**<https://www.100sp.ru/vladivostok>**

* Вкладка новинки

# Response

**x-powered-by -**  указывает платформу приложений, на которой работает сервер

**content-security-policy** - дополнительный уровень безопасности, позволяющий распознавать и устранять определённые типы атак.

**x-frame-options -** при помощи данного заголовка можно защититься от так называемого Кликджекинга [Clickjacking].

**alt-svc** - позволяет серверу определить альтернативный способ обращения к сайту и проинструктировать браузер о необходимости перенаправить запрос на новый хост, например, для балансировки нагрузки.

**content-length** - указывает размер отправленного получателю тела объекта в байтах

**vary** – определяет, как сопоставить будущие заголовки запроса, чтобы решить, можно ли использовать кешированный ответ, а не запрашивать новый с исходного сервера.

**strict-transport-security** - заголовок ответа, позволяющий web-сайтам уведомить браузер о том, что доступ к ним должен быть осуществлён только посредством HTTPS вместо HTTP.

**etag** - является идентификатором специфической версии ресурса. Он позволяет более эффективно использовать кеш и сохраняет пропускную способность, позволяя серверу отправлять не весь ответ, если содержимое не изменилось

**expires** - содержит дату/время, по истечении которой ответ сервера считается устаревшим.

**last-modified** – передает клиенту время последнего изменения документа (веб-страницы).

# Request

**accept-encoding** – список форматов сжатия данных, которые поддерживает клиент.

**accept-language** – определяет языковые предпочтения клиента (русский, английский и т.д.).

**accept** – список MIME типов, которые ожидает клиент.

**referer** – содержит URL исходной страницы, с которой был осуществлён переход на текущую страницу.

**sec-fetch-site** ­– указывает на связь между источником инициатора запроса и источником запрашиваемого ресурса.

**sec-fetch-mode** ­– указывает режим запроса.

**upgrade-insecure-requests** – отправляет на сервер сигнал, выражающий предпочтение клиента зашифрованному и аутентифицированному ответу, и что он может успешно обработать директиву CSP для небезопасных запросов на обновление.

**sec-ch-ua-mobile** – заголовок, который клиент отправляет на сервер.

**sec-fetch-dest** ­– указывает место назначения запроса.

**user-agent** – позволяет серверам и сетевым узлам идентифицировать приложение, операционную систему, поставщика и/или версию запрашивающего агента пользователя.