CloudContact

Надежность и Безопасность

ОБЛАЧНЫЙ КОНТАКТ ЦЕНТР

ООО «Клауд Контакт»
127521 г.Москва 17-й проезд Марьиной рощи,
д.4, корп.1, офис 715

www.cloudcontact.ru

info@cloudcontact.ru

+7 (495) 927-01-41

Содержание:

НАДЕЖНОСТЬ 4
Резервирование Дата Центров 4
Отсутствие Единой точки отказа (SPOF, Single Point Of Failure)....4
Обновление настроек в режиме реального времени 5
Управление нагрузкой 5
Быстрое обнаружение проблемы 5
Переключение и балансировка 5
Отказоустойчивость 5
Резервирование 6
Техническое обслуживание....7
Аварийное восстановление 7
Дополнительная защита....7
БЕЗОПАСНОСТЬ 8
Использование протокола HTTPS 8
Шифрование речи и видео 8
Инфраструктура....8
Контроль доступа 8
Хранение и обработка конфиденциальных данных 9
Журнал действий 9
Поддержка российских стандартов информационной безопасности....9
Соответствие стандарту PCI-DSS 9
Соответствие стандарту HIPAA 10
Соответствие требованиям GDPR 10
ХАРАКТЕРИСТИКИ 11

Платформа Облачного контакт центра обеспечивает надежную работу сервиса и безопасность клиентских данных благодаря специальной программно-аппаратной архитектуре, наличию встроенных функций и процедур, соответствующих стандартам ГОСТ TLS, PCI DSS, HIPAA, GDPR **.**

Вся инфраструктура и серверное оборудование сервиса Облачного Контакт Центра расположены на территории Российской Федерации.

ВЫСОКОДОСТУПНЫЙ И ОТКАЗОУСТОЙЧИВЫЙ ОБЛАЧНЫЙ СЕРВИС

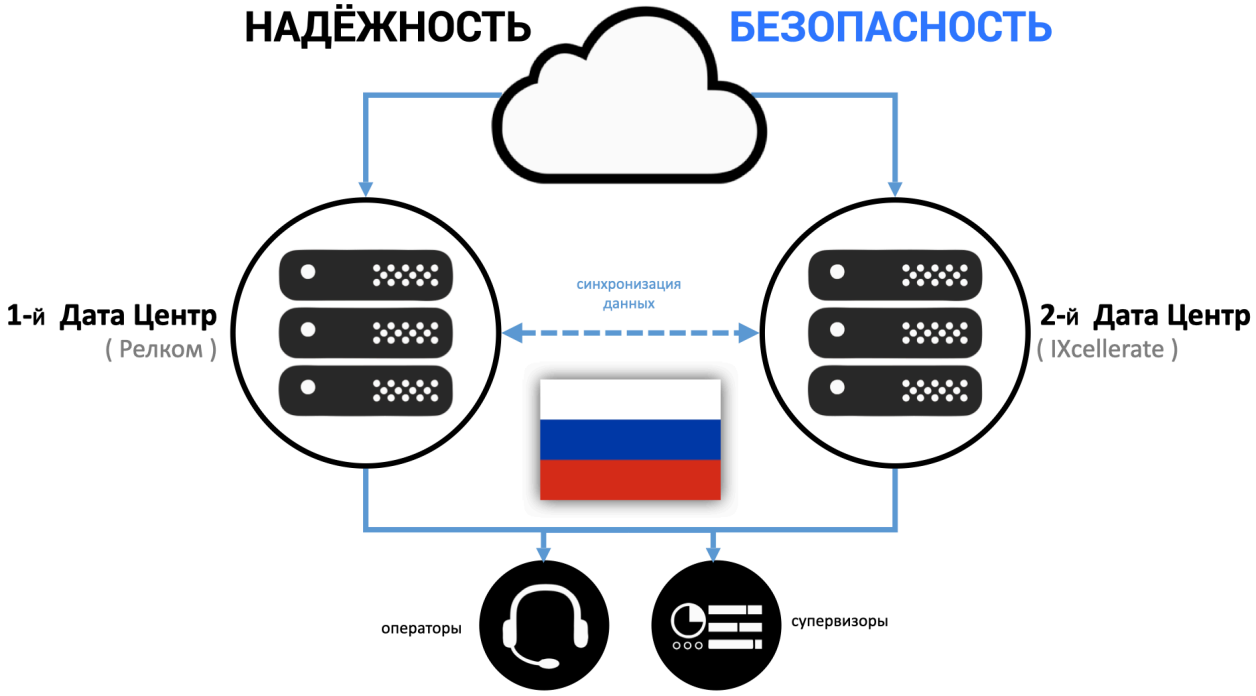
НАДЕЖНОСТЬ

Резервирование Дата Центров

Инфраструктура и оборудование Облачного Контакт Центра размещены в нескольких Дата Центрах для резервирования работы и балансировки нагрузки.

Одним из Дата Центров является *ДЦ «Москвич» / компания Релком* (г.Москва): один из самых современных ДЦ уровня *Tier III*, расположен в технополисе «Москва». Высокая отказоустойчивость инфраструктуры (99,982 %) обеспечивается распределением потоков: системы кондиционирования, каналов связи и электрооборудования, а также физической безопасности.

Одновременно с ним используется *ДЦ Кампус Moscow North / компания IXcellerate* (г.Москва) : соответствует уровню надёжности *Tier III* и обладает сертификатами *PCI DSS* и *ISO*. Компания *IXcellerate* является ведущим оператором сети коммерческих центров обработки данных и входит в топ-3 крупнейших игроков в России.



Отсутствие Единой точки отказа (*SPOF, Single Point Of Failure*)

Архитектура Облачного КЦ построена таким образом, что программные компоненты сервиса одновременно работают на нескольких серверах. Каждая компонента существует в нескольких экземплярах. Компоненты постоянно взаимодействуют друг с другом, образуя логические кластеры.

База данных *Mongo*, используемая для хранения данных, применяется в конфигурации “master/slave” на зарезервированных группах серверов с переключением «на лету».

База данных *MySQL*, используемая для хранения настроек конфигурации сервиса и отчетов, применяется в виде пар “ master/slave ” с переключением «на лету».

Обновление настроек в режиме реального времени

Все компоненты сервиса могут быть обновлены в режиме реального времени. Для их применения не требуется перезапуск системы.

Управление нагрузкой

Когда компоненте облачного сервиса требуется обратиться к другой компоненте, задействуется список активных компонент, содержащийся в Серверах конфигурации. При выборе компоненты используется алгоритм последовательного выбора.

За счет того, что все компоненты постоянно находятся в работе, исключается простой сервиса при переключении компонент.

Быстрое обнаружение проблемы

Платформа Облачного Контакт Центра использует два механизма обнаружения проблем:

1. Все компоненты поддерживают постоянное соединение с Серверами конфигурации. Соединение используется для уведомлений о изменении конфигурации в режиме реального времени и контроля за работоспособностью компонент (*keepalive*). Сервера конфигурации используют данную информацию для отслеживания рабочего статуса компонент и изменений в балансировке нагрузки, когда это будет необходимо.
2. Многие компоненты связаны между собой напрямую и используют данные соединения для контроля работоспособности и оценки возможности выполнения того или иного запроса за установленный интервал времени.

Переключение и балансировка

При обнаружении проблемы, незавершенный запрос перенаправляется на другую компоненту. Сервера конфигурации сообщают о проблемной компоненте и сделанных изменениях всем остальным задействованным компонентам.

Например, если один из Серверов маршрутизации стал неисправным, Сервера конфигурации перенаправляют запросы на другой сервер и, одновременно, сообщают о проблемном сервере другим компонентам.

Отказоустойчивость

При построении архитектуры платформы Облачного Контакт Центра особое внимание было уделено использованию специальных механизмов, позволяющих обеспечить обработку обращения даже при отказе одной или нескольких компонент сервиса.

Примеры:

- При отказе одного из Медиа-серверов, соответствующий Сервер сигнализации выбирает другой Медиа-сервер и информирует обе стороны обращения о переключении на него. На время переключения происходит короткий период тишины, а затем – продолжение разговора. Разрыва соединения не происходит.
- Отказ одного из серверов маршрутизации ставит обращение в очередь и переводит его на другой сервер. Информация не теряется, время ожидания в очереди увеличивается максимум до 30 сек. Разрыва соединения не происходит.

- При отказе одного из блоков сценария обработки обращения, обращение передается в другой аналогичный блок для продолжения обработки. Вызов, обрабатываемый оператором, продолжается; вызов в очереди продолжает своё обслуживание; вызов в IVR – начинается с головного меню. Разрыва соединения не происходит.
- Отказ Сервера, контролирующего р.м. операторов, подключает к работе другой аналогичный сервер. Р.м. оператора автоматически переподключается к новому серверу. На время переподключения возможна задержка в несколько секунд о чём свидетельствует сообщение «*Соединение…*»

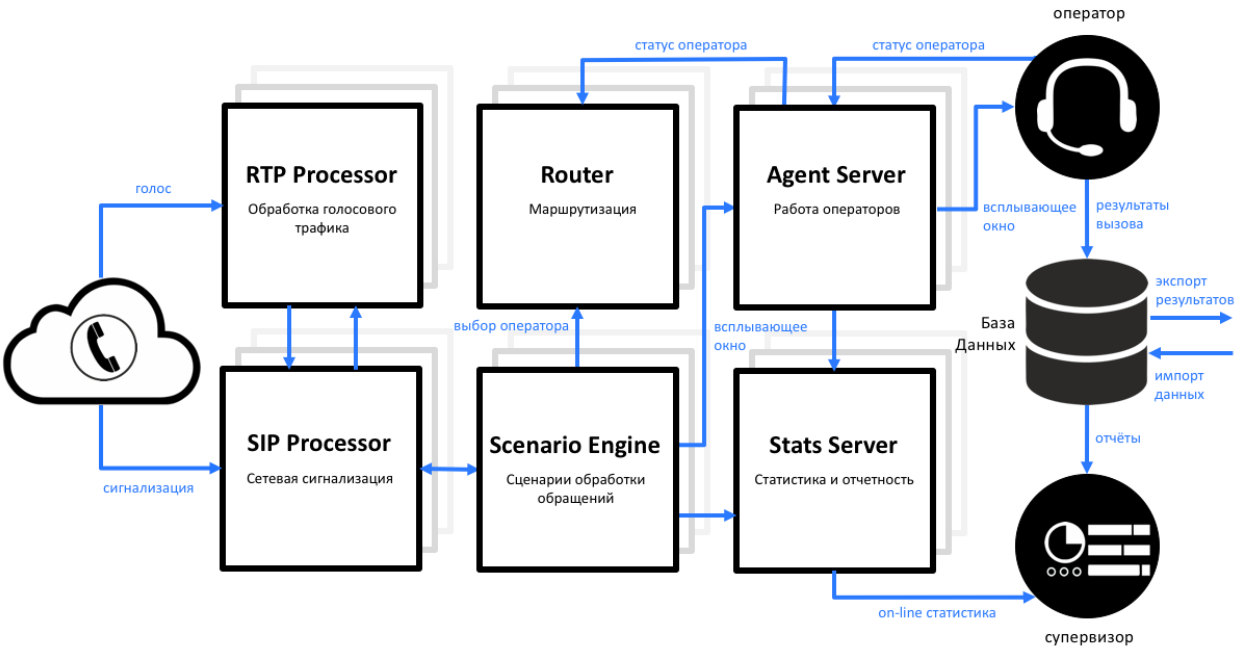
Резервирование

В стандартных системах нагрузка распределяется между всеми задействованными компонентами. В случае отказа одной из компонент, нагрузка на другие компоненты резко возрастает, что приводит к их перегрузке.

Платформа Облачного Контакт Центра полностью использует возможности протокола *SNMP* (*Simple Network Management Protocol* — Простой Протокол Сетевого Управления) для контроля состояния уровней системных ресурсов, уведомления при превышении установленных пределов и потребности в увеличении их емкости.

Важно, что резервирование не означает простое дублирование всех компонент, т.к. в платформе Облачного КЦ реализован принцип N + 1, означающий, что резервные мощности должны превышать или, как минимум, соответствовать возможному росту нагрузки при отказах компонент.

Дополнительным преимуществом используемого принципа резервирования является возможность проведения обновлений и иных регламентных работ без снижения производительности сервиса.



Техническое обслуживание

Когда сервис работает в режиме 24x7, проведение работ по техническому обслуживанию и обновлению становится сложной задачей. Поэтому в платформе Облачного Контакт Центра применяются специальные алгоритмы для проведения работ по обновлению ПО и оборудования, минимизирующие влияние на функционирование сервиса.

Когда надо временно отключить компоненту или сервер в целом, они прекращают обрабатывать новые запросы, завершают обработку текущих запросов и выключатся. Новые компоненты или сервера включаются в работу также «на лету».

Например, при замене серверов, сначала включается в работу новый сервер, а затем из работы выводится старый сервер. Аналогичным образом выполняются работы по добавлению/ перемещению оборудования между стойками или дата центрами.

Аварийное восстановление

Использование возможностей резервного копирования БД *MongoDB* и *MySQL* позволяет передавать актуальную информацию об обращении в режиме реального времени в резервный Дата центр. При возникновении аварийной ситуации в основном Дата центре, технический персонал переводит оборудование в резервном ДЦ в активный режим. Перенаправление информационных обращений происходит за счет обновления информации по протоколу *IP Border Gateway Protocol* (*BGP* - протокол граничного шлюза) или *Domain Name System* (*DNS* - системы доменных имён).

Дополнительная защита

ПО серверов, имеющих прямой выход в Интернет, регулярно обновляется и проходит обязательное тестирование на попытки несанкционированного доступа.

БЕЗОПАСНОСТЬ

Использование протокола *HTTPS*

Платформа Облачного контакт центра использует протокол *HTTPS* (*Hypertext Transport Protocol Secure*) для обеспечения конфиденциальности обмена данными между платформой и устройствами пользователей сервиса. Безопасность передаваемой информации обеспечивается за счет использования специальных криптографических протоколов SSL/TLS, имеющих 3 уровня защиты: шифрование данных (защита от перехвата); сохранность данных (контроль изменения данных); аутентификация (защита от перенаправления пользователя).

Шифрование речи и видео

Заказчик может выбрать вариант зашифрованной передачи голосовых сообщений между клиентом и оператором. В сочетании с безопасным подключением рабочих мест операторов по защищенному протоколу HTPPS , **шифрование голосового трафик**а значительно повышает безопасность использования Облачного КЦ. Шифрование голоса осуществляется по алгоритму **AES-128** (*Advanced Encryption Standard*), одному из наиболее часто используемых и наиболее безопасных алгоритмов шифрования в мире.

Безопасное соединение через браузер - *WEB RTC (Secure phone via browser audio)* также использует шифрование голосового трафика по алгоритму **AES-128**. Этот вариант позволяет устанавливать соединение, используя только браузер и не требует установки дополнительных плагинов, обеспечивая быстрое подключение новых рабочих мест.

Все данные, относящиеся к конфиденциальной информации могут быть зашифрованы. Это касается записей разговоров, экранов операторов, содержания email, записей чатов, а также отдельных полей в формах (скриптах), заполняемых операторами в процессе работы с обращением.

Инфраструктура

Платформа Облачного контакт центра обеспечивает одновременную параллельную работу нескольких Заказчиков Сервиса. Каждый Заказчик имеет доступ только к своему Контакт центру и его настройкам; критические параметры, влияющие на работу КЦ, могут быть защищены с помощью независимых межсетевых экранов (*firewall*). Доступ по API может быть ограничен только для заданного диапазона IP-адресов. Для каждого КЦ Заказчика создаётся свой собственный *ключ шифрования данных*, который может быть изменен в любое время. Данный ключ защищён *специальным ключом шифрования*, хранящимся в отдельном месте.

Контроль доступа

Платформа Облачного Контакт Центра контролирует права доступа к различным функциям КЦ с помощью *ролей* – специального набора полномочий, предоставляющих/ ограничивающих доступ к той или иной функции. Каждая учетная запись пользователя защищена паролем, требования к которому могут настраиваться на уровне провайдера сервиса или конкретного Заказчика. Пароли никогда не отображаются и не хранятся в явном виде. После заданного количества неудачных входов в сервис, учетная запись может быть заблокирована. Если учетная запись не используется в течении длительного времени (период настраивается), она может быть отключена. При этом вся историческая отчетность и записи обращений, связанные с данной записью, сохраняются. Неактивные сессии пользователей с правами администратора завершаются автоматически.

Хранение и обработка конфиденциальных данных

Все данные, относящиеся к конфиденциальной информации (включая карточные данные), могут быть зашифрованы. Это касается записей разговоров, экранов операторов, содержания email, записей чатов, а также отдельных полей в формах (скриптах), заполняемых операторами в процессе работы с обращением. Требование использовать защищенное соединение может быть распространено для внешних приложений, участвующих в сценарии обработки обращения. Сохранение конфиденциальных данных также может полностью отключено при запуске сервиса в работу. Согласно последним требованиям *PCI*, запрещающим хранение авторизационных данных (PIN, CCV и т.п.) в любой форме, запись разговора на время ввода данных может быть остановлена вручную оператором или автоматически специальным приложением с использованием API. Процесс авторизации также может быть выполнен с помощью IVR без участия оператора.

Журнал действий

Платформа Облачного Контакт Центра хранит данные обо всех попытках входа в сервис, включая неуспешные. Сохраняются подробные данные о всех действиях уровня администратора КЦ, включая дату/время, тип действия и задействованные ресурсы. Доступ к Журналу действий защищен требованием наличия специального полномочия. Срок хранения данных в Журнале действий соответствует требованиям PCI: минимум 1 год, быстрый доступ к данным за последние 3 месяца.

Поддержка российских стандартов информационной безопасности

Платформа Облачного Контакт Центра поддерживает протокол *ГОСТ TLS* и сертификаты *Национального удостоверяющего центра (НУЦ) Минцифры России*.

ГОСТ TLS обеспечивает защищенную передачу данных с использованием российских криптографических алгоритмов. Поддержка реализована для веб-интерфейсов оператора, супервизора и администратора Облачного Контакт Центра. Это позволяет организовать защищенный доступ к сервису с использованием отечественных средств криптографической защиты.

Поддержка сертификатов *Национального удостоверяющего центра Минцифры России* используется параллельно с сертификатами международных удостоверяющих центров, что позволяет сохранить совместимость с привычными средствами доступа и одновременно обеспечить поддержку требований российского законодательства и отраслевых регуляторов, касающихся защиты конфиденциальной информации.

Проверить поддержку протоколов *TLS*, включая *ГОСТ TLS*, на выбранном сайте или сервере и получить информацию о параметрах соединения можно с помощью специального тестировщика, размещенного на сайте компании. Инструмент доступен всем посетителям сайта и не требует регистрации.

Соответствие стандарту *PCI-DSS*

Стандарт *PCI DSS* (*Payment Card Industry Data Security Standard*) - Стандарт безопасности данных индустрии платежных карт, разработан международными платежными системами *Visa* и *MasterCard* и предназначен для использования компаниями, осуществляющими приём и обработку данных банковских карт. Несмотря на то, что данный стандарт изначально предназначен для обеспечения работы подразделений, связанных с обработкой карточных транзакций, технологические решения, используемые в данных подразделениях, также должны соответствовать требованиям стандарта. В их число входит и Контакт Центр. Платформа Облачного Контакт Центра в полной мере соответствует требованиям стандарта *PCI DSS* и обеспечивает надежную и безопасную работу с клиентскими данными.

Соответствие стандарту *HIPAA*

Стандарт *HIPAA* (*Health Insurance Portability and Accountability Act*, США) - представляет собой набор специальных стандартов конфиденциальности и безопасности на основе Закона о преемственности и подотчетности медицинского страхования (*HIPAA*). Стандарты определяют правила обмена Охраняемой информацией о здоровье (*Protected Health Information – PHI*) и ее защиты от несанкционированного использования. Отдельный закон *HITECH Act* ужесточил контроль за нарушениями стандартов и расширил область действия стандартов HIPAA на т.н. бизнес-партнеров, включая поставщиков облачных сервисов. Платформа Облачного Контакт Центра полностью соответствует положениям *HIPAA* и *HITECH* в части защиты персональных данных.

Соответствие требованиям GDPR

Платформа Облачного Контакт Центра обеспечивает полное соответствие услуг, оказываемых Вашей компанией, требованиям GDPR (*General Data Protection Regulation - Общий регламент по защите данных*, предназначенный для защиты персональных данных в Европейском Союзе).

Предоставляется несколько вариантов защиты и документирования согласия клиента на запись разговоров, многоуровневые разрешения для доступа к данным и расширенные возможности удаления записей.

ХАРАКТЕРИСТИКИ

Всё оборудование и инфраструктура расположены на территории РФ

Поддержка российских стандартов информационной безопасности

Применение безопасного протокола *HTTPS*

Использование зарезервированных Дата-центров уровня Tier III

Инфраструктура

Независимая работа КЦ многих Заказчиков
Разделение функций управления платформой сервиса и отдельных КЦ
Независимые межсетевые экраны для системных функций
Защита от Межсайтового скриптинга (*XSS - Cross-Site Scriptin*)
Защита от Межсайтовой подделки запроса (*CSRF - Cross Site Request Forgery*)
Ключи шифрования данных, уникальные для каждого КЦ
Защита ключей шифрования данных с помощью специального ключа шифрования, хранящегося отдельно
Смена ключа шифрования данных в любое время

Контроль доступа

Учетные записи пользователей защищены паролем
Доступ только с заданных IP-адресов (двухфакторная авторизация)
Обязательная смена пароля при первом входе в сервис
Настройка требований к паролю на уровне провайдера сервиса
Шифрование/скрытие пароля
Ограничение срока действия пароля
Контроль за повторным использованием пароля
Блокировка учетной записи после заданного количества неуспешных попыток входа
Отключение учетной записи с сохранением статистик и записей обращений
Автоматическое отключение после заданного периода неактивности
Ролевая политика контроля доступа к функциям сервиса
Специальные полномочия для доступа к конфиденциальным данным клиентов

Хранение и обработка конфиденциальных данных

Шифрование речи по протоколу AES 128
Шифрование всех конфиденциальных данных
Использование безопасных протоколов для внешних приложений (*SSL/TLS, HTTPS, SFTP*)
Поддержка российского протокола *ГОСТ TLS*
Наличие сертификата *Национального удостоверяющего центра (НУЦ) Минцифры России*
Скрытие конфиденциальных данных в логах работы КЦ
Ручная остановка записи разговора из приложения оператора
Автоматическая остановка записи разговора с помощью API
Поддержка передачи DTMF сигналов вне разговорного тракта (*out-of-band DTMF*, стандарт *RFC 2833/4733*)
Авторизация в IVR

Журнал действий

Раздельные журналы действий для сервиса в целом и конкретного КЦ
Данные о всех попытках входа
Протоколирование всех действий уровня администратора КЦ
Протоколирование доступа к записям разговоров и экранов оператора
Подробные данные о каждом действии (дата/время, пользователь, тип действия, задействованный ресурс)
Специальное полномочие для доступа к Журналу действий
Настраиваемый период хранения данных в Журнале действий

© ООО «Клауд Контакт», 2026 г. Составление и содержание. Перепечатка и использование данных материалов без письменного разрешения запрещено.