**Общая информация**

Протокол сигнализации: sip

Передача DTMF, формат: RFC2833

Предпочтительные кодеки: g711a,g711u

Адрес сервера (домен) персональный для каждой ВАТС. Посмотреть можно в ЛК.

**Типовые настройки систем ограничения доступа (Firewall, брандмауэры и тому подобное)**

Для работы услуги необходимо открыть доступ на фаерволе/роутере/брандмауэре и т.д., осуществив следующие действия:
• разрешить входящие соединения и исходящий трафик по протоколу UDP для прохождения сигнальных SIP сообщений для адресов:
  91.143.36.250, 212.34.47.196, 212.34.47.197  порты с 1024 по 65535.

**Безопасность**

**В последнее время участились атаки на VoIP-оборудование. Данный материал должен помочь обезопасить от взлома ваше оборудование.**

**Общие правила по безопасности:**

**1. Никогда не используйте стандартные авторизационные данные например, логин: admin, пароль: admin;**

**2. Никогда не используйте легкие пароли: qwerty, rfvtgb, edcbhu, p@ssw0rd, ....;**

**3. По возможности не используйте стандартные порты SSH: 22, http: 80 (8080), telnet: 23, sip: 5060. Все сканнеры в первую очередь сканируют стандартные порты;**

**4. Работать с SIP телефонами по возможности только за NAT (подключайте SIP оборудование к маршрутизатору (router);**

**5. Не настраивайте на маршрутизаторе и точек доступа опцию DMZ;**

**6. Не пользоваться сомнительными Софтфонами;**

**7. Настоятельно рекомендуем настраивать опцию в Личном кабинете "Разрешить доступ по протоколу SIP только с указанных адресов" Пример и Разрешенных направлений вызовов в Личном кабинете, Пример;**

**8. Рекомендуем обновлять SIP-оборудование на последние ПО, Пример;**

**9. Использовать антивирусы на компьютерах, где установлены программные телефоны;**

**10. Рекомендуем настроить проброс не со всего интернета, а только с адресов провайдера**

**Требования к Интернет-каналу**

Только при соблюдении нижеперечисленных показателей качества интернет соединения, мы можем гарантировать качественную работу сервиса передачи голоса.

1. ПОЛОСА ПРОПУСКАНИЯ.

Ваш канал доступа в Интернет должен быть рассчитан исходя из того, что один разговор требует минимальную полосу пропускания 100 кбит/с

2. ПОТЕРЯ ПАКЕТОВ.

Максимальный процент потерь не должен составлять более 5 %.

3. ЗАДЕРЖКА В ПЕРЕДАЧЕ ПАКЕТОВ.

IP пакеты должны передаваться с максимальной задержкой 100-150 млсек.

4. ОТКЛОНЕНИЕ ОТ СРЕДНЕГО УРОВНЯ ЗАДЕРЖКИ.

Джи́ттер. не более 100-150 мс.

5. Некоторые провайдеры ограничивают своим клиентам количество сессий, инициированных пользователями, и поэтому в голосовой передаче также наблюдаются сбои. Для этого можно рекомендовать клиентам выключать скайп (это минус до 200 сессий на одного пользователя).

**Диагностика качества соединения**

При использовании SIP-телефонии возникают проблемы с плохим качеством связи: искажение голоса, задержка, эхо, проблемы с завершением вызова (нарушения сигнализации).

У многих начинающих, а порою и у "продвинутых" пользователей первое, что приходит в голову: "В этом виноват SIP-провайдер".  Прежде, чем делать скоропостижные выводы или открывать сайт определения скорости, рекомендуем ознакомится с  данным руководством которое поможет Вам более точно установить причину происходящего. Для начала обязательно отключите все работающие на данный момент закачки на Вашем компьютере, это могут быть торренты или другие файлообменные сети, обновления антивируса или операционной системы и т.п. Убедитесь, что Ваш тарифный план поддерживает скорость, которую Вы предполагаете увидеть, посмотрите условия тарифного плана, сделайте тест пропускной способности. Начните проверку с пункта Отклик. Для более точной информации о конкретном сайте или узле используйте Трассировку. Чтобы сообщить о проблеме нам, нужно подготовить данные для анализа - о том, как это сделать, смотрите пункт Pathping.

**Отклик (ping).**

**ping** - утилита для проверки соединений в сетях.

Она отправляет запросы указанному узлу сети и фиксирует поступающие ответы. Время между отправкой запроса и получением ответа позволяет  определять двусторонние задержки по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах. Утилита ping является одним из основных диагностических средств в сетях и входит в поставку всех современных сетевых операционных систем.

Важно!

Некоторые сервера, узлы или маршруты могут блокировать отклик (ping), так же может быть увеличенный отклик, если отклик-запросы стоят в низком приоритете обработки данных у данного оборудования.

Проверить отклик до какого то определенного сайта или узла элементарно. Запустите консольную строку (**Пуск > Выполнить > наберите cmd > Ок**)

В появившемся черном окне наберите команду **ping vats.cifra1.ru** нажмите **Enter**, дождитесь окончания проверки.



Как видно из скриншота, все пакеты были доставлены, потерь связи не наблюдается, средний отклик составляет 1мс, в вашем случае он может быть 60мс.

Более подробно в [Википедии](https://ru.wikipedia.org/wiki/Ping).

**Трассировка (tracert)**

**tracert** - это служебная компьютерная утилита, предназначенная для определения маршрутов следования данных в сетях.

Утилита tracert выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки. Данной утилитой стоит пользоваться в личных целях для определения сложившийся ситуации в Интернете. Запустите консольную строку (Пуск > Выполнить > наберите cmd > Ок) В появившемся черном окне наберите команду **tracert vats.cifra1.ru,**нажмит **Enter**, дождитесь окончания проверки, появится надпись Трассировка завершена.

Теперь Вы наглядно видите какой путь совершает запрос с Вашего компьютера до сервера Виртуальной АТС. Увеличение отклика (ping) зависит от нагрузки оборудования,

через которое проходит запрос и обрабатывается, это хорошо видно.

Более подробно в [Википедии](https://ru.wikipedia.org/wiki/Traceroute).

**Pathping**
**Pathping** - это утилита для трассировки сетевого маршрута, сочетает в себе функциональность утилит ping и tracert и обладает дополнительными возможностями.

PathPing предоставляет информацию о латентности сети и потерях данных на промежуточных узлах между исходным пунктом и пунктом назначения. Команда pathping в течение некоторого периода времени отправляет многочисленные сообщения с эхо-запросом каждому маршрутизатору, находящемуся между исходным пунктом и пунктом назначения, а затем на основании пакетов, полученных от каждого из них, вычисляет результаты. Поскольку pathping показывает коэффициент потери пакетов для каждого маршрутизатора или связи, можно определить маршрутизаторы или подсети, на которых имеются проблемы. Команда pathping выполняет эквивалентное команде tracert действие, идентифицируя маршрутизаторы, находящиеся на пути.
Существенным отличием от программы tracert в Windows является то, что маршрут следования icmp-пакета записывается в тело этого icmp-пакета, что накладывает определенные ограничения. Во-первых, такой метод поддерживается не всеми маршрутизаторами, а во вторых, накладывается ограничение на длину маршрута.

Данную утилиту стоит использовать для более детального сбора информации, в частности, для уточнения каких-либо вопросов по качеству своего интернет-соединения.

Запустите командную строку (**Пуск > Выполнить > наберите cmd > Ок**)

В появившемся черном окне наберите команду **pathping mail.ru** (вместо mail.ru укажите свой сайт), нажмите **Enter**, дождитесь окончания проверки.

Скопируйте результаты проверки: нажмите правой кнопкой мыши на черном экране, в появившемся окне нажмите Пометить или Выделить все, обведите весь текст который выдал pathping (для "Выделить все" не требуется), еще раз нажмите правую кнопку мыши или Enter, результаты скопированны.