МЕТОДЫ И ИНСТРУМЕНТЫ ПРОВЕРКИ КАЧЕСТВА И БЕЗОПАСНОСТИ ВЕБ-САЙТОВ: ЭКСПЕРТНЫЙ И АВТОМАТИЗИРОВАННЫЙ АУДИТ

Иванова Г.Р., старший преподаватель

Минибаева К.А., студент

ФГБОУ ВО Башкирский ГАУ, г. Уфа, Россия

Аннотация. В статье разбираются направления проверки веб-сайтов (функциональность, удобство использования, производительность, доступность, безопасность, соответствие нормативным требованиям) и круг тех, кто этим занимается: внутренние тестировщики, заказчик, независимые аудиторы, поисковые системы, регулирующие органы и сами пользователи. Сопоставлены сильные и слабые стороны автоматизированного и ручного подходов. Предложен порядок комбинированного аудита, в котором массовую проверку берёт на себя автоматика, а содержательную оценку и интерпретацию результатов выполняет эксперт.

Ключевые слова: веб-сайт, аудит сайта, тестирование, качество, информационная безопасность, доступность, автоматизация проверки.

Автор: Иванова Г.Р., Минибаева К.А.
01.06.2026 11:57 -

Современный веб-сайт это уже не статичная визитка, а полноценный программный продукт. От его устойчивой работы зависят выручка компании, её репутация и правовая защищённость. Сайт государственного учреждения, интернет-магазина или сервисной компании каждый день обрабатывает обращения пользователей и персональные данные, поэтому качество и безопасность сайта это уже не только техника, но и право, и организационная сторона дела. Проверка веб-сайтов давно оформилась в отдельный вид работы со своими методами, инструментами и составом участников.

Спрос на проверку растёт вместе с цифровизацией государственного сектора и числом сайтов, через которые проходят юридически значимые операции. Для студии, которая делает и сопровождает сайты, навык проверки часть основной работы: от качества и безопасности сданного продукта зависит и удовлетворённость заказчика, и репутация компании. В статье разбираются виды проверки, круг тех, кто её выполняет, нормативные требования и возможности двух подходов: автоматизированного и ручного.

Виды проверки веб-сайта

Проверку веб-сайта удобно рассматривать как набор относительно самостоятельных направлений: каждое отвечает на свой вопрос о состоянии ресурса. Функциональная проверка показывает, корректно ли работают сценарии использования: регистрация, оформление заказа, отправка формы обратной связи. Здесь применяют и заранее описанные тест-кейсы, и исследовательское тестирование, в котором специалист изучает поведение системы без жёсткого сценария [2; 3].

Проверка удобства использования отвечает по сути на бытовой вопрос: легко ли пользователь добирается до своих целей. Понятна ли навигация? Очевидны ли элементы управления? Не путается ли он на ключевых шагах? Проверка производительности измеряет скорость загрузки страниц и устойчивость к нагрузке: медленный отклик прямо снижает конверсию и ухудшает позиции в поисковой выдаче [6]. Отдельное направление, проверка доступности, оценивает, насколько ресурс пригоден для людей с ограничениями жизнедеятельности; для государственных и многих коммерческих сайтов эти требования закреплены национальным стандартом [1] и согласуются с международными рекомендациями [7].

Проверка безопасности ищет уязвимости, через которые возможны несанкционированный доступ, искажение содержимого или утечка данных. Для сайтов, обрабатывающих персональные данные, к технической стороне добавляется проверка соответствия требованиям законодательства [5]. Соответствие направлений проверки конкретным характеристикам и инструментам показано в таблице 1.

Таблица 1. Направления проверки веб-сайта и типовой инструментарий

Направление	**Проверяемые характеристики**	**Типовые инструменты и методы**

Функциональное
Корректность пользовательских сценариев
Тест-кейсы, исследовательское тестирование
Удобство использования
Навигация, понятность интерфейса
Эвристическая оценка, юзабилити-тестирование
Производительность
Скорость загрузки, устойчивость к нагрузке
Браузерные аудиторы, нагрузочное тестирование
Доступность

Пригодность для лиц с ограничениями

Проверка по ГОСТ Р 52872 и	WCAG	, программы экранного доступа

Безопасность

Уязвимости, защита данных

Сканеры уязвимостей, ручной анализ	OWASP, перечень

Круг тех, кто проверяет сайты, шире, чем принято думать. Внутри компании-разработчика этим занимаются специалисты по тестированию: проверка встроена в процесс разработки и идёт ещё до сдачи продукта заказчику. На стороне заказчика проверку проводят при приёмке: сверяют результат с техническим заданием, при необходимости подключают независимых экспертов или специализированные студии аудита.

Отдельная группа это автоматические сервисы и поисковые системы. Поисковые роботы непрерывно оценивают сайты по множеству показателей: скорости, мобильной адаптивности, безопасности соединения. По сути, они выступают постоянным внешним контролёром и напрямую влияют на видимость ресурса. К проверке причастны и регулирующие органы: в отношении сайтов, работающих с персональными данными, контроль соблюдения законодательства осуществляет уполномоченный надзорный орган [5]. Не последнюю роль играют сами пользователи и независимые исследователи безопасности, которые находят ошибки в ходе эксплуатации и сообщают о них владельцу, в том числе в рамках программ поощрения за найденные уязвимости.

Заметная часть аудита это проверка соответствия требованиям нормативных правовых актов и стандартов. Для ресурсов, которые собирают сведения о пользователях, главную роль играет законодательство о персональных данных [5]. Оно предписывает получение согласия на обработку, публикацию политики и применение мер защиты. Несоблюдение этих требований ведёт к правовым последствиям независимо от технического качества сайта, поэтому такая проверка идёт наравне с функциональной и нагрузочной.

Для государственных информационных ресурсов и социально значимых сайтов обязательной становится проверка доступности по национальному стандарту [1], близкому к международным рекомендациям [7]. Сюда входят текстовые альтернативы к изображениям, достаточный цветовой контраст, возможность управления с клавиатуры и совместимость с программами экранного доступа. Эта проверка во многом экспертная: автоматические средства видят только формальные нарушения, а пригодность для реального пользователя оценивает только специалист.

Инструменты проверки делят на средства автоматизации и методы экспертной (ручной) оценки. Автоматика быстро и одинаково точно обрабатывает большой объём проверок. Для производительности, доступности и базовых технических параметров применяют браузерные аудиторы. Корректность разметки проверяют валидаторами консорциума W
3
C
. Для поиска типовых уязвимостей используют сканеры безопасности, ориентированные на распространённые классы дефектов из признанных отраслевых перечней [4]. Сильная сторона автоматики это скорость, повторяемость и независимость результата от субъективного мнения проверяющего.

У автоматики есть и серьёзные ограничения. Инструмент видит формальное нарушение, но не оценивает смысл: он не скажет, удобна ли формулировка кнопки, логичен ли порядок шагов в оформлении заказа, соответствует ли содержание ожиданиям пользователя. Сканеры безопасности дают ошибки двух родов: ложные срабатывания и пропуски уязвимостей, которые требуют понимания бизнес-логики приложения. Поэтому ручная экспертная проверка остаётся незаменимой там, где нужна интерпретация, а не формальное сравнение с эталоном [2; 6]. Сопоставление подходов по нескольким критериям приведено в таблице 2.

Таблица 2. Сопоставление автоматизированного и экспертного подходов

Критерий	**Автоматизированный подход**	**Экспертный (ручной) подход**
Скорость	Высокая	Низкая
Воспроизводимость		

Высокая
Зависит от специалиста
Охват рутинных проверок
Широкий
Ограниченный
Оценка смысла и контекста
Практически отсутствует
Высокая
Характерные ошибки
Ложные срабатывания, пропуски
Субъективность оценки

Стоимость масштабирования

Низкая

Высокая

Результат проверки приобретает практическую ценность только тогда, когда найденные недостатки упорядочены по значимости. Каждому дефекту присваивают уровень критичности (тяжесть последствий) и приоритет устранения (срочность с точки зрения бизнеса). Уязвимость, открывающая доступ к персональным данным, и опечатка в подписи к картинке формально считаются дефектами, но реакция на них должна быть совершенно разной. Разделение тяжести и приоритета помогает разумно распределить ресурсы на исправление.

Если свести вместе сильные стороны обоих подходов, получается комбинированный аудит. Сначала автоматика снимает массовую и рутинную часть работы: производительность, корректность разметки, наличие типовых уязвимостей, базовую доступность. Дальше эксперт интерпретирует данные, отсеивает ложные срабатывания и проверяет то, что недоступно автоматике: удобство ключевых сценариев, логику бизнес-процессов, осмысленность содержания и соответствие правовым требованиям к обработке данных. Итог сводится в один отчёт с приоритизацией дефектов.

Проверка веб-сайта это работа сразу по нескольким направлениям: функциональность, удобство использования, производительность, доступность, безопасность и

соответствие нормативным требованиям. Её ведут самые разные участники: разработчик, заказчик, автоматические сервисы, поисковые системы и надзорные органы. У автоматики и ручной экспертизы разные сильные стороны: первая даёт скорость и повторяемость, вторая берёт на себя понимание контекста и смысла. Комбинированный аудит, при котором они работают по очереди, а итог попадает в общий отчёт с приоритизацией дефектов, даёт реалистичную и применимую на практике оценку качества и безопасности ресурса.

Литература

1. ГОСТ Р 52872-2019. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности. М.: Стандартинформ, 2019. 30 с.

2. Канер С., Фолк Дж., Нгуен Е.К. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений: пер. с англ. К.: ДиаСофт, 2001. 544 с.

3. Куликов С.С. Тестирование программного обеспечения. Базовый курс. 3-е изд. Минск: Четыре четверти, 2020. 312 с.

4. Нильсен Я., Лоранжер Х. Web-дизайн: удобство использования веб-сайтов: пер. с англ. М.: Вильямс, 2009. 368 с.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм. и доп.) [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 14.05.2026).

6. OWASP Top 10: The Ten Most Critical Web Application Security Risks [Электронный ресурс] // OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 14.05.2026).

7. Web Content Accessibility Guidelines (WCAG) 2.1 [Электронный ресурс] // World Wide Web Consortium (W3C). URL: https://www.w3.org/TR/WCAG21/ (дата обращения: 14.05.2026).