

Что означают ошибки 403, 404, 500, 502, 503, 504 и как их исправить?

Большинство известных видов ошибок в сети Интернет сопровождаются кодом состояния «**HTTP**». Обычно пользователи могут наблюдать сообщение об ошибке, содержащее помимо объясняющего текста еще числовое значение формата «**4XX**» или «**5XX**» (за числами четыре или пять следуют две дополнительные цифры, например, код ошибки имеет вид «**404**»).

И вариант формата «**4XX**», и «**5XX**» являются ошибками, но они имеют существенную разницу. Формат «**4XX**» – это ошибки, возникающие вследствие деятельности клиента, а «**5XX**» – результат ошибки сервера. Если при обращении к сетевому ресурсу всплывает сообщение с ошибкой в виде «**4XX**», то, скорее всего, пользователи могут ее самостоятельно исправить.

Ошибки вида «**5XX**» – это ошибки сервера, которые означают, что пользователи не оказывали влияния на результат, приведший к возникновению ошибки, и источником сбоя является неработающий сервер, к которому пользователи пытаются получить доступ. Независимо от вида ошибки, связанна ли она с деятельностью пользователей или работоспособностью удаленного сетевого сервера, пользователи могут предпринять несколько шагов, которые могут помочь решить проблему и устранить существующую неисправность.

В последующих разделах мы постарались перечислить наиболее распространенные сетевые ошибки, с которыми могут сталкиваться пользователи при взаимодействии с ресурсами сети Интернет, а также упомянули пару полезных решений для исправления каждой ошибки. Пользователи не могут решить все онлайн-ошибки, так как некоторые из них происходят по вине серверов, и с ними мало что можно поделать для успешного восстановления работоспособности. Тем не менее, в ряде случаев, стоит попробовать устранить возникшую ошибку.

Ошибка 403 Forbidden (доступ запрещен)

Для начала разберемся, что вообще из себя представляет такая ошибка.

Ошибка 403 (Forbidden) – это код состояния HTTP, который указывает на то, что сервер понял запрос, но отказывается его выполнить из-за ограничений доступа.

Другими словами, ошибка 403 означает, что у пользователя нет прав доступа к запрашиваемому ресурсу или действию.

Такая ошибка может появиться вследствие:

- неправильных настроек прав доступа на сервере – он может быть настроен таким образом, что определенные ресурсы доступны только для конкретных пользователей или их групп;
- отсутствия аутентификации – если запрашиваемый ресурс требует аутентификации, а пользователь не предоставил соответствующих учетных данных, сервер может вернуть ошибку 403;
- блокировки IP-адреса или ограничения при доступе – сервер может быть настроен для блокировки определенных IP-адресов или ограничения количества запросов от одного IP-адреса, что и может привести к ошибке 403;
- запрета авторизованных пользователей на выполнение определенного действия – даже если пользователь успешно пройдет аутентификацию, он может не иметь прав доступа к определенным действиям или ресурсам.

Теперь пройдемся по самым популярным причинам ошибки 403 и вариантам ее исправления:

Отсутствие файла index.php или index.html

Файл index.(php/html) – это общепринятое название основного файла сайта, с которого начинается обработка запроса к сайту. Если этого файла нет, то сайт вернет 403 код ошибки. На самом деле точный код ошибки зависит от настроек веб-сервера, но в большинстве типовых конфигураций используется 403 код. Для решения этой проблемы нужно убедиться в том, что при разворачивании сайта не потерялся файл index и что в его названии нет ошибок. В ispmanger вы можете это сделать, перейдя к файлам сайта в верхнем меню в разделе «Сайты».

Прямой запрет на доступ к файлам сайта внутри конфигурационного файла веб-сервера

Зачастую такой запрет встречается из-за некорректной настройки или вирусного заражения сайта. В данном случае необходимо проверить содержимое файла .htaccess, если в качестве веб-сервера используется Apache, либо конфигурационный файл nginx, если используется он. С анализом и решением проблемы может помочь техподдержка хостинга либо профильные сторонние специалисты.

Настроенные ограничения или аутентификация на стороне веб-сервера

Одна из самых частых ситуаций – слишком общая настройка ограничений для защиты от DDOS-атак (например, если запрещен доступ для какого-либо браузера/страны), вторая распространенная ситуация – некорректная настройка правил аутентификации для доступа к определенным разделам сайта. В обоих случаях необходимо проверить настройки в конфигурационных файлах веб-сервера. С анализом и решением в этом случае тоже может помочь техподдержка хостинга либо профильные сторонние специалисты.

В последних двух случаях, когда речь идет о запрете на доступ к файлам сайта внутри конфигурационного файла веб-сервера и настройках аутентификации на стороне веб-сервера, пользователи isrpmanger могут посмотреть файлы сайта прямо в панели, в разделе “Сайты”. При использовании веб-сервера apache подобные ограничения настраиваются в файле .htaccess в директории сайта.

Искать необходимо следующие строки (ниже приведены примеры правил, которые могут приводить к проблемам):

для запрета доступа:

```
Order Deny,Allow
Deny from all
```

для настроек авторизации:

```
AuthName "Protected area, need authorization"
AuthType Basic
AuthUserFile /home/t/test/.authfile
require valid-user
```

Обратите внимание: Внесение изменений без отчетливого понимания своих действий может привести к неработоспособности сайта, поэтому если вы не разработчик и у вас нет нужного опыта, лучше всего обратиться в техподдержку хостинга либо к профильным сторонним специалистам.

Ошибка 404 Not Found (не найдено)

Ошибка «404 Not Found» – самая распространенная ошибка в сети, которая возникает при попытке посетить несуществующую веб-страницу. В основном, данная ошибка подразумевает, что серверу не удалось найти, искомый пользователями, удаленный ресурс. В большинстве случаев, в обозревателе появится сообщение об ошибке «404» после неудачной попытки ввести «URL» искомой страницы или перейти по соответствующей ссылке, которая на сервере абсолютно не представлена. И если пользователи сталкиваются с ошибкой «404», то можно попробовать ее исправить несколькими способами.

Обновите проблемную страницу. Нажатие клавиши «**F5**» инициирует обновление страницы в подавляющем большинстве современных веб-браузеров. Не всегда такое решение сможет устранить ошибку «404». Но иногда, на веб-серверах может происходить случайный сбой и, как следствие, отображение страницы, которая действительно

существует, будет временно приостановлено. Поэтому необходимо обязательно опробовать данный способ и перегрузить страницу, в особенности, если на обновление будет потрачено всего несколько секунд, но существует шанс добиться корректной загрузки.

Убедитесь в правильности «URL- адреса». Неверно введенные «URL-адреса» (независимо от того, была ли допущена ошибка в процессе набора или веб-страница содержит неверную ссылку) являются наиболее частой причиной отображения в обозревателе сообщения об ошибке «404 Not Found».

Осуществите поиск требуемой страницы на сайте. Возможно пользователи получили неверный «URL-адрес» или на веб-сайте, с которого был осуществлен переход, указана ошибочная ссылка, но страница на искомом ресурсе существует. Попробуйте найти, посредством использования возможностей поисковой панели сайта, «URL» требуемой страницы по названию.

Ошибка 500 Internal Server Error (Внутренняя ошибка сервера)

Ошибка 500 (Internal Server Error) – это общий код состояния HTTP, который указывает на внутреннюю ошибку сервера. Она возникает, когда сервер не может выполнить запрос в результате какого-либо внутреннего сбоя или ошибки в работе серверного приложения.

Чаще всего ошибка 500 появляется, когда присутствуют ошибки в работе сайта, вызванные неправильной версией ПО (к примеру, сайты, несколько лет назад написанные на PHP 5.6, могут не работать на PHP 8, поскольку на современных ОС ставится актуальная версия) или ошибками в коде сайта.

Для решения проблемы необходимо проанализировать ошибки в логах веб-сервера и исправить их. После определения ошибки можно воспользоваться поисковиками или популярными нынче чат-ботами для поиска решения проблемы либо обратиться к профильным специалистам или в техподдержку хостинга.

В `ispmanager` логи можно посмотреть в разделе “WWW” -> “Журналы”. Анализировать необходимо файл лога ошибок, который называется: `название_сайта.error.log`. В нем содержатся ошибки веб-сервера.

К сожалению, ввиду того, что причины ошибки 500 уникальны для каждого отдельного случая, приводить конкретные примеры решений довольно затруднительно. Рассмотрим возможные варианты решения:

1. Проверьте сайт, созданный с помощью CMS, на наличие проблем с плагинами или ошибок в коде. В этом вам могут помочь лог-файлы. При обнаружении проблемного плагина обновите его или верните прежнюю версию. Если это не помогло, откажитесь от него. Если ошибка произошла после обновления CMS, проведите обновление повторно.

2. Посмотрите файл `.htaccess` на предмет ошибок в командах. Закомментируйте директиву `Options`, поставив перед ней решётку: если после этого ошибка 500 перестанет появляться, значит, есть нарушения в синтаксисе и в описании команд.
3. Убедитесь, что права доступа к файлам, папкам и скриптам выставлены верно. Для папок рекомендуется значение 755, для скриптов — 600, а для других файлов — 644. При других вариантах прав доступ к сайту может блокироваться в целях безопасности.
4. Проверьте, всё ли в порядке со скриптами. Возможно, какой-то из скриптов слишком медленный или время ожидания ответа от сервера слишком мало. Если при просмотре лог-файлов выяснится, что какой-то из скриптов незапланированно требует слишком много памяти, оптимизируйте его или удалите. А если обнаружится, что какой-то из скриптов вовсе не запускается, убедитесь, что функция прописана верно, поддерживается сервером и соответствует используемой версии PHP.
5. Отдельно обратите внимание на CGI-скрипты: вероятно, строки в них имеют не те окончания, что исправляется загрузкой скриптов через FTP в режиме ASCII. Также некорректная работа CGI-скриптов может быть причиной ошибок в HTTP-заголовках, что тоже приводит к ошибке 500. Либо же имеются ошибочные директивы, предназначенные для работы со скриптами.

Ошибка 502 Bad Gateway (Ошибочный шлюз)

Ошибка «502 Bad Gateway» означает, что посещаемый вами сервер пытался получить некоторую информацию с другого сервера, но получил неверный ответ. Причиной могут послужить несколько факторов. Возможно, сервер перегружен или возникли неполадки с сетью между двумя серверами, что носит временный характер, и может быть быстро исправлено. Также, как вариант, могут оказывать влияние на отсутствие доступа неправильные настройки брандмауэра или даже ошибка кодирования. В довольно редких случаях ошибка может возникать из-за проблемы на пользовательском компьютере или сетевом оборудовании. Поэтому стоит попробовать применить несколько шагов для возможного исправления ситуации.

1. Обновите страницу после отображения сообщения об ошибке. Как и в предыдущих случаях, воспользуйтесь быстрым способом перезагрузки страницы посредством нажатия в веб-браузере клавиши «F5».
2. Проверьте, доступен ли сайт для других пользователей. Посетите сайт, такой как [IsItDownRightNow](#) или [DownforEveryoneorJustMe](#), который отслеживает состояние веб-сайтов и проверяет их работоспособность для уточнения данных, испытывают ли другие пользователи трудности с доступом к конкретному ресурсу, или проблемы возникают только локально на пользовательском устройстве.
3. Выполните очистку «cookie» и содержимого кэша пользовательского браузера. Иногда (хотя и редко) серверы возвращают ошибки формата «502», потому что веб-браузер, который регулярно использует пользователь для выхода в сеть «Интернет», кэшировал устаревшие или поврежденные файлы. Процедура очистки содержимого кэша и файлов «cookie» может помочь исправить ошибку.

4. Убедитесь, что на ваш сайт не совершается DDoS-атака. В противном случае обратитесь к хостинг-провайдеру.
5. Если на вашем ресурсе фиксируется значительный рост посещаемости, то подберите более продвинутые условия хостинга, чтобы ошибка не появлялась вновь.
6. Проверьте нагрузку на сервер. Если лимит превышает, необходимо увеличить объём оперативной памяти.
7. Посмотрите настройки сервера. Возможными поводами для появления ошибки 502 могут быть:
 - неполадки после установки обновлений;
 - превышение лимитов на число обращений к внешним ресурсам и на время ответа сервера;
 - некорректные лимиты в файлах конфигурации ini;
 - превышение лимита на число php-cgi-процессов;
 - недостаточная оптимизация скриптов;
 - недостаточная оптимизация запросов;
 - неправильная работа модулей (если ошибка возникает при обращении к скриптам конкретного расширения).
8. Если ошибка продолжает появляться и если вы пользуетесь виртуальным хостингом, уточните у хостинг-провайдера, не создают ли другие сайты на сервере чрезмерную нагрузку.

Ошибка 503 Service Unavailable (Сервис недоступен)

Ошибка 503 Service Unavailable (сервис недоступен) возникает, если сервер временно не может обработать запрос из-за перегрузки или обслуживания. Проще говоря, когда сервер не может предоставить запрашиваемый ресурс или функцию в данный момент времени.

Эта ошибка может быть вызвана различными причинами, включая такие, как:

1. Перегрузка сервера из-за высокой нагрузки – это может быть связано с большим количеством запросов или неэффективной работой приложения.
2. Проблемы с обслуживанием сервера – например, обновление программного обеспечения или настройка сервера и ряд других специфических причин.
3. Если используется связь с удалённым сервером, убедитесь, что она стабильная, а тайм-аут ожидания ответа невысокий.
4. Проверьте, не слишком ли активно посещают ваш сайт поисковые роботы. Если это имеет место быть, ограничьте их активность.
5. Удалите тяжёлые или вовсе ненужные плагины и компоненты.
6. Если возможно, оптимизируйте подгрузку файлов сайта, чтобы снизить число запросов.
7. Организуйте передачу больших статичных файлов напрямую, а не через скрипты.
8. Оптимизируйте почтовую рассылку: распределяйте отправку писем по времени, запускайте рассылку в часы наименьшей нагрузки.
9. Оптимизируйте SQL-запросы, выявите самые медленные из них с помощью лог-файлов.

Самой частой причиной возникновения 503 ошибки, пожалуй, является большое количество запросов к сайту, из-за чего серверу не хватает ресурсов на их обработку.

Как показывает практика, чаще всего настолько большое количество запросов к сайту обычно вызвано DDOS-атакой, цель которой, собственно, вывести сервер из строя большим количеством запросов за короткий промежуток времени.

Для защиты от DDOS-атаки можно проанализировать логи доступа веб-сервера и заблокировать мусорные запросы на стороне веб-сервера по какому-либо паттерну (чаще всего атаки идут из какой-то конкретной страны или имеют один и тот же user-agent) либо подключить сервисы для защиты от DDOS-атак – например, Cloudflare или DDoS-Guard.

В ispmanager есть готовые интеграции с Cloudflare и DDoS-Guard, подключить их можно в разделе «Модули». **Данная возможность недоступна на услуге виртуального хостинга.** Вы можете заказать виртуальный/выделенный сервер и панель ISPmanager 6. Там будут доступны все возможности.

Ошибка 504 Gateway Timeout (Шлюз не отвечает)

Ошибка 504 Gateway Timeout – это ошибка, которая возникает при попытке установить соединение между клиентом и сервером, если сервер не отвечает в установленный временной интервал (который и называется тайм-аутом).

Иными словами, такая ошибка появляется, когда сервер не может обработать запрос в заданное время и не возвращает запрашиваемую информацию – ведь, как известно, время обработки запросов и в целом ресурсы любого сервера ограничены.

Есть две ситуации, из-за которых может возникнуть 504 ошибка:

1. Запросы к серверу должны обрабатываться в течение определенного длительного промежутка времени, но ограничение времени обработки запроса на веб-сервере меньше времени обработки самого запроса.

Такая ситуация часто встречается на различных виртуальных хостингах или в случае некорректной настройки веб-сервера. Если вы самостоятельно администрируете сервер, то для решения этой проблемы нужно увеличить время обработки запроса в конфигурационном файле веб-сервера. Если вы используете виртуальный хостинг, то в большинстве случаев у вас не будет доступа к конфигурационным файлам веб-серверов и для увеличения тайм-аута будет необходимо обратиться в техподдержку хостинга.

2. Обычно запросы к серверу обрабатываются быстро, но по каким-либо причинам они начали обрабатываться долго.

Причины могут быть самыми разными – например, долгое выполнение запросов к базе данных из-за слишком большого их количества или проблемы на стороннем сервере, к которому обращается сайт при обработке запроса. В данной ситуации

лучше всего заняться полной диагностикой работы сайта, чтобы точно определить причины проблемы. Также диагностику могут произвести сторонние специалисты, а справиться с выявленной проблемой поможет техподдержка хостинга, которым вы пользуетесь.

Версия #2

Кирилл создал 9 ноября 2023 08:19:46

Кирилл обновил 9 ноября 2023 10:46:57