocol — протокол передачи файлов
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста
IMS	IP Multimedia Subsystem — спецификация передачи мультимедийного содержимого на базе IP
MCU	Multipoint Control Unit — сервер многоточечной конференции
NAT	Network Address Translation — преобразование сетевых адресов
NAPT	Network Address and Port Translation — преобразование сетевых адресов и портов
NGN	Next Generation Network — сеть следующего поколения
QoS	Quality of Service — качество обслуживания
RTCP	Real-Time Transport Control Protocol — протокол, управляющий передачей данных в режиме реального времени. Работает совместно с RTP
RTP	Real-Time Transport Protocol — протокол передачи данных в режиме реального времени
SBC	Session Border Controller — пограничный контроллер сессий
SCP	Secure Copy — протокол удалённого копирования файлов
SDP	Session Description Protocol — протокол описания сессий
SFTP	SSH File Transfer Protocol или Secure File Transfer Protocol — безопасный протокол передачи файлов
SIP	Session Initiation Protocol — протокол создания сессий
SNMP	Simple Network Management Protocol — протокол сетевого управления
SSH	Secure Shell — безопасная оболочка
TCP/IP	Transmission Control Protocol/Internet Protocol — протокол управления передачей/интернет-протокол
TLS	Transport Layer Security — протокол защиты транспортного уровня

Термин	Описание
ToS	Type of Service — тип обслуживания
UDP	User Datagram Protocol — протокол передачи датаграмм пользователей
URI	Uniform Resource Identifier — единый идентификатор сетевого ресурса
VLAN	Virtual Local Area Network — виртуальная локальная сеть
VoIP	Voice over Internet Protocol — телефонная связь, использующая IP
АТС	Автоматическая телефонная станция
СОРМ	Система оперативно-розыскных мероприятий
СПО	Специальное программное обеспечение
ПО	Программное обеспечение
ТА	Телефонный аппарат

2 Общие сведения

2.1 Обозначение и наименование программы

Обозначение – RUS.ПАМР.49300-01 13

Наименование – Специальное программное обеспечение «ПРОТЕЙ-SBC».

Краткое наименование – ПРОТЕЙ-SBC.

2.2 Состав документа

Документ состоит из следующих основных частей:

1. «Термины и сокращения» — раздел, содержащий расшифровку аббревиатур и понятий, используемых в документе.
2. «Общие сведения» — раздел, описывающий назначение и состав документа, содержащий сведения о производителе и технической поддержке.
3. «Назначение и основные свойства» — раздел, описывающий функциональные возможности, виды деятельности и объекты, для автоматизации которых предназначен ПРОТЕЙ-SBC.
4. «Описание системы» — раздел, описывающий структуру ПО и необходимые условия для корректной и стабильной работы.
5. «Взаимосвязи с другими системами» — раздел, описывающий взаимодействие с внешними системами.
6. «Подсистемы» — раздел, описывающий элементы SBC, их функционирование, структуру и назначение.

Внимание!

Перед установкой и началом эксплуатации изделия необходимо внимательно ознакомиться с паспортом изделия и эксплуатационной документацией.

Данный документ должен постоянно находиться при изделии.

2.3 Техническая поддержка

Техническая поддержка, а также дополнительное консультирование по вопросам, возникающим в процессе установки и эксплуатации изделия, осуществляются производителем и службой технической поддержки.

2.3.1 Производитель

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком»

Тел.: (812) 449-47-27

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: sales@protei.ru

2.3.2 Служба технической поддержки

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком»

Тел.: (812) 449-47-27 доб. 5999 (круглосуточно)

(812) 449-47-31

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: mak.support@protei.ru, support.mak@protei.ru

3 Назначение и основные свойства

Пограничный контроллер сессий ПРОТЕЙ-SBC — программное оборудование операторского класса, является одним из ключевых элементов NGN и IMS-сетей.

Назначение пограничных контроллеров сессий:

1. Успешное и безопасное функционирование операторской сети.
2. Стабильное развитие операторского бизнеса.
3. Защита сетей от несанкционированного трафика и специфических типов воздействия.
4. Устранение проблем с совместимостью различных устройств между различными сетями.

ПРОТЕЙ-SBC эффективно решает эти задачи, выполняя функции пограничного контроллера сессий в мультисервисных NGN и IMS-сетях. Помимо этого, маршрутизирует VoIP-трафик между внешними сетями и внутренним защищенным коммутационным ядром.

3.1 Виды деятельности

ПРОТЕЙ-SBC устанавливается на границе сети оператора и является единой точкой входа-выхода в домашнюю сеть. В результате повышается надежность, отказоустойчивость и безопасность, упрощаются конфигурирование и администрирование.

SBC решает ряд задач доступа, коммутации и управления вызовами. Особое значение ПРОТЕЙ-SBC имеет в сетях сервис-провайдеров для управления SIP-трафиком. В этом случае продукт обеспечивает совместную работу разнородного VoIP-оборудования и реализует возможности телефонии, которые отсутствуют у межсетевых экранов и маршрутизаторов.

3.2 Объекты автоматизации, на которых используется ПРОТЕЙ-SBC

SBC применяется для взаимодействия как NGN и IMS-сетей между собой, так и NGN и IMS-сетей с абонентами.

ПРОТЕЙ-SBC не имеет жестких требований к сетевому окружению. Техническое обеспечение взаимодействующих сетей не влияет на возможность использования ПРОТЕЙ-SBC. При этом осуществляется работа с любыми IP-терминалами и устройствами.

3.3 Функциональные возможности (характеристики)

ПРОТЕЙ-SBC выполняет следующие функции:

1. Сокрытие сетевой топологии.
2. Нормализация и трансляция сигнальных протоколов.
3. Нормализация и трансляция медиапротоколов (транскодирование медиаданных из одного кодека в другой).
4. Организация единой точки съема трафика (например, для зеркалирования или СОРМ).
5. Организация единой точки для сбора биллинговой информации.
6. Управление нагрузкой для защиты от атак, сглаживания резких всплесков трафика, защиты внутренней сети от перегрузки.
7. Контроль доступа (CDR, анализ трафика).

3.4 Соответствие международным техническим стандартам

1. RFC3261 “SIP: Session Initiation Protocol”.
2. RFC3262 “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”.
3. RFC3264 “An Offer/Answer Model with Session Description Protocol (SDP)”.
4. RFC2976 “The SIP INFO Method”.
5. RFC2327 “SDP: Session Description Protocol”.
6. RFC2617 “HTTP Authentication: Basic and Digest Access Authentication”.
7. RFC3311 “The Session Initiation Protocol (SIP) UPDATE Method”.
8. RFC5806 “Diversion Indication in SIP”.
9. RFC3324 “Short Term Requirements for Network Asserted Identity”.
10. RFC3326 “The Reason Header Field for the Session Initiation Protocol (SIP)”.

11. RFC3581 “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”.

12. RFC3265 “Session Initiation Protocol (SIP)-Specific Event Notification”.

13. RFC3455 “Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)”.

14. RFC768 “User Datagram Protocol”.

15. RFC1889 “RTP: A Transport Protocol for Real-Time Applications”.

16. RFC1890 “RTP Profile for Audio and Video Conferences with Minimal Control”.

17. RFC2833 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”.

18. RFC3550 “RTP: A Transport Protocol for Real-Time Applications”.

19. RFC3362 “Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration”.

20. RFC4346 “The Transport Layer Security (TLS) Protocol Version 1.1”.

21. RFC3711 “The Secure Real-time Transport Protocol (SRTP)”.

22. RFC3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”.

23. RFC3325 “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”.

24. RFC3966 “The tel URI for Telephone Numbers”.

25. RFC3515 “The Session Initiation Protocol (SIP) Refer Method”.

26. RFC2046 “Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types”.

27. RFC3608 “Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration”.

28. RFC3372 “Session Initiation Protocol for Telephones (SIP-T): Context and Architectures”.

4 Описание системы

4.1 Структура

ПРОТЕЙ-SBC является одним из ключевых элементов IP-сети, поскольку защищает внутреннюю сеть оператора, построенную по архитектуре NGN и IMS.

ПРОТЕЙ-SBC предотвращает потенциальные DoS-атаки на сеть телефонии и соответствующие сервера, выполняя функции, аналогичные SIP прокси-серверам. Пограничный контроллер сессий выступает в роли агентского сервера UAS (User Agent Server) и агентского клиента UAC (User Agent Client), т.е. работает с каждым плечом вызова по отдельности и завершает или инициирует сессии, не используя сторонние инструменты.

ПРОТЕЙ-SBC может создавать списки контроля доступа ACL (Access Control Lists) и анализировать полученные пакеты, чтобы выявлять умышленные искажения информации. Для этого, в частности, предусмотрена проверка заголовков и значений атрибутов SIP-сообщений. Эта проблема актуальна для некоторых протоколов, например, SDP, поскольку у них нет полноценной защиты от перехвата, модификации трафика и т.п.

Помимо сигнальной информации, ПРОТЕЙ-SBC обрабатывает RTP-потоки, обеспечивая шифрование медиатрафика, а также его преобразование из одного кодека в другой. Применяется в случаях, когда стороны не могут согласовать единые параметры SDP. Тем не менее, необходимо учитывать, что транскодирование требует дополнительных затрат аппаратных ресурсов и уменьшает скорость передачи, что критически важно в системах реального времени.

С точки зрения внутренней архитектуры, функциональность ПРОТЕЙ-SBC можно разбить на два логических элемента:

1. I-SBC обеспечивает безопасную работу между сетями операторов, выполняет функции IBCF, TrGW (IBGF), IMS-ALG/IMS-AGW в IMS-архитектуре.

2. A-SBC обеспечивает безопасную работу между сетью оператора и конечными пользователями, выполняет функции P-CSCF, I-CSCF, IMS-ALG/IMS-AGW в IMS-архитектуре.

4.2 Требования к аппаратно-программному обеспечению

Для функционирования ПРОТЕЙ-SBC требуется сервер, на который устанавливаются программные модули ПРОТЕЙ-SBC.

Необходимые системные требования для развертывания стенда:

1. Процессор — не менее 6 ядер с тактовой частотой не менее 2,4 ГГц.
2. Оперативная память — не менее 8 Гб.
3. Свободное место на жестком диске — не менее 600 Гб.

Программное обеспечение сервера реализовано на базе ядра Linux.

Для доступа к подсистеме технического обслуживания пользователю потребуется персональный компьютер со следующим программным обеспечением:

1. Операционная система — Debian, Windows или RPM-система на базе ядра Linux.
2. Браузер — Firefox, Google Chrome, Safari, Opera последней версии.

4.3 Возможности программного обеспечения

Установка программного обеспечения ПРОТЕЙ-SBC предоставляет доступ к следующим возможностям:

1. Поддержка 5000 одновременных соединений.
2. Количество попыток вызовов в секунду — 500 cps.
3. Поддерживаемый режим работы — полнодуплексный (full-duplex).
4. Поддержка физических интерфейсов и VLAN.

4.4 Алгоритм установления соединения и вызова

На рисунке 1 показаны процессы установления соединения, осуществления вызова и дальнейшего завершения сессии.

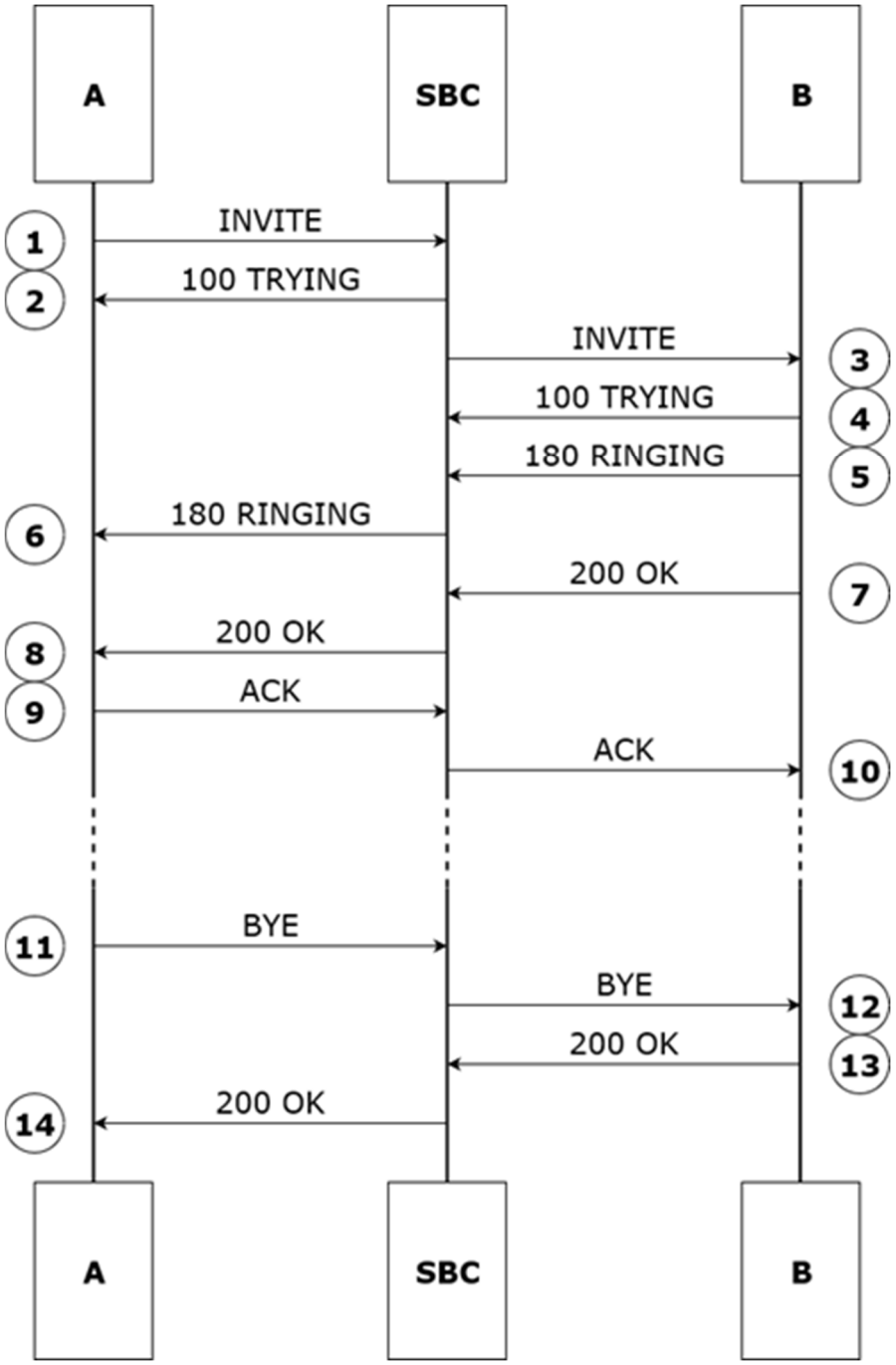

Рисунок 1 — Схема вызова с использованием SBC

На представленной схеме абонент А намерен совершить вызов абоненту В.

SBC расположен между абонентами, в связи с чем принимает и транслирует все SIP-сообщения. Пограничный контроллер сессий проверяет, верно ли выполняются указанные ниже шаги, и соответствуют ли установленному алгоритму текущие действия абонентов.

1. Абонент А посылает запрос INVITE вместе со своими данными для установления SIP-соединения.

2. SBC получает запрос INVITE для абонента В. SBC посылает абоненту А сообщение 100 TRYING, подтверждая получение запроса.

3. SBC транслирует запрос INVITE абоненту В.

4. При успешной доставке запроса INVITE абонент В подтверждает получение и отвечает абоненту А сообщением 100 TRYING.

5. Вместе с приглашением абонент В также принимает сообщение о попытке вызова. Абонент В сообщает абоненту А о необходимости активировать контроль посылки вызова с помощью запроса 180 RINGING.

6. SBC принимает ответы абонента В и передает абоненту А запрос 180 RINGING.

7. Как только абонент В соглашается принять вызов, например, подняв трубку телефонного аппарата, абоненту А направляется уведомление 200 OK в ответ на INVITE.

8. SBC получает согласие абонента В и передает абоненту А сообщение 200 OK в ответ на INVITE.

9. Абонент А подтверждает получение сообщений от абонента В и отвечает сообщением ACK.

10. SBC принимает от абонента А сообщение ACK и передает абоненту В.

Начиная с этого момента, обе стороны подтвердили свое согласие, и осуществляется переход в фазу разговора. В случае, указанном на схеме выше, абонент А заканчивает разговор, например, положив трубку телефонного аппарата в исходное положение.

11. Поскольку именно абонент А завершает звонок, по окончании вызова сообщение BYE направляется абоненту В. Это сообщение, как правило, идет напрямую другой стороне, минуя все прокси.

12. SBC получает от абонента А сообщение BYE и передает абоненту В.

13. Абонент B принимает сообщение и посылает ответ абоненту A в виде уведомления 200 OK в ответ на BYE.

14. SBC получает от абонента B уведомление 200 OK в ответ на BYE и передает абоненту A.

В этот момент сессия полностью завершается.

5 Взаимосвязи с другими системами

5.1 Общая информация

Оборудование ПРОТЕЙ-SBC является одним из ключевых элементов NGN, не предоставляя непосредственно услуги, но обеспечивая надежную работу сети.

ПРОТЕЙ-SBC успешно взаимодействует с сетевыми устройствами:

1. Все IP-терминалы.
2. Гибкие коммутаторы (softswitch).
3. Межсетевые экраны (firewall).
4. Устройства преобразования сетевых адресов (NAT).

При наличии сложностей с каким-либо упомянутым выше оборудованием можно обратиться к линейке продуктов NGN, разработанных ООО «НТЦ Протей».

ПРОТЕЙ-SBC может контролировать качество и полосу пропускания для передаваемого трафика. однако его возможности маршрутизации трафика ограничены. В связи этим задачами по управлению обслуживания вызовов и взаимодействием с базами данных и серверами прикладного уровня занимается гибкий коммутатор, а обработкой трафика и сигнальных сообщений — ПРОТЕЙ-SBC.

NAT используется в сетевых коммуникациях, чтобы задать группе устройств в локальной сети единый IP-адрес. Маршрутизатор использует этот адрес во всех взаимодействиях с внешними системами. Все сетевые средства способны определить лишь общий адрес, поскольку NAT скрывает всю локальную сеть, в которой находится. Для возможности передавать информацию только конкретным устройствам составляются так называемые «таблицы NAT». В них отражено однозначное соответствие между глобальным IP-адресом и персональными для каждого устройства. ПРОТЕЙ-SBC способен выполнять схожие функции для обслуживаемых соединений.

Межсетевой экран — оборудование и/или программное обеспечение для контроля входящего и исходящего трафика сети или соединения. Выступая в роли заграждения, устанавливает сетевые фильтры и отслеживает все потоки данных. С помощью фильтров определяются правила, по которым трафик блокируется или пропускается и

проходит дальше. ПРОТЕЙ-SBC взаимодействует с межсетевым экраном и регулирует действующие правила.

Пограничный контроллер сессий поддерживает широкий спектр кодеков для голосовой связи и осуществляет транскодирование между узкополосными/широкополосными голосовыми кодеками, нормализуя SDP в SIP-сообщениях. ПРОТЕЙ-SBC обеспечивает совместимость с ведущими решениями unified-communication и провайдерами SIP-каналов.

Элементы ПРОТЕЙ-SBC позволяют четко разграничить функциональность, зоны безопасности и ответственности.

На рисунке 2 показаны взаимосвязи элементов ПРОТЕЙ-SBC с другими системами.

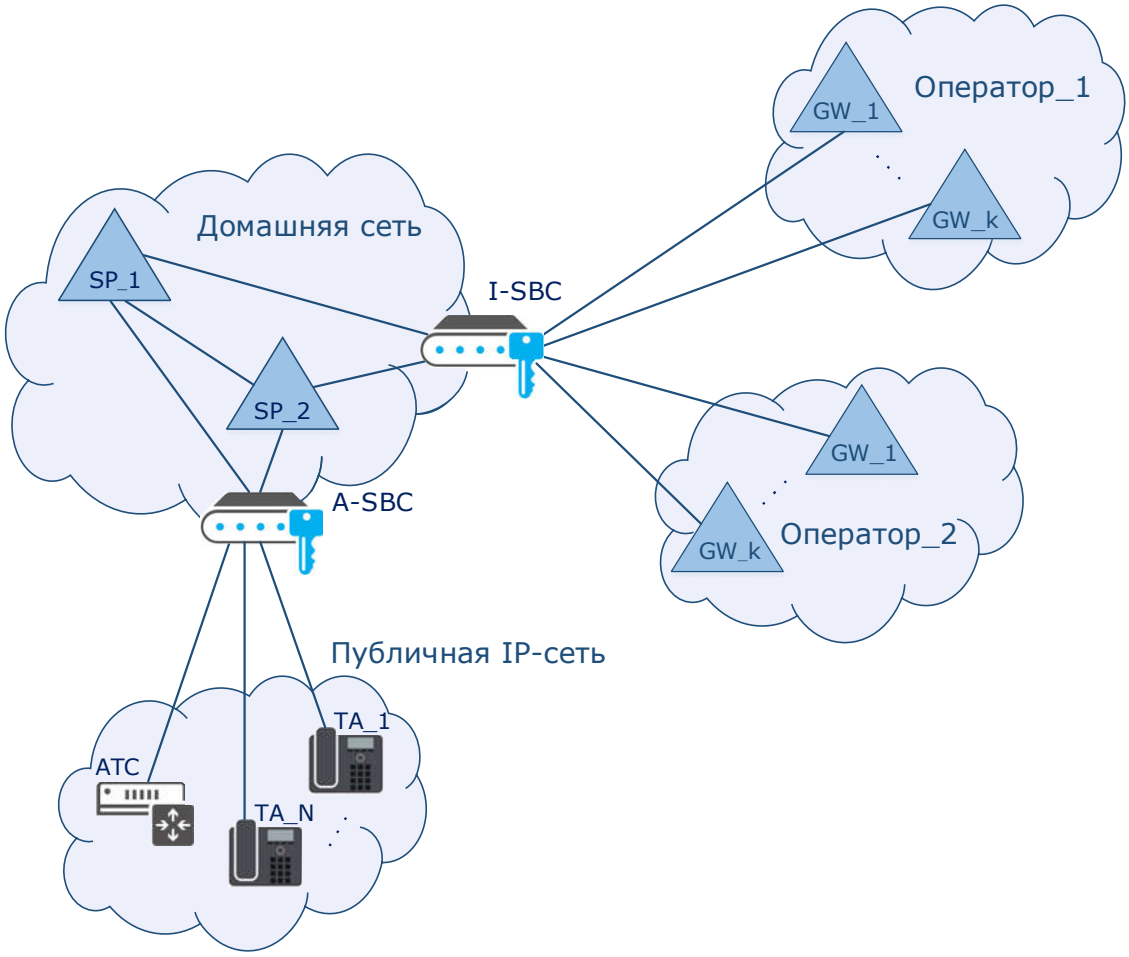

Рисунок 2 — Взаимосвязи элементов SBC с внешними системами

Схема включения SBC аналогична включению межсетевого экрана — в разрыв между внешней сетью и защищаемыми ресурсами.

Устройства ПРОТЕЙ-SBC подключаются с помощью стандартных интерфейсов Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet. Выбор того или иного варианта зависит от предполагаемой нагрузки: количество одновременных сессий, объем трафика и т.д.; от выполняемых задач: контроль версий и протоколов сигнализаций, необходимость простой передачи медиатрафика или транскодирования и т.д.

5.2 Взаимодействие с CDR Viewer

CDR Viewer — программное обеспечение, с помощью которого пользователь может запросить, загрузить и отобразить журналы CDR и статистики по вызовам. Более подробная информация указана в документе «CDR Viewer. Руководство пользователя Web-интерфейса».

CDR Viewer позволяет автоматизировать следующие операции:

1. Запросить, загрузить и отобразить в окне браузера журналы CDR согласно введенным параметрам.
2. Запросить и отобразить в окне браузера статистики вызовов согласно введенным параметрам.
3. Экспортировать CDR и статистики вызовов в форматы csv, pdf, xls.
4. Создать шаблоны для отчетов журналов CDR.
5. Сформировать отчеты журналов CDR и отобразить их в окне браузера.
6. Настроить отчеты журналов CDR для дальнейшей рассылки на указанные адреса электронной почты.

При просмотре деталей вызовов данное программное обеспечение отображает множество информации о вызове и участниках:

1. Параметры вызова и разговора: дата, время, длительность вызова, длительность разговора и т.д.
2. Сетевые данные каждой стороны: Call-ID, номера сторон в плечах вызова и т.д.

3. Сетевые характеристики вызова: ID вызова, количество отправленных, полученных, потерянных пакетов и т.д.

4. Данные для определения причины отбоя в случае разрыва соединения: SIP-сообщение, причины перемаршрутизации и т.д.

На рисунках 3, 4, 5 и 6 показаны примеры конфигурирования, администрирования и просмотра CDR-файлов с помощью CDR Viewer.

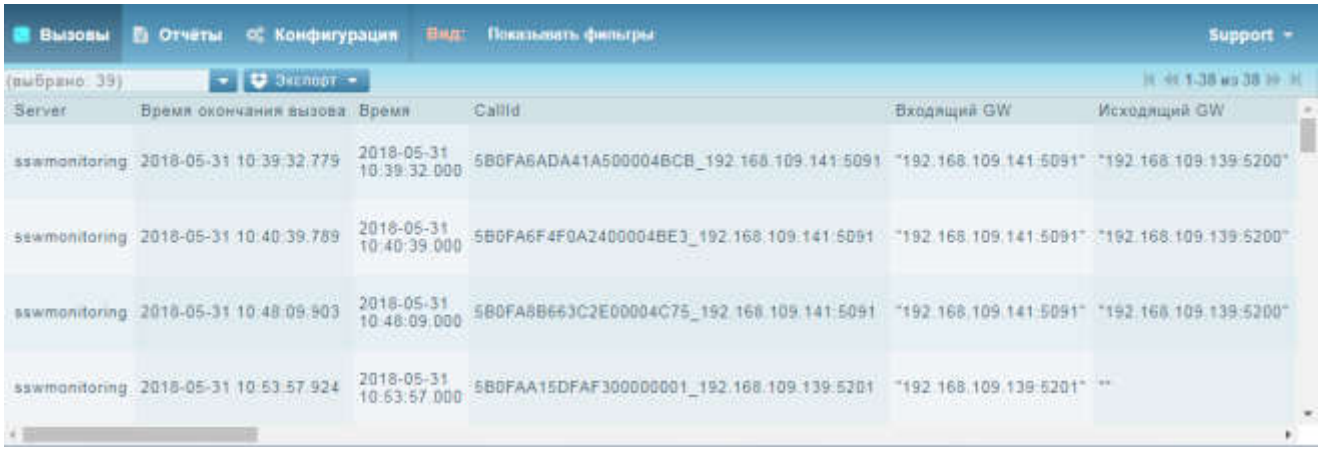

Рисунок 3 — Работа с CDR-файлом

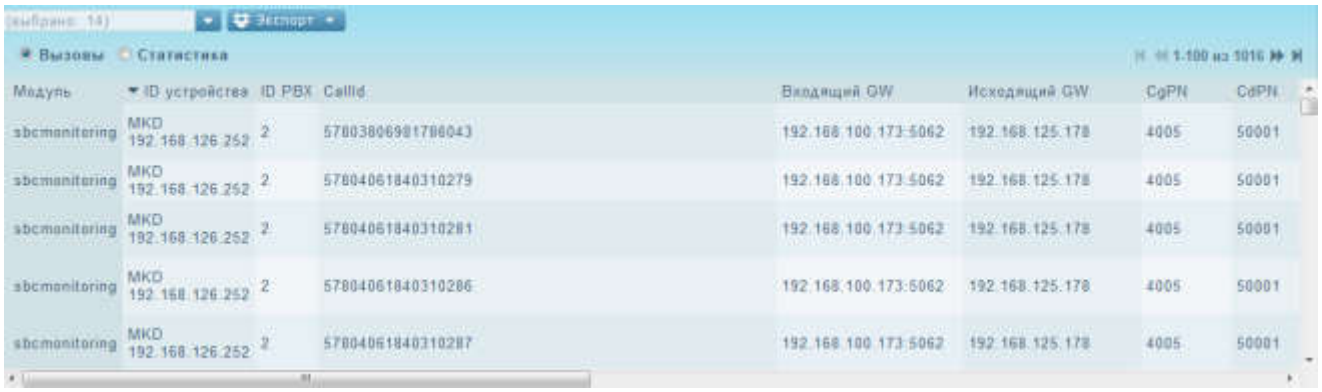

Рисунок 4 — Работа с CDR-файлом

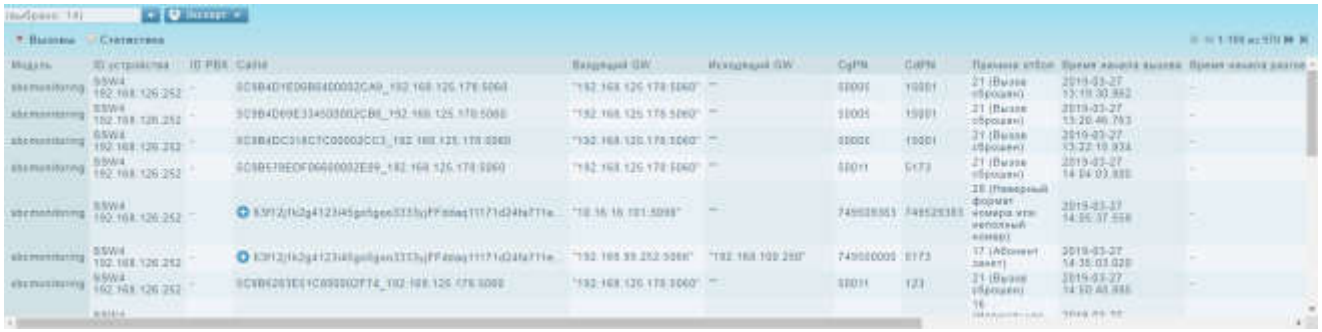

Рисунок 5 — Работа с CDR-файлом

Изм.	Лист	№ докум.	Подпись	Дата

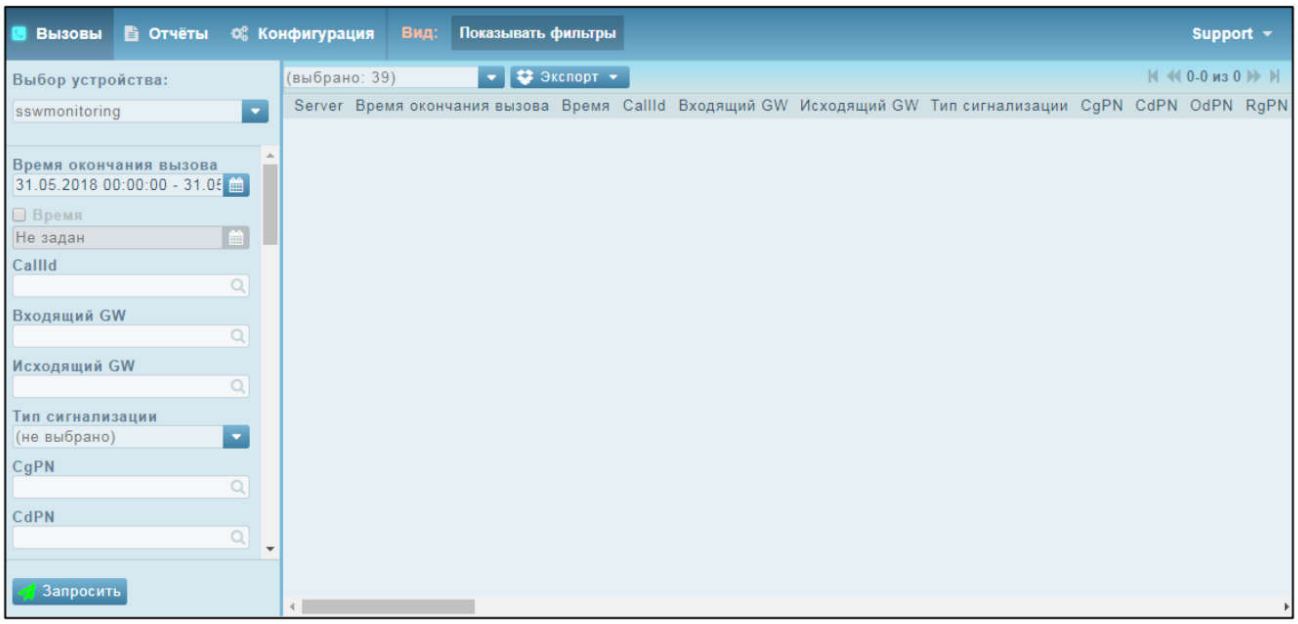

Рисунок 6 — Работа с CDR-файлом

5.3 Взаимодействие с Grafana

В комплекте с ПРОТЕЙ-SBC может поставляться также и Grafana, программный комплекс для сетевого управления, мониторинга и оповещения при аварийных ситуациях.

Это программное обеспечение позволяет:

1. Представить большой объем информации в удобном графическом виде.
2. Обрабатывать метрики.
3. Получать уведомления в случае аварийных ситуаций.
4. Записывать и анализировать логи журналов.
5. Объединить большое количество разнородных данных в одном месте с помощью панелей.

На рисунках 7, 8 и 9 показаны примеры использования Grafana для вывода информации о текущей нагрузке на сеть оператора, к которой подключен I-SBC.

Рисунок 7 — Пример использования Grafana

Рисунок 8 — Пример использования Grafana

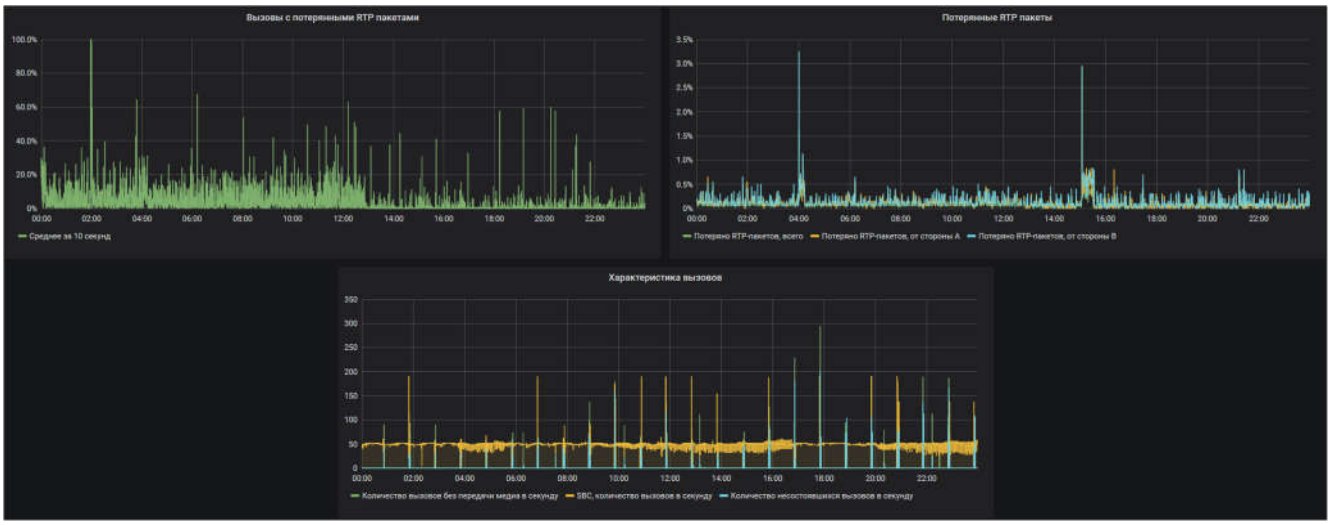

Рисунок 9 — Пример использования Grafana

Изм.	Лист	№ докум.	Подпись	Дата

6 Подсистемы

6.1 I-SBC

Как было указано выше, I-SBC устанавливается на границе сети оператора и обеспечивает взаимодействие VoIP-оборудования домашней сети с внешними системами. Домашняя сеть оператора представлена определенным набором сервисных платформ, обрабатывающих сигналы SIP и медиапотоки. В рамках конфигурации I-SBC устанавливается однозначное соответствие между конкретной сервисной платформой и оператором. С помощью I-SBC создаются соединения с медиашлюзами операторов.

Подробное описание примера настройки ПРОТЕЙ-SBC приведено в документе «Пограничный контроллер сессий. Руководство пользователя».

На рисунке 10 показана условная сеть связи с установленным I-SBC.

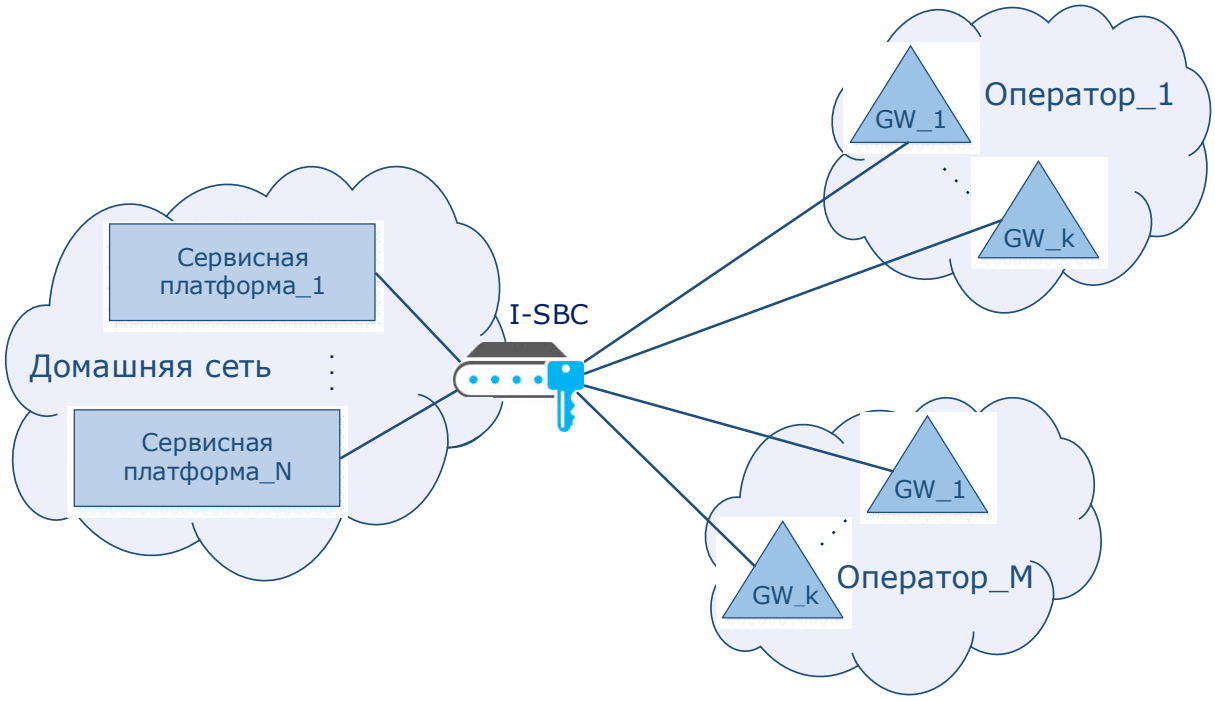

Рисунок 10 — Условная схема сети с участием I-SBC

Для информационного взаимодействия I-SBC поддерживает следующие протоколы:

1. SIP — протокол для сигнализации VoIP.

SIP используется для обеспечения взаимодействия между двумя программными коммутаторами.

2. RTP/RTCP — протокол для пакетной передачи аудио-потока.

Для корректного взаимодействия I-SBC с внешними сетями и защищаемыми ресурсами поддерживаются дополнительные протоколы сигнализации: UDP, RTP/RTCP, RSTP, SSH, SNMP, NTP. Для шифрования сигнализации поддерживаются протоколы SRTP и TLS.

При взаимодействии с сетью оператора реализуются следующие возможности I-SBC:

1. Поддержка виртуальных интерфейсов.
2. Поддержка VLAN и IPv4.
3. Маркировка QoS по направлениям (ToS/Diffserv).
4. Поддержка технологии IntelDPDK для виртуальных решений.
5. Определение доступных SIP-транков.
6. Преобразование метода PRACK.
7. Маршрутизация вызовов с использованием Proxy FlexibleDirection, заключается в преобразовании пользовательской информации (userinfo) из Request-URI в hostport получателя.
8. Поддержка режима Delayed Offer.

6.1.1 Функциональные характеристики

Включение I-SBC на границе сетей операторов позволяет реализовать следующие функции:

1. Трансляция сигнальных сообщений и медиаданных между интерфейсами.
2. Транскодирование медиаданных из одного кодека в другой: G.711 A/μ-Law, G.722, G.722.2 (AMR-WB), G.723.1, G.729 A.
3. Анализ качества медиаканалов, по которым осуществляется маршрутизация голосового трафика: задержка, джиттер, процент потерь пакетов и пр.
4. Автоматическая блокировка вызовов от неизвестных источников.

5. Обеспечение качества обслуживания (QoS).

6. Модификация атрибутов сигнальных сообщений.

7. Ограничение полосы пропускания для защиты от DoS-атак.

8. Сокрытие сетевой топологии с помощью трансляции IP-адресов и портов (NAPT).

9. Создание альтернативных маршрутов и балансировка нагрузки.

10. Лицензирование количества одновременных сессий, попыток соединений в секунду и сеансов с транскодированием.

11. Контроль статического и динамического доступа.

12. API для проверки маршрутизации, интерфейс для отображения/принудительного разрушения установленных соединений.

13. Контроль за установленными соединениями с помощью внутренних инструментов.

14. Формирование журналов трассировки.

15. Формирование RTCP-статистики по направлениям.

16. Формирование CDR-журналов с возможностью передачи по протоколам FTP/SFTP/SCP и мониторинг по протоколу SNMP.

17. Анализ вызовов, запись переговоров в *cap формате и формирование отчетов.

6.1.2 Описание структуры и работы I-SBC

В рамках продукта I-SBC применяются следующие основные сущности и понятия:

1. Сервисная платформа — оборудование внутренней сети оператора, взаимодействующее с сетями внешних операторов через пограничный контроллер сессий.

2. Маршрутизация описывает взаимодействие сервисной платформы и внешнего оператора.

3. Маршрут описывает используемое оборудование внешнего оператора.

4. MCU задает и контролирует взаимодействия с медиапотоками.

5. Медиапрофиль — набор списков разрешенных, запрещенных, обязательных и поддерживаемых кодеков.

Медиапрофиль применим как к сервисной платформе, так и к оператору и/или маршруту оператора. По умолчанию для всех операторов и сервисных платформ используется нулевой медиапрофиль, в котором нет ограничений. Данный профиль изменять не рекомендуется.

Шлюз — именованная пара <ip:port>, однозначно определяющая точки входа и выхода в домашнюю сеть оператора.

На рисунке 11 показано установление соединения между сервисной платформой и внешним оператором через I-SBC.

Рисунок 11 — Структурная схема I-SBC

Конкретный маршрут устанавливает однозначное соответствие между SIP-транком на оператора (ExtLocalGate ↔ ExtGate) и обслуживающей платформой. Все вызовы, пришедшие на IntLocalGate, направляются во внешнюю сеть оператора с ExtLocalGate на ExtGate. При этом вызовы в/из внутренней сети оператора имеют ограничения по количеству попыток вызовов в секунду и одновременному их количеству. Доступность шлюзов оператора для входящих вызовов определяется с

помощью SIP-запросов OPTIONS. Маршрутизация вызовов определяется набором маршрутов, заданных в конфигурации I-SBC.

Медиашлюз конкретного оператора содержит список подсетей, конкретных адресов и портов медиашлюзов оператора, с которых разрешено принимать медиатрафик. Если источник медиатрафика не указан в настройках медиа шлюза как разрешенный, то сервисная платформа отбросит все такие RTP-пакеты.

Сервисная платформа описывает конфигурацию внутренней сети (или ее конкретного сегмента) и содержит набор шлюзов для сигнализации, определяемых приоритетами и весами.

MCU определяет настройки профилей для приема и отправки медиатрафика от/к оператору, позволяет управлять медиаресурсами и распределять их, указывая количество одновременных аудио- и видеосессий.

6.1.3 Резервирование I-SBC

В I-SBC применяется резервирование SBC.Core, чтобы исключить выход I-SBC из строя и простоя при неполадках с основным I-SBC.

SBC.Core — ядро I-SBC, выполняющее следующие функции:

1. Обработка сигнальных сообщений.
2. Взаимодействие и преобразование протоколов.
3. Идентификация вызывающей стороны.
4. Сокрытие внутренней сетевой топологии.
5. Разрешение или запрет вызовов, основываясь на количестве доступных ресурсов.
6. Обработка медиапотоков.

На рисунке 12 показан основной вариант резервирования.

Для резервирования SBC.Core используется хранилище объектов In-Memory Data Grid. В этом хранилище в виде ключей и значений находятся текущие данные по трафику, который обрабатывается в SBC.Core. В качестве хранилища объектов используется облачный кластер Hazelcast. Основной режим работы резервирования —

Active/StandBy. Весь трафик передается через основной SBC.Core, при этом резервный SBC.Core находится в режиме ожидания.

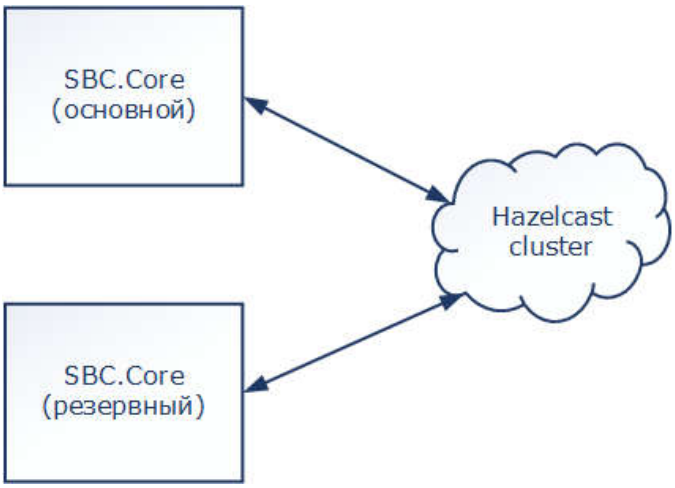

Рисунок 12 — Основная схема резервирования

Если основной SBC.Core выходит из строя, то через кластер Hazelcast текущую нагрузку принимает резервный SBC.Core, который начинает обрабатывать трафик и выполняет все функции основного I-SBC.

Модульная структура SBC обеспечивает высокую надежность и предусматривает экономически выгодное масштабирование системы по мере увеличения количества абонентов и нужд операторов.

6.1.4 Алгоритм внутренней маршрутизации

В общем случае алгоритм можно разбить на 3 фазы (Рисунок 13):

1. Определение источника вызова.

I-SBC анализирует принимаемые сообщения. Из входящего SIP-запроса INVITE заполняет контекст вызова всей доступной информацией, определяет источник вызова (абонента A) и проверяет ограничения для этого источника вызова.

2. Маршрутизация.

I-SBC модифицирует контекст вызова, определяет компоненты принимающей стороны (абонент B), а затем осуществляет маршрутизацию вызова. Для дальнейшей работы I-SBC сохраняет данные об абоненте B в контекст вызова.

3. Определение получателя вызова.

Для корректного завершения маршрутизации проверяются данные принимающей стороны (абонента B) и вносятся в контекст вызова.

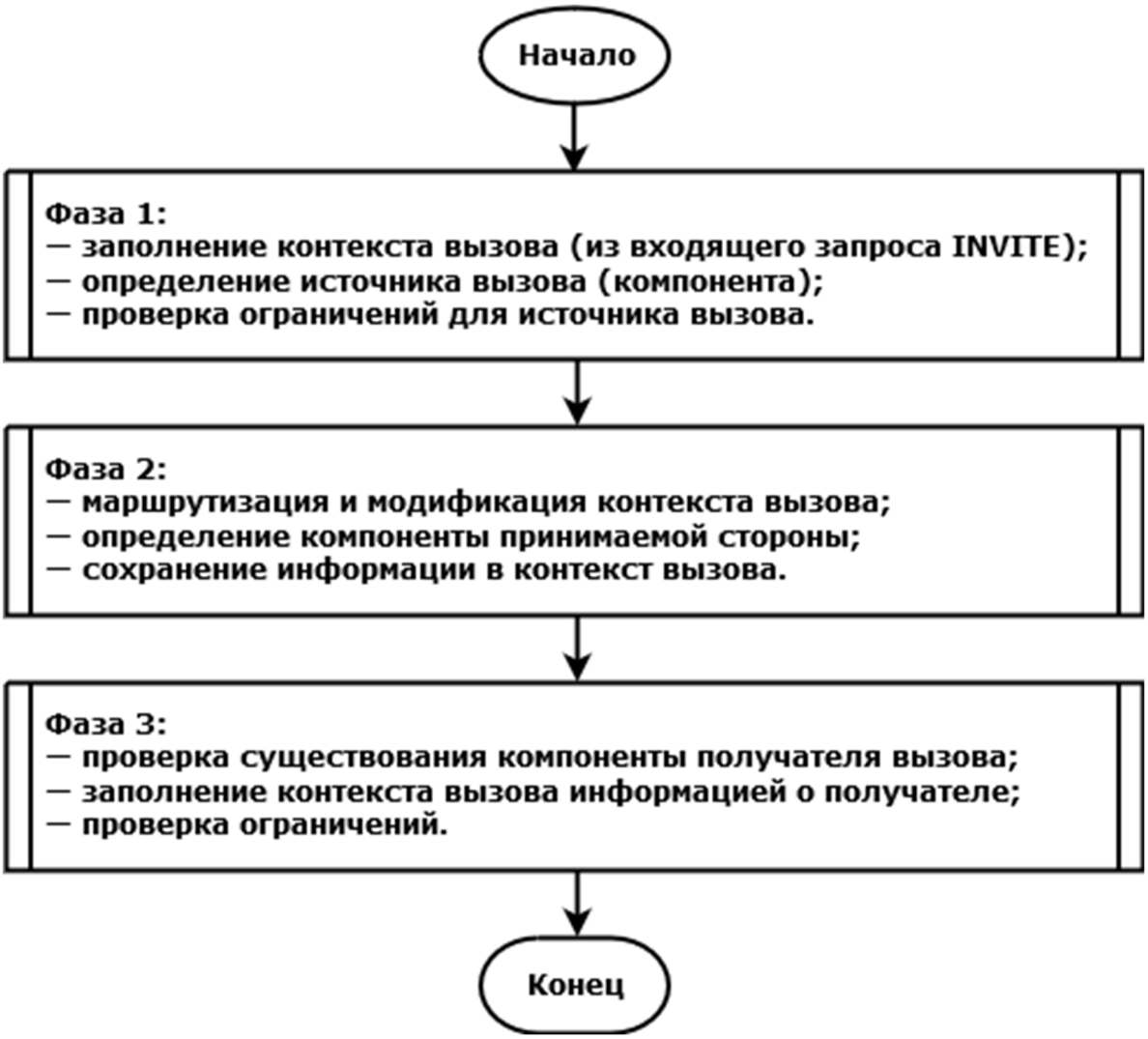

Рисунок 13 — Фазы маршрутизации

6.1.5 Перемаршрутизация

Алгоритм перемаршрутизации используется в случаях, если при попытке совершить вызов поступает сообщение, принудительно завершающее соединение.

Процесс проходит в несколько этапов. В начале SBC определяет характер отбоя от второй стороны, а затем проверяет выполнение всех условий для перемаршрутизации источника вызова.

Далее, если были использованы не все попытки перемаршрутизации, то в системном сообщении ищется код Q.850, указывающий причину разъединения. Если

причина установлена, и при ее возникновении предусмотрено перенаправление, то выполнение алгоритма продолжается. Если причина не определена, то для ее идентификации будут использованы внутренние таблицы соответствий между SIP-сообщениями и кодами ошибки Q.850.

Если вызов направлялся сервисной платформе, то начинается поиск шлюза сервисной платформы, который еще не задействовался в текущей сессии. Если таковые есть, то среди них по правилам маршрутизации выбирается один, на который отправляется вызов.

Если свободных не нашлось или изначально вызов предназначался не сервисной платформе, то после этого проводится анализ правил маршрутизации. В ситуации, когда правила заданы, не перенаправляют друг на друга, а указанные дальше еще не использовались, то выполняется следующее указанное правило перемаршрутизации. Таким образом, осуществляется еще одна попытка маршрутизации.

В случаях, когда не выполнено хотя бы какое-нибудь из вышеперечисленных условий, т.е. ни один из сценариев не подходит для сложившейся ситуации, то вызов отбивается, и выводится информация об этом вызове.

6.2 A-SBC

Как было указано выше в описании SBC, A-SBC устанавливается на границе сети оператора и обеспечивает безопасное взаимодействие между сетью оператора и конечными пользователями.

На рисунке 14 приведена условная сеть связи с установленным A-SBC.

Для информационного взаимодействия A-SBC поддерживает следующие протоколы:

1. SIP — протокол для сигнализации VoIP.

SIP используется для взаимодействия между программным коммутатором и абонентским терминалом.

2. RTP/RTCP — протокол для пакетной передачи аудиопотока.

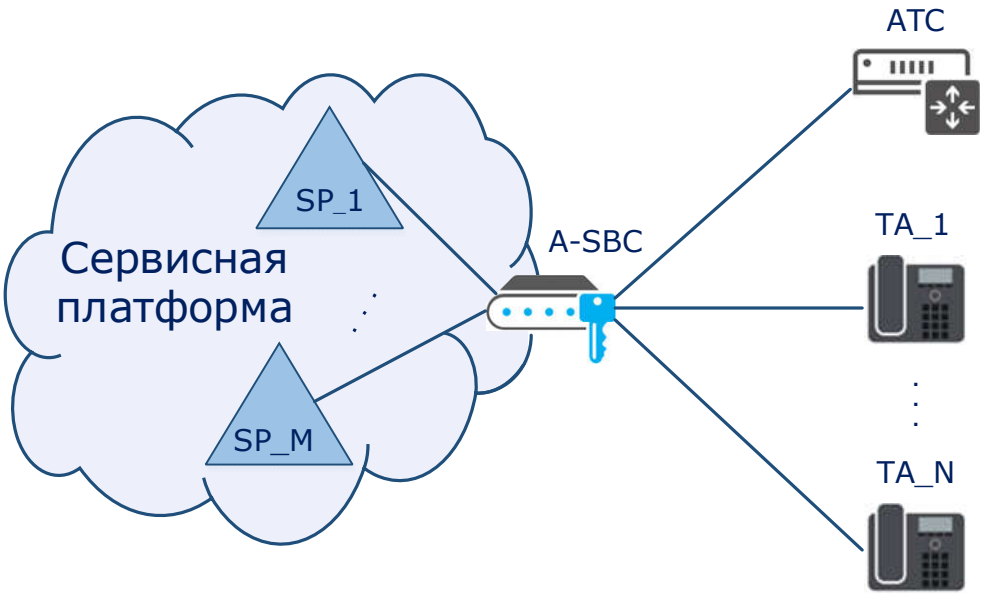

Рисунок 14 — Условная схема построения сети связи с участием A-SBC

Для корректного взаимодействия A-SBC с внешними сетями и защищаемыми ресурсами поддерживаются дополнительные протоколы сигнализации: UDP, RTP/RTCP, RSTP, SSH, SNMP, NTP, HTTP API. Для шифрования сигнализации поддерживаются протоколы SRTP и TLS.

При взаимодействии с оконечными пользователями реализуются следующие возможности A-SBC:

1. Поддержка виртуальных интерфейсов.
2. Поддержка VLAN и IPv4.
3. Маркировка QoS по направлениям (ToS/Diffserv).
4. Поддержка технологии Intel DPDK для виртуальных решений.
5. Определение доступных SIP-транков.
6. Возможность восстановления активных вызовов/регистраций при сбоях/плановых переключениях.
7. Поддержка режима Delayed Offer.

6.2.1 Функциональные характеристики

Включение A-SBC на границе сети оператора позволяет реализовать следующие функции:

1. Трансляцию сигнальных сообщений и медиаданных между интерфейсами.

2. Транскодирование медиаданных из одного кодека в другой: G.711 A/μ-Law, G.722, G.722.2 (AMR-WB), G.723.1, G.729 A.

3. Модификация атрибутов сигнальных сообщений.

4. Сокрытие сетевой топологии.

5. Создание альтернативных маршрутов и балансировка нагрузки.

6. Автоматическое блокирование вызовов от неизвестных источников.

7. Ограничение интенсивности сигнальной нагрузки и максимальной длительности вызовов.

8. Задание пороговых значений для количества одновременных сессий и ширины полосы для медиапотока по каждому направлению.

9. Обнаружение мошеннических SIP-запросов INVITE и RTP-пакетов.

10. Обеспечение единой точки подключения абонентов.

11. Контроль таймеров для медиатрафика.

12. Лицензирование количества одновременных сессий, попыток соединений в секунду и количества сеансов с транскодированием.

13. Контроль статического и динамического доступа.

14. Контроль установленных соединений с помощью внутренних инструментов.

15. Формирование журналов трассировки.

16. Обеспечение сквозного тракта VoIP.

17. Прохождение через NAT-устройства и межсетевые экраны.

18. Стыкование VPN.

19. Биллинг и т.д.

6.2.2 Описание структуры и работы A-SBC

В рамках продукта A-SBC можно выделить следующие основные сущности и понятия:

1. Сервисная платформа — оборудование внутренней сети оператора, взаимодействующее с абонентами через пограничный контроллер сессий.

2. Маршрутизация описывает взаимодействие сервисной платформы и абонента.

3. MCU задает и контролирует взаимодействия с медиапотоками.

4. Медиапрофиль — набор списков разрешенных, запрещенных, обязательных и поддерживаемых кодеков.

Медиапрофиль применим как к сервисной платформе, так и к абоненту и/или маршруту абонента. По умолчанию для всех абонентов и сервисных платформ используется нулевой медиапрофиль, в котором нет ограничений. Данный профиль изменять не рекомендуется.

Шлюз — именованная пара <ip:port>, однозначно определяющая точки входа и выхода в домашнюю сеть оператора.

На рисунке 15 показано установление соединения между сервисной платформой и конечным пользователем через A-SBC.

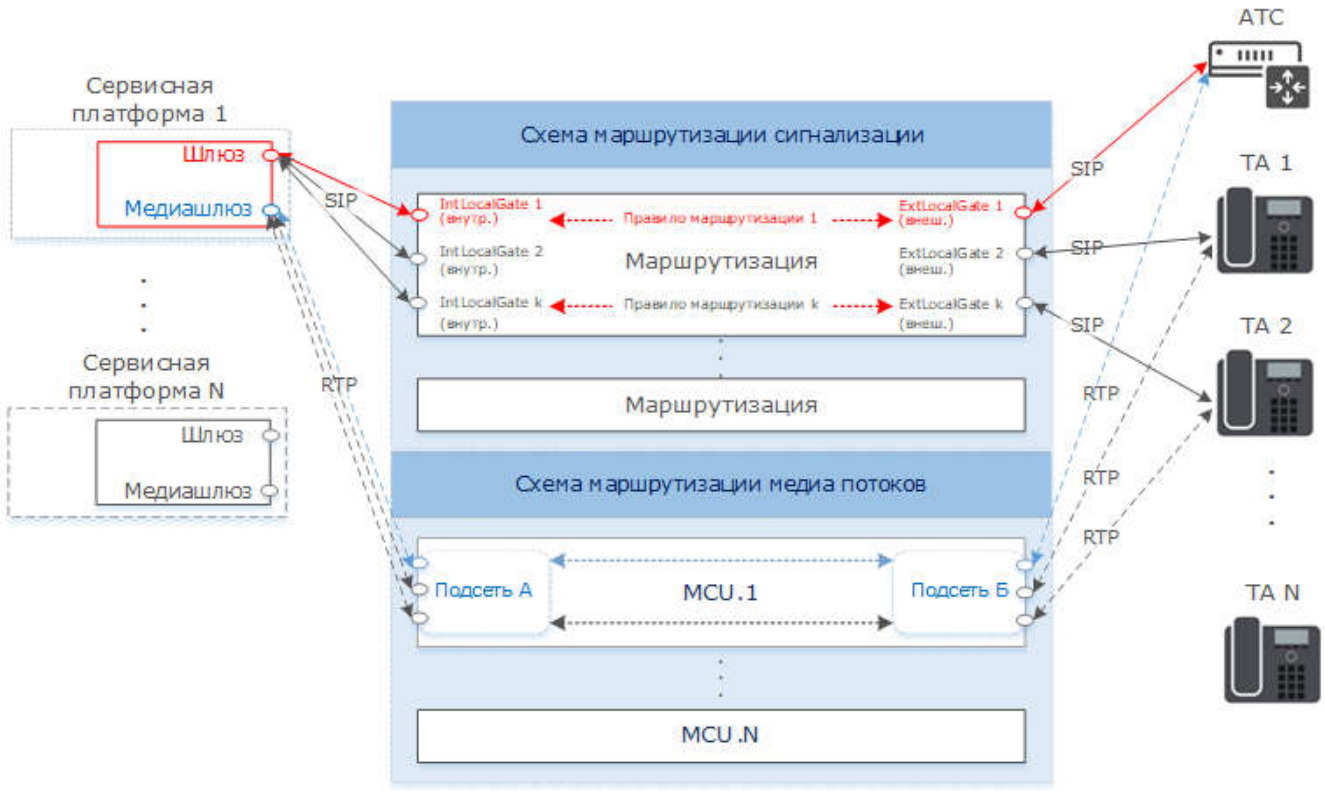

Рисунок 15 — Структурная схема A-SBC

Конкретный маршрут устанавливает однозначное соответствие между SIP-транком на конечного пользователя (ExtLocalGate ↔ TA) и сервисной платформой. Все

вызовы, пришедшие на IntLocalGate, отправляются во внешнюю публичную сеть с ExtLocalGate на оборудование конечного пользователя (IP-телефон абонента, АТС и прочее). При этом вызовы в/из внутренней сети оператора ограничены по количеству попыток вызовов в секунду, а также одновременному их количеству. Доступность шлюзов оператора для вызовов на оборудование конечного пользователя определяется с помощью SIP-запросов OPTIONS.

MCU определяет настройки профилей для приема и отправки медиатрафика от/к оператору, позволяет управлять медиаресурсами и распределять их, указывая количество одновременных аудио- и видеосессий.

6.2.3 Резервирование A-SBC

Схема резервирования A-SBC аналогична схеме резервирования I-SBC, описанной в пункте 6.1.3 «Резервирование I-SBC».

6.2.4 Алгоритм маршрутизации вызова

На рисунке 16 показан алгоритм маршрутизации вызова, подписки на событие или регистрации абонента.

В исходном состоянии при поступлении вызова, регистрации абонента или подписки на событие A-SBC определяет направление.

Если запрос поступил от абонента (абонент A), то пограничный контроллер сессий начинает поиск группы абонентов (UserProfile), к которой относится абонент A. После этого определяется оптимальный маршрут.

Если запрос поступил к абоненту (абонент B), то пограничный контроллер сессий начинает поиск и определение сервисной платформы. После этого запрос отправляется во внутреннюю сеть оператора на конкретную сервисную платформу. Далее A-SBC определяет получателя вызова или профиль пользователя для соединения, а также группу абонентов (UserProfile), к которой относится данный абонент.

Чтобы маршрутизация вызова была корректной, проверяются ограничения для данного конечного пользователя: определяется номер, тип сообщения и т.д.

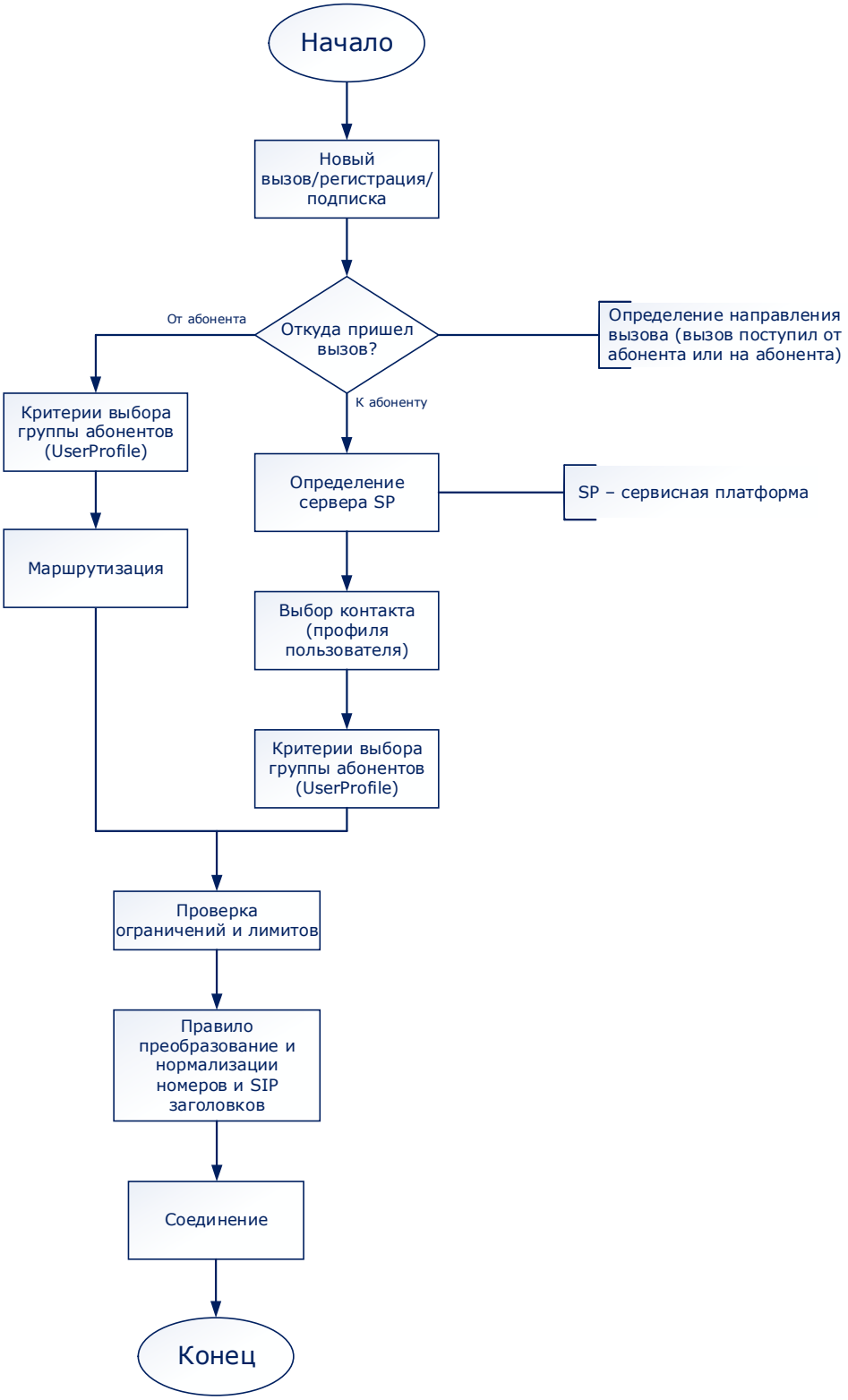

Рисунок 16 — Маршрутизация нового вызова/подписки/регистрации

Затем выполняется преобразование и нормализация номеров и заголовков в SIP-сообщениях (изменения атрибутов «from», «via», «contact», «call-ID» и т.д.)

Примечание: в режиме работы сквозных медиапотоков меняются заголовки RTP.

A-SBC обеспечивает VoIP-соединение между абонентами, подписку на событие или регистрацию абонента.

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в док.	№ документа	Входящий № сопроводительного докум. И дата	Подпись	Дата
	Замененных	Измененных	Новых	Аннулированных					

Изм.	Лист	№ докум.	Подпись	Дата