

БЕЛАЯ КНИГА

Отказоустойчивость сетей и сервисов Cloudflare



Содержание

3	Обзор
4	Жизнь в несовершенном мире
5	Как Cloudflare проектирует отказоустойчивость
5	Отказоустойчивость плоскости управления
6	Отказоустойчивость плоскости данных
7	Достигаемость периферии сетит
9	Доступность периферии сети
11	Доступность сервера-источника
12	Приверженность операционной прозрачности
12	Заключение

Обзор

Интернет построен на несовершенных системах, которые отдают приоритет бесперебойной работе превыше всего. Такие протоколы, как [TCP](#) и [BGP](#), основаны на [принципах распределенных систем](#) — предполагать наличие сбоев и учитывать их — и Интернет был спроектирован соответствующим образом. Однако точки отказа по-прежнему существуют и могут оказывать влияние на работу сети. Поставщики сетевых услуг должны иметь возможность планировать сбои, обнаруживать их при их возникновении и минимизировать последствия для пользователей.

В связи с тем, что многие приложения в Интернете работают в режиме реального времени, сети должны не только покрывать как можно большую часть Интернета, но также должны реагировать и минимизировать последствия в режиме реального времени. Простои продолжительностью в несколько минут недопустимы: клиенты ожидают устранения проблем за считанные секунды. устранения неполадок за считанные секунды.

Cloudflare предоставляет критически важные услуги сетевой инфраструктуры для поддержки безопасности и коммуникации организаций в Интернете. Мы разработали нашу сеть и услуги, которые она предоставляет, чтобы поддерживать высочайший уровень операционного совершенства. Cloudflare обрабатывает в среднем более 84 млн HTTP-запросов и 61 млн DNS-запросов в секунду, предоставляя услуги миллионам интернет-ресурсов и пользователей.

Как Cloudflare обеспечивает надежные услуги в таком масштабе, учитывая непредсказуемые характеристики Интернета?

Ответ кроется в архитектуре [сети Cloudflare](#), которая обладает возможностями обеспечения отказоустойчивости, разработанными для автономной работы и устойчивости к широкому спектру сбоев. Наши вычислительные, сетевые возможности и возможности хранения данных, наряду с нашими операционными процессами, разработаны таким образом, чтобы сделать Cloudflare таким же надежным, как гудок телефонной сети общего пользования. Cloudflare обеспечивает метафорический «облачный гудок» для сетевых сервисов и сервисов безопасности, на которые полагаются клиенты, независимо от текущих условий Интернета.

В данном техническом документе рассматриваются проблемы работы в режиме реального времени в Интернете и уникальные возможности Cloudflare для решения этих проблем.

Жизнь в несовершенном мире

Интернет — несовершенное место, и все же он необходим организациям для построения своего бизнеса и управления организациями, которые связывают распределенных пользователей, данные и устройства с облачными приложениями. Любой сбой в работе сервиса имеет серьезные последствия. На протяжении многих лет Cloudflare [сообщала о ряде крупных сбоев в работе интернет-сервисов](#) по всему миру, начиная от аварий, DDoS-атак и заканчивая стихийными бедствиями и многим другим.

Интернет представляет собой разнообразную сеть, построенную как слабо связанный конгломерат тысяч участвующих сетей различного размера и пропускной способности. Эти сети имеют различные уровни обслуживания: некоторые функционируют, насколько могут, в качестве проявления доброй воли, а другие — как часть их коммерческих услуг. Благодаря взаимным соглашениям об обмене трафиком, который может быть предназначен или не предназначен для хостов в их собственной сети, Интернет функционирует как глобальная структура благодаря добросовестному участию региональных и местных интернет-обменных узлов и поставщиков услуг.

Однако с таким многообразием приходит и определенная степень непредсказуемости. Путь, который проходит любой пакет, зависит от последовательности эвристических решений и принципов best effort при доставке. В отсутствие данных в режиме реального времени или прогностического моделирования фактических условий сети в данный момент времени, пакет, как правило, выбирает свой следующий переход либо по маршрутам по умолчанию, либо по предполагаемому кратчайшему пути. Ни один из этих вариантов не учитывает состояние сети при принятии [решений о маршрутизации](#). Это означает, что пакеты часто подвергаются ряду неблагоприятных условий:

- На самом базовом уровне в сетях могут возникать временные сбои и деградации работы, которые снижают пропускную способность и приводят к потере пакетов.
- По мере того как сети становятся насыщенными, перегрузки снижают производительность и пользовательский опыт.
- Хотя такого рода замедления могут происходить в нормальных условиях работы, растущее число сбоев умышленно вызвано враждебными субъектами, которые злонамеренно потребляют доступные ресурсы.

Миссия Cloudflare — внести свой вклад в создание лучшего Интернета. С этой целью мы создаем инфраструктуру, чтобы сделать Интернет быстрее, надежнее и безопаснее. Это становится возможным благодаря сервисам, предоставляемым сетью Cloudflare — одной из крупнейших сетей в мире, работающей на наших собственных физических серверах (без виртуализации), частной магистральной сети и огромному глобальному охвату, доступному в среднем в пределах 50 мс от 95 % населения мира.¹

Клиенты часто хотят узнать, как это делается. Как Cloudflare предоставляет сервисы в таких масштабах, без компромиссов между безопасностью и производительностью, и обеспечивая надежность, необходимую организациям? Ответ заключается в наборе целей «North Star», который определяет, как мы строим нашу инфраструктуру, чтобы поддерживать производительность, несмотря на разрушительное влияние внешних и внутренних факторов.

Как Cloudflare проектирует отказоустойчивость

Многие организации сосредоточены на повышении доступности, пытаясь лучше или быстрее реагировать на сбои. Это требует постоянных инвестиций в возможности аварийного переключения и процессы [их тестирования](#). И хотя это обоснованные цели, Cloudflare придерживается другого подхода: наши инженерные команды по отказоустойчивости тратят огромные усилия на то, чтобы сократить число сценариев, в которых требуется реагирование в рамках аварийного восстановления.

Обеспечение отказоустойчивости от Cloudflare начинается с простой предпосылки: **Как можно построить критически важную инфраструктуру, которая остается работоспособной в случае сбоев?**

Когда сбои неизбежны, отказоустойчивые сервисы Cloudflare обнаруживают и изолируют их, чтобы они не повлияли на доступность сервисов. Сбои устраняются вне основного контура предоставления сервисов. Мы стремимся к отказоустойчивости по всей нашей инфраструктуре.

Чтобы понять принципы обеспечения отказоустойчивости, полезно сначала определить ключевые понятия, связанные с путями трафика в Cloudflare, а также цели проектирования ключевых систем. На самом абстрактном уровне архитектуру Cloudflare можно разделить на два компонента: **плоскость управления и плоскость данных**. Каждая из них имеет уникальные характеристики отказоустойчивости и стратегии реагирования на аварийные ситуации.

Отказоустойчивость плоскости управления

Плоскость управления предоставляет интерфейс управления, который формирует единый источник истины для конфигурации сетевых и защитных сервисов в среде клиента. Сама плоскость управления не обрабатывает трафик (в этом роль плоскости данных). Она определяет, какие политики должна применять плоскость данных, и управляет конфигурациями в различных центрах обработки данных.

Сервисы плоскости управления Cloudflare обычно развертываются в более традиционной, централизованной архитектуре, состоящей из трёх логически связанных, но независимых центров обработки данных в основном регионе (например, в США). Эти три центра обработки данных реплицируются с эквивалентной пропускной способностью во вторичный регион (например, ЕС). Сервисы плоскости управления предназначены для обеспечения отказоустойчивости и поддержания стабильного предоставления услуг в случае сбоя любого центра обработки данных в основной локации. Потеря дополнительных центров обработки данных в основной локации приведет к аварийному переключению на центры обработки данных другого региона (например, в Европе вместо США).

Сохраняя приоритет отказоустойчивости над восстановлением, Cloudflare продолжает инвестировать в укрепление нашей устойчивости.

Например:

- Мы все чаще используем два региона плоскости управления конфигурации active-active, что одновременно повышает нашу емкость и скорость реагирования, а также нашу устойчивость к сбоям. Соответственно, мы можем выдержать больше типов сбоев без нарушения работы сервисов или необходимости аварийного переключения.
- Мы также увеличиваем степень детализации перемещения сервисов между различными площадками плоскости управления, что позволяет нам более точно реагировать на проблемы локальной инфраструктуры.

Хаос-тестирование

Отказоустойчивость — это не процесс, который можно настроить один раз и забыть о нем. Даже самые надежные планы по обеспечению отказоустойчивости могут оказаться неэффективными из-за «дрейфа» системы — медленного и часто незаметного накопления изменений, которые могут снизить ожидаемое поведение и привести к непредвиденным режимам отказа. Чтобы проактивно устранять этот риск, Cloudflare регулярно проводит хаос-тесты, систематически выявляя потенциальные уязвимости, связанные с дрейфом.

Отказоустойчивость плоскости данных

Плоскость данных обрабатывает трафик клиентов Cloudflare в соответствии с политиками, установленными в плоскости управления. Хотя сервисы плоскости данных получают указания от плоскости управления, их функционирование от этого не зависит. Все политики поддерживаются через [Quicksilver](#), наше глобально распределенное хранилище ключей и значений, чтобы гарантировать, что сервисы останутся работоспособными с заведомо корректной конфигурацией в случае нарушения связи с плоскостью управления.

Anycast играет важную роль в обеспечении избыточности центров обработки данных. Центры обработки данных Cloudflare, расположенные в более чем 330 городах, автономны на локальном уровне, но при этом взаимозаменяемы между собой через Anycast и BGP. Это связано с тем, что каждый центр обработки данных может обрабатывать любые сервисы локально, без взаимозависимости от сервисов в другом центре обработки данных. Благодаря Anycast каждый центр обработки данных фактически является избыточным по отношению к другим. Поскольку каждый центр обработки данных участвует в Anycast, нет необходимости инструктировать клиента о переключении на альтернативный центр обработки данных по другому IP-адресу.

Будь то потребитель, посещающий защищенный Cloudflare веб-сайт, сотрудник, работающий с интернет-приложениями, или офис, подключающийся к своей WAN — во всех этих сценариях используется BGP для определения ближайшего центра обработки данных Cloudflare Anycast. Если выбранный ими центр обработки данных становится недоступным, BGP автоматически переключится на следующий доступный центр обработки данных Cloudflare.



Cloudflare обеспечивает отказоустойчивость плоскости данных, решая три различные задачи:

- **Достижимость периферии сети:** обеспечение возможности попадания трафика конечных пользователей в центры обработки данных и устранение единых точек отказа на входе трафика.
- **Доступность периферии сети:** поддержание качества кода и непрерывной доступности программного обеспечения за счет тщательного управления изменениями.
- **Достижимость сервера-источника:** адаптивная маршрутизация к клиентским приложениям, обеспечивающая отсутствие потерь на исходящих маршрутах.

Достигаемость периферии сети

Достигаемость периферии сети — это возможность конечных пользователей достигать сети Cloudflare. Это, без сомнения, самая важная часть задачи обеспечения отказоустойчивости. Если интернет-провайдеры (ISP) или центры обработки данных выходят из строя, достигаемость периферийных узлов снижается или деградирует, что препятствует или замедляет перемещение пользователей к нужным им ресурсам в Интернете. Cloudflare решает проблемы с достигаемостью периферии сети четырьмя основными способами:

1. Сеть Anycast



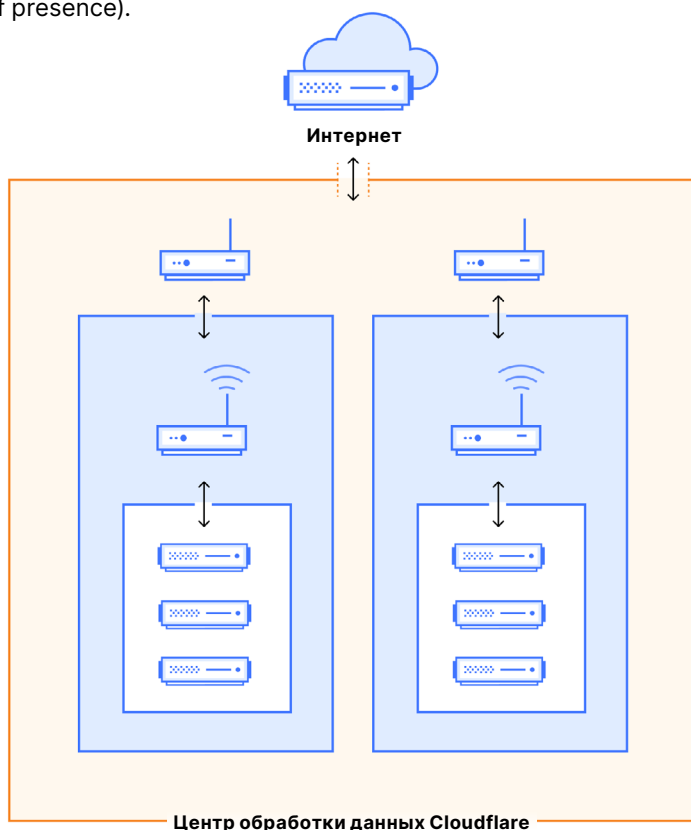
Улучшенная производительность сети с учётом отказоустойчивости заложена в нашу сетевую архитектуру, которая в значительной степени использует технологию Anycast. Anycast — инженерная «сверхспособность» Cloudflare — означает, что IP-пространство анонсируется повсеместно: если одна из наших точек присутствия (PoP) становится недоступной, трафик будет просто перенаправлен в другие локации, а не отброшен. То, что Cloudflare представлена в большом числе городов по всему миру и [имеет пиринг](#) с местными сетями, означает, что мы обрабатываем клиентский трафик максимально близко к пользователю. Например, даже если транзит интернет-провайдера отключен или центр обработки данных теряет питание, трафик не пострадает.

2. Все сервисы Cloudflare работают во всех локациях

Помимо Anycast, центры обработки данных Cloudflare разработаны таким образом, чтобы обрабатывать трафик локально и не находиться во взаимозависимости с прокси-цепочками к другим вычислительным узлам. Мы запускаем практически все сервисы на каждом сервере. Это означает, что центр обработки данных может быть отключен от сети без ущерба для клиентов. Серверы в центре обработки данных взаимозаменяемы, поскольку сотни серверов выполняют один и тот же сервис и могут заменить вышедший из строя в случае необходимости.

3. Мультиколокационные точки присутствия

Конструкция центров обработки данных Cloudflare и их расположение соответствуют потребностям наших клиентов. Сеть Anycast позволяет нам добавлять и удалять центры обработки данных по своему усмотрению, но мы должны постоянно отслеживать производительность клиентов. Мы адаптировали топологию наших центров обработки данных таким образом, чтобы различные участки вычислительных мощностей (колокации) могли выходить из строя независимо друг от друга. Эти центры обработки данных (с несколькими колокациями) называются мультиколокационными точками присутствия или локациями MCP (multi-collocation points of presence).



Эти локации разделяют подключение к Интернету и внутреннее подключение вычислительных ресурсов, что позволяет отключать колокации по отдельности. Это означает, что даже если с колокацией возникает проблема, вся точка присутствия в регионе остается онлайн, обеспечивая повышенное время безотказной работы и производительность для клиента. Этот тип центра обработки данных также устраняет единые точки отказа за счет наличия избыточных устройств на интернет-ориентированном уровне: если один периферийный к Интернету (периферийный) маршрутизатор выйдет из строя, другой сможет принять на себя трафик и обеспечить непрерывность работы локации.

Эта операционная модель помогает локациям MCP избегать ненужного перераспределения трафика, что дополнительно повышает время безотказной работы клиентов Cloudflare.

4. Cloudflare Traffic Manager

Центры обработки данных MCP работают в тесной связке, образуя более широкую сеть Cloudflare. Эта сеть использует Anycast, чтобы гарантировать обслуживание клиентского трафика. Anycast улучшен за счет детерминированного управления трафиком, гарантируя, что запросы клиентов будут обслуживаться там, где это возможно, с максимальной производительностью. Система управления трафиком, Traffic Manager, работает, постоянно зондируя сеть Cloudflare и автоматически уводя трафик от центров обработки данных, испытывающих перегрузку ЦП. Это предотвращает перегрузку в центрах обработки данных с большим объемом трафика; вместо этого трафик интеллектуально направляется в другой центр обработки данных, который может его обработать.

Доступность периферии сети

Доступность периферии сети означает способность Cloudflare обрабатывать трафик после того, как он попадает в нашу сеть. Когда изменения в сетевых инструментах или программном обеспечении приводят к непреднамеренным изменениям, доступность может снизиться и повлиять на пользовательский опыт. Для предотвращения инцидентов, связанных с изменениями кода, Cloudflare вложила значительные средства в следующие механизмы контроля развертывания:

1. Воронка развертывания

При развертывании программного обеспечения качество кода обеспечивается с помощью отслеживания и ограничения возможностей разработчиков и клиентов вносить изменения в экосистему. Cloudflare ограничивает количество способов внесения изменений в нашу инфраструктуру, чтобы мы могли тщательно отслеживать каждое изменение и гарантировать прохождение полного набора тестов перед развертыванием в рабочей среде.

2. Управление изменениями радиуса поражения

Еще один способ, с помощью которого Cloudflare поддерживает доступность периферии сети во время развертывания, — это ограничение развертывания тестовыми центрами обработки данных или тестовыми группами до их широкомасштабного внедрения. Мы называем это управлением радиусом поражения.

После развертывания изменений в сети они могут быть активированы глобально в течение нескольких минут. Ограничивая изменения средой развертывания и внедряя последующие изменения по каскадной модели, мы можем отслеживать их влияние, чтобы выявить ожидаемые и неожиданные последствия — до того, как они затронут более крупные географические регионы или группы пользователей.

У нас есть два способа ограничить влияние изменений кода:

- Ограничение количества локаций, получающих изменения; и
- Ограничение числа пользователей, получающих изменения

Ограничивая количество локаций и серверов, получающих изменения, мы можем гарантировать правильное проведение А/В-тестирования кода в одной локации для оценки его работоспособности прежде чем продолжить. Ограничивая количество пользователей, получающих изменения, мы можем подвергнуть исправления боевому тестированию на меньших группах пользователей перед массовым внедрением.



3. Развертывание с учетом состояния

Развертывание на основе показателей работоспособности — это система, которая программно оценивает целесообразность того или иного релиза на основе заданных показателей, которые дают сигнал «можно» или «нельзя» в зависимости от потенциального воздействия. Такая серия автоматических проверок может не только предотвратить выход вредоносного релиза, но и откатить его при обнаружении инцидента.

Каждый продукт и сервис, развернутые через Cloudflare, должны иметь цель уровня обслуживания (SLO), которая содержит как метрику, отражающую работоспособность продукта, так и целевое значение, ниже которого продукт считался бы неработоспособным.

SLO имеют скорость выгорания или допустимые пороги отказов. Любой сервис, обеспечивающий работоспособность, будет предоставлять SLO автоматизированной системе при слиянии изменений для развертывания. В каждом установленном объеме развертывания (бесплатные планы, подмножество серверов в Ашберне и т. д.) автоматизированная система будет:

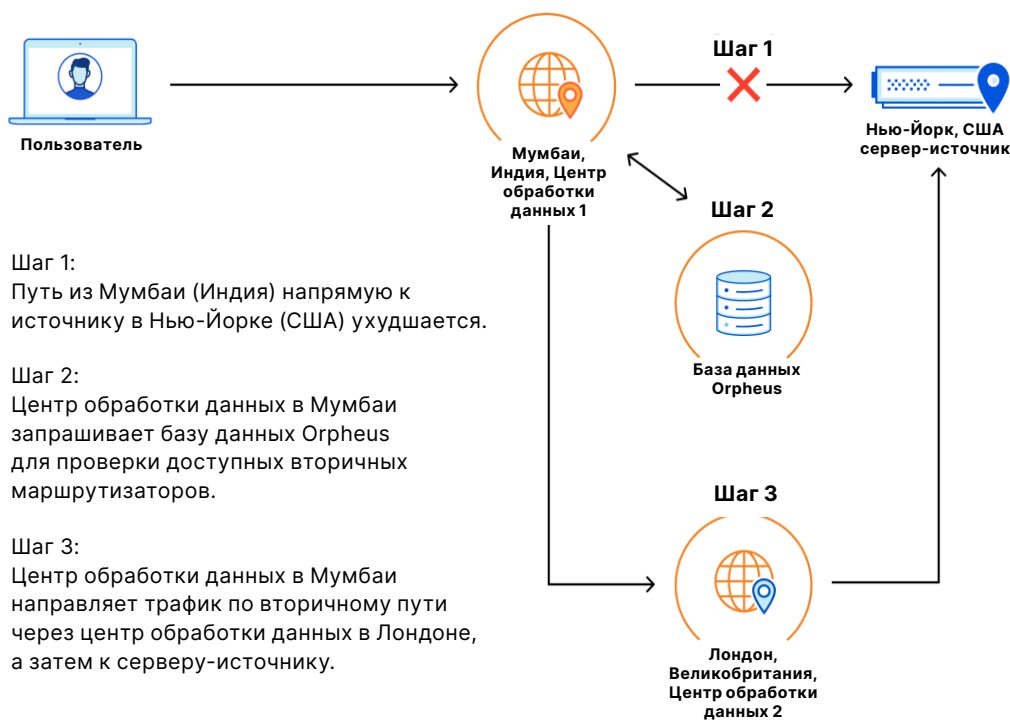
- Сначала отслеживать SLO сервиса в течение заданного периода времени, чтобы убедиться, что работоспособность не падает ниже порогового значения.
- Если SLO остается в допустимых диапазонах в течение установленного периода выдержки, система автоматически перейдет к более крупному этапу развертывания.
- Однако, в случае нарушения SLO, система автоматически останавливает развертывание и выполняет откат, чтобы ущерб автоматически нейтрализовывался.

Эти шаги гарантируют, что развертывание кода не повлияет на работоспособность клиента, а продолжительность развертывания будет максимально короткой.

Доступность сервера-источника

Достигаемость сервера-источника означает способность Cloudflare достигать конечных точек, будь то сервер-источник клиента, SaaS-сайт или общедоступный Интернет через Cloudflare Gateway. При этом маршрутизация запросов в нужное место критически важна для пользователей, получающих доступ к сети Cloudflare. Например, [Argo Smart Routing](#) — инструмент Cloudflare, оптимизирующий производительность (в частности, время до первого байта), постоянно проверяет сеть Cloudflare, чтобы найти самый быстрый путь к серверам-источникам.

[Orpheus](#), аналог Argo, имеет похожую философию, но выполняет другую функцию. Orpheus предназначен для установления надежных соединений с серверами-источниками. Orpheus специально анализирует метрики, влияющие на способность Cloudflare достигать сервера-источника (в отличие от самого быстрого пути к нему), и находит маршруты, которые минимизируют потерю пакетов, не влияя на стабильность работы. Это означает, что при возникновении проблем трафик автоматически перенаправляется в обход обнаруженных ошибок.



До того как Cloudflare выпустила Orpheus в 2021 году, мы успешно маршрутизировали трафик к серверам-источникам в 99,9 % случаев. После внедрения Orpheus наша способность направлять трафик к серверам-источникам увеличилась до 99,99 %. В следующем году мы планируем расширить Orpheus, чтобы защищать больше типов трафика, обрабатывать больше сценариев сбоев и ускорить работу с целью сокращения времени воздействия на пользователей.

Приверженность операционной прозрачности

Даже самые устойчивые и инновационные сети могут столкнуться с перебоями. Когда возникают инциденты, затрагивающие клиентов, Cloudflare соблюдает протокол реагирования, который включает тщательное расследование, внутренний и внешний отчеты об инциденте, а также, если необходимо, [обновления состояния](#) на протяжении всего периода воздействия.

В некоторых случаях, когда инциденты приводят к серьезным последствиям — или инновациям — постмортемы будут публиковаться в [блоге Cloudflare](#).

Заключение

Инженерная работа, стоящая за сетью Cloudflare, — это нелегкая работа, но работа, которую мы с гордостью выполняем для наших клиентов. Награда заключается в создании сетевой платформы, которая приносит пользу нашим клиентам и всему интернет-сообществу.

В конечном итоге, отдавая приоритет отказоустойчивости не просто как технической проблеме, а как основному операционному принципу, мы делаем больше, чем просто укрепляем оборону: мы активно строим компанию, которая по своей сути готова к будущему. Проактивный подход к постоянному тестированию и адаптации позволяет нам плавно развиваться в соответствии с постоянно меняющимися требованиями как наших клиентов, так и динамичным ландшафтом самого Интернета.

Мы понимаем, что многие концепции, представленные в этом документе, связаны с сетевыми вопросами, с которыми многие предприятия не сталкиваются, так как они касаются внутренней архитектуры работы глобальной облачной среды операторского класса.

Если вы хотите получить подробный брифинг, чтобы узнать больше об инженерии отказоустойчивости Cloudflare, [свяжитесь с вашим представителем Cloudflare](#).



Настоящий документ носит исключительно информационный характер и является собственностью Cloudflare. Настоящий документ не создает каких-либо обязательств или заверений со стороны Cloudflare или ее аффилированных лиц по отношению к вам. Вы несете ответственность за собственную независимую оценку информации, содержащейся в данном документе. Информация в настоящем документе может быть изменена и не подразумевает полноту или наличие всей информации, которая может вам понадобиться. Ответственность и обязательства Cloudflare перед ее клиентами регулируются отдельными соглашениями, и данный документ не является частью каких-либо соглашений между Cloudflare и ее клиентами и не изменяет их. Сервисы Cloudflare предоставляются «как есть», без каких-либо гарантий, заявлений или условий, явных или подразумеваемых.

© Cloudflare Inc., 2025. Все права защищены. CLOUDFLARE® и логотип Cloudflare являются товарными знаками компании Cloudflare. Все остальные названия компаний и продуктов могут являться товарными знаками соответствующих компаний, с которыми они связаны.