

Основные виды тестирования веб-приложений

Тестирование веб-приложений – это проверка работы программы на соответствие утвержденным ранее требованиям по её разработке до ввода в эксплуатацию конечному пользователю.

На сегодняшний день, специалисты по тестированию веб-сайтов применяют такие виды как:

1. **Функциональное тестирование**
2. **Тестирования удобства пользования (юзабилити)**
3. **Тестирование производительности и скорости загрузки сайта**
4. **Тестирование совместимости**
5. **Тестирование интерфейса пользователя (UI testing)**
6. **Тестирование безопасности.**

1. Тестирование Функциональности:

Функциональным тестированием проверяют работают ли все функции Веб-приложения согласно спецификации. В данном тестировании проверяют: работу имеющихся на странице ссылок, форм пользователя, файлы Cookie, проверка кода HTML и CSS и т.д.

Вид проверки	Что проверяет тестировщик
Проверка ссылок	ссылки, исходящие от всех страниц к конкретному домену; внутренние ссылки; ссылки на другие элементы, расположенные внутри страниц; ссылки для отправления электронной почты администратору или другим пользователям веб-страниц; нет ли ссылок на изолированные страницы.
Проверка форм Формы используются для получения информации от пользователей и взаимодействия с ними.	правильность работы валидации в каждом поле формы; значения полей, используемые по умолчанию; опции для создания форм, удаления, просмотра и редактирования форм (если такие имеются). <i>Пример: есть различные виды валидации, например, проверка электронной почты, финансовой информации пользователя и т.д. Все поля с валидацией нужно протестировать в ручном или автоматическом режиме.</i>
Тестирование Cookie Cookie — это небольшие файлы, хранящиеся на компьютере пользователя. Чаще всего они используются для поддержки сеансов с авторизацией.	Проверяет приложение, включая и включая cookies в опциях браузера. Проверяет, шифруются ли Cookie перед записью на компьютере. Тестирует сеансы регистрации и статистику пользователя, когда сеанс посещения сайта закончится. Проверяет влияет ли на безопасность приложения удаление файлов cookie.
Проверка HTML/CSS Для оптимизации сайта с поисковыми системами, валидация HTML/CSS особенно важна.	Проверяет сайт на наличие синтаксических ошибок в HTML-коде; проверяет доступен ли сайт для различных поисковых систем.
Тестирование базы данных Взаимодействие веб-приложения с базой данных является очень важным моментом.	Целостность данных и проводит тестирование сайта на наличие ошибок при редактировании, удалении, изменении форм или других действиях, имеющих отношение к базе данных. Проверяет, все ли запросы к базе данных выполняются правильно, данные извлекаются и обновляются должным образом.

2. Тестирование удобства использования (юзабилити сайта)

Тестирование юзабилити — это анализ взаимодействия пользователя и сайта, поиск ошибок и их устранение. При этом проверяется: легкость обучения, навигация, субъективная удовлетворенность пользователей, общий вид.

Вид проверки	Что проверяет тестировщик
Проверка навигации подразумеваются средства для просмотра страниц пользователем	Сайт должен быть простым в использовании, инструкции должны быть очень четкими и достигают ли они поставленной цели, главное меню должно быть доступно на каждой странице и оно должно быть построено в логической последовательности.
Проверка контента	Контент должен быть логичным и простым для понимания. Проверьте текст на наличие ошибок и раздражающих элементов (темных цветов в теме оформления) Контент должен быть содержательным, ссылки работать надлежащим образом, изображения соответствующего размера.
Другая информация для пользователей	Варианты поиска, карта сайта, справочные материалы и т.д. Проверьте работу всех ссылок в карте сайта. Функция «Поиск по сайту» должна помогать легко находить нужный контент.
Тестирование пользовательского интерфейса	

3. Тестирование производительности и скорости загрузки сайта.

Проводится проверка веб-приложения на способность выдерживать большие нагрузки. Проверка производительности приложения проводится на различной скорости интернета. Тест производительности можно применять для проверки масштабируемости сайта или оценки продуктивности при использовании стороннего программного обеспечения.

Вид проверки	Что проверяет тестировщик
Нагрузочное тестирование сайта -тестирование, при котором большое количество пользователей одновременно выполняют запрос к одной и той же странице.	Выдерживает ли система пиковые нагрузки?
Стрессовое тестирование — нагрузка системы, выходящая за пределы установленных лимитов.	Стрессовое тестирование выполняется с целью достичь сбоя в работе сайта или веб-приложения путем увеличения нагрузки. А также проверить, как система реагирует на стресс, и как она восстанавливается после сбоев. Стрессовой нагрузке подвергают поля для ввода информации, входа и регистрации.
аb тестирование функциональности	проверка на ошибки, связанные с оперативной памятью.
Скорость соединения — Сплит тестирование сайта при использовании различных вариантов интернет-соединения: через модем, ISDN и т.д.	Тестирование нагрузки: количество пользователей, одновременно посещающих сайт; проверка работы системы при пиковых нагрузках; пользователь осуществляет доступ к большому количеству данных. Стрессовая нагрузка: Непрерывная нагрузка, производительность памяти, процессора, обработки файлов и т. д. Проверка, правильности осуществления связи с сервером. Проверка совместимости сервера с используемым программным обеспечением, аппаратными средствами, сетью и базой данных.

4. Тестирование совместимости.

В данном виде тестирования проверяется кроссбраузерность, совместимость с ОС, работа в мобильных устройствах и функции печати.

Вид проверки	Что проверяет тестировщик
Совместимость с браузерами Работа некоторых веб-приложений зависит от типа браузера. Сайт должен быть совместим с различной конфигурацией и параметрами разнообразных браузеров. Верстка сайта должна быть кроссбраузерной. При использовании Java-скриптов и AJAX, обеспечивающего функциональность пользовательского интерфейса, проверки безопасности или валидации создают большую нагрузку на систему.	Проверяет работу веб-приложения в браузерах Internet Explorer, Firefox, Netscape Navigator, AOL, Safari, Opera разных версий.
Совместимость с операционными системами Некоторые функции веб-приложения могут быть несовместимы с определенными операционными системами. Не во всех из них поддерживаются новые технологии, используемые в веб-разработке.	Проверяет работу приложения в Windows, Unix, MAC, Linux, Solaris и их различных версиях.
Просмотр на мобильных устройствах	проверяет, как просматриваются веб-страницы с помощью мобильных браузеров. Проблемы с совместимостью также могут возникнуть из-за мобильных устройств. Также не стоит забывать о тестировании сайта на разных разрешениях экрана.
Параметры печати Если предусмотрена возможность печати страницы	проверяет, что шрифты, выравнивание, графика и т. д. отображаются на бумаге должным образом. Страницы должны подходить под размеры, которые устанавливаются в опциях печати.

5. Тестирование интерфейса пользователя (UI testing)

Цель тестирования проверить правильно ли осуществляется связь с сервером: совместимость сервера с используемым программным обеспечением, аппаратными средствами, сетью и базой данных.

Вид проверки	Что проверяет тестировщик
Интерфейсы веб-сервера и приложения	Что происходит, когда пользователь прерывает какое-либо действие. А также, что происходит при повторном подключении к серверу в ходе выполнения какой-либо операции.
Интерфейсы сервера базы данных и сервера приложения	Если база данных или веб-сервер для какого-либо запроса, исходящего от сервера приложения, возвращает сообщение об ошибке, сервер приложения должен фиксировать его и отображать пользователю.

6. Тестирование безопасности

Тестирование безопасности системы проводится с целью поиска потенциальных уязвимостей и их последующее устранение. Принципами безопасности ПО являются: целостность и доверие - гарантия того что сайт не может меняться под действием третьих лиц,

конфиденциальность, повреждение и восстановление - возможность восстановления данных приложения или данных авторизованных пользователей.

Тестирование безопасности включает в себя:

проверку аутентификации, проверка доступа к защищенным страницам, каталогам и файлам (не должны быть доступны напрямую, если для них не предусмотрена возможность скачивания), загрузку файлов без соответствующего доступа, раскрытие защищенных данных, ссылка на небезопасный прямой объект, тайм-аут сеанса после длительного бездействия пользователя, проверку полей CAPTCHA, и многое другое.