Основные виды тестирования сайта

1. Тестирование функциональности;
2. Тестирование удобства использования;
3. Тестирование интерфейса;
4. Тестирование совместимости;
5. Тестирование производительности и скорости загрузки сайта;
6. Тестирование безопасности.
7. Тестирование функциональности

Проверьте все ссылки, присутствующие на веб-странице, а также ссылки на базы данных, формы, используемые для подтверждения действий и получения информации от пользователей, файлы Cookie и т.д.

* 1. Проверьте все ссылки
* Проверьте 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.
* Проверьте, нет ли ссылок на изолированные страницы.
  1. Проверьте формы

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)
  1. Тестирование файлов cookie

Cookie — это небольшие файлы, хранящиеся на компьютере пользователя. Чаще всего они используются для поддержки сеансов с авторизацией. Проверьте приложение, выключая и включая cookies в опциях браузера.

Проверьте, шифруются ли Cookie перед записью на компьютере. Протестируйте сеансы регистрации и статистику пользователя, когда сеанс посещения сайта закончится. Проверьте, влияет ли на безопасность приложения удаление файлов cookie.

* 1. Проверьте HTML/CSS

Если вы оптимизируете сайт для поисковых систем, то валидация HTML/CSS особенно важна. Первым делом проверьте сайт на наличие синтаксических ошибок в HTML-коде. Проверьте, доступен ли сайт для различных поисковых систем.

* 1. Тестирование базы данных

Взаимодействие веб-приложения с базой данных является очень важным моментом. Проверьте целостность данных и проведите тестирование сайта на наличие ошибок при редактировании, удалении, изменении форм или других действиях, имеющих отношение к базе данных.

Проверьте, все ли запросы к базе данных выполняются правильно, данные извлекаются и обновляются должным образом.

При тестировании функциональности сайтов нужно проверить:

* 1. Ссылки

1. Внутренние ссылки;
2. Внешние ссылки;
3. Ссылки на электронную почту;
4. Битые ссылки.
   1. Формы
5. Валидация полей;
6. Сообщения об ошибке при неверном вводе;
7. Обязательные и необязательные к заполнению поля.
8. Тестирование удобства использования

Тестирование юзабилити — это анализ взаимодействия пользователя и сайта, поиск ошибок и их устранение.

При этом проверяется:

* Легкость обучения;
* Навигация;
* Субъективная удовлетворенность пользователей;
* Общий вид.

2.1. Проверка навигации

Под навигацией подразумеваются средства для просмотра страниц пользователем. Это кнопки, блоки. А также то, как посетитель сайта использует ссылки на другие страницы.

Проверка юзабилити:

* Сайт должен быть простым в использовании;
* Инструкции должны быть очень четкими;
* Проверьте, достигают ли предоставленные инструкции поставленной цели;
* Главное меню должно быть доступно на каждой странице;
* Главное меню должно быть построено в логической последовательности.

2.2. Проверка контента

Контент должен быть логичным и простым для понимания. Проверьте текст на наличие ошибок. Применение темных цветов раздражает пользователей, не нужно использовать их в теме оформления.

Для контента и фона страницы лучше применять общепринятые стандарты, чтобы цвет шрифта, рамок и т.д. не раздражал пользователей.

Контент должен быть содержательным, ссылки работать надлежащим образом, изображения соответствующего размера. Это основные стандарты, соблюдаемые при веб-разработке. Ваша задача — проверить все в рамках тестирования пользовательского интерфейса.

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.

1. Тестирование интерфейса

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

Основные интерфейсы:

* Интерфейсы веб-сервера и приложения.
* 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.

Проверьте, что происходит, когда пользователь прерывает какое-либо действие. А также, что происходит при повторном подключении к серверу в ходе выполнения какой-либо операции.

1. Тестирование совместимости

Нужно проверить:

* Совместимость с браузерами;
* Совместимость с операционными системами;
* Просмотр на мобильных устройствах;
* Параметры печати.

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.

Проверьте 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. Поэтому проверьте работу приложения в Windows, Unix, MAC, Linux, Solaris и их различных версиях.

Просмотр на мобильных устройствах

Проведите тестирование сайта на мобильных устройствах и проверьте, 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.

Параметры печати

Если вы предусматриваете возможность печати страницы, удостоверьтесь, что шрифты, выравнивание, графика и т. д. отображаются на бумаге должным образом. Страницы должны подходить под  размеры, которые устанавливаются в опциях печати.

1. Тестирование производительности сайта

Тестирование производительности сайта или веб-приложения должно включать в себя:

* Нагрузочное тестирование.
* Стрессовое тестирование.

Проверьте производительность приложения на различной скорости интернета.

Нагрузочное тестирование сайта (веб-приложения)  — это 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.

ab тестирование функциональности также включает в себя проверку на ошибки, связанные с оперативной памяти.

Тест производительности можно применять для проверки масштабируемости сайта  или оценки продуктивности при использовании стороннего программного обеспечения.

**Скорость соединения**

Сплит тестирование сайта при использовании различных вариантов интернет-соединения: через модем, ISDN и т.д.

**Нагрузка**

1. Количество пользователей, одновременно посещающих сайт;
2. Проверьте работу системы при пиковых нагрузках;
3. Пользователь осуществляет доступ к большому количеству данных.

**Стрессовая нагрузка**

1. Непрерывная нагрузка;
2. Производительность памяти, процессора, обработки файлов и т. д.

6. Тестирование безопасности

Ниже приведены некоторые наборы для тестирования веб-безопасности:

* Проверка с помощью вставки внутреннего URL в адресную строку браузера без авторизации. Внутренние страницы при этом не должны открываться.
* После авторизации с помощью логина и пароля, а также просмотра внутренних страниц попробуйте изменять URL. Например, вы проверяете какую-то статистику сайта под идентификатором ID= 123. Попробуйте изменить ID URL на другой ID сайта, который не имеет отношения к авторизованному пользователю. В любом случае доступ этого пользователя к просмотру других показателей должен быть запрещен.
* Попробуйте ввести неверные данные в поля формы для авторизации. Выясните, как система реагирует на ввод недопустимых данных.
* Каталоги или файлы не должны быть доступны напрямую, если для них не предусмотрена возможность скачивания.
* Проверьте работу капчи для защиты от автоматического входа с помощью программного кода.
* Проверьте, используется ли в целях безопасности SSL. Если да, то должно отображаться сообщение при переходе пользователя с незащищенных HTTP-страниц к защищенным и наоборот.
* Все операции, сообщения об ошибках, нарушения безопасности должны записываться в файл журнала на веб-сервере.

Основной причиной тестирования безопасности сайта является поиск потенциальных уязвимостей и их последующее устранение.

* Сетевое сканирование;
* Сканирование уязвимостей;
* Возможность потенциального взлома паролей;
* Обзор журнала;
* Средства для проверки целостности;
* Обнаружение вирусов.