Отчёт по 152-ФЗ

Проверка сайта на соответствие требованиям закона о персональных данных

Домен
demo-shop152.ru
Адрес скана
https://demo-shop152.ru/

Тип скана
Полный (платно)
Дата отчёта
12.05.2026 16:18

54
из 100

Есть существенные нарушения

Проверок: 35 · OK: 15 · нарушений: 12

Потенциальные штрафы по выявленным нарушениям

67 000 ₽ — 2 924 000 ₽

по статье 13.11 КоАП РФ. Размер взыскания определяет надзорный орган.

Детализация проверок

Юридические (12)

НАРУШЕНИЕ

Cookie-баннер с уведомлением показан до сбора cookies

Уровень: критическое · КоАП 13.11 ч.6 · штраф до 150 000 ₽

Метрика стартует до согласия пользователя · найдено: mc.yandex.ru/metrika/tag.js

Что делать: Установите cookie-баннер, который блокирует Метрику/GA до согласия.

✕ Как это выглядит сейчас: Сайт сразу подгружает Метрику/_ym/_ga без баннера согласия — пользователь не успевает отказаться.

✓ Как должно быть: До первого визита показывается баннер: «Мы используем cookie. [Принять] [Отказаться] [Настроить]» + ссылка на политику.

НАРУШЕНИЕ

На форме обратной связи есть чекбокс согласия на обработку ПД

Уровень: критическое · КоАП 13.11 ч.1 · штраф до 700 000 ₽

На форме /contact нет чекбокса согласия · https://demo-shop152.ru/contact

Что делать: Добавьте обязательный чекбокс согласия с ссылкой на политику ПД ко всем формам.

✕ Как это выглядит сейчас: <form><input name="email"><button>Отправить</button></form> — нет чекбокса согласия.

✓ Как должно быть: <input type="checkbox" name="consent" required> Я согласен на обработку персональных данных

НАРУШЕНИЕ

В политике указан контакт ответственного за ПД

Уровень: важное · ФЗ-152 ст.22.1 · штраф до 3 000 ₽

В политике нет email ответственного за ПД

Что делать: Назначьте ответственного за обработку ПД и укажите его email в политике.

✕ Как это выглядит сейчас: В политике нет ФИО/email/телефона ответственного за обработку ПД.

✓ Как должно быть: «Ответственное лицо: Иванов И.И., privacy@company.ru, +7 495 000-00-00».

НАРУШЕНИЕ

Срок хранения ПД указан

Уровень: важное · КоАП 13.11 ч.1 · штраф до 6 000 ₽

Срок хранения ПД не указан в политике

Что делать: Укажите срок хранения для каждой категории ПД.

✕ Как это выглядит сейчас: Срок хранения ПД в политике не указан.

✓ Как должно быть: «Срок хранения: до отзыва согласия, но не более 5 лет с последнего обращения».

НАРУШЕНИЕ

Порядок запроса субъекта (DSR) прописан

Уровень: важное · КоАП 13.11 ч.5 · штраф до 5 000 ₽

Нет описания, как получить/удалить свои ПД

Что делать: Опишите как субъект может запросить/удалить/получить копию своих ПД.

✕ Как это выглядит сейчас: Нет порядка, как субъект ПД может запросить свои данные или их удаление.

✓ Как должно быть: «Чтобы запросить/удалить данные — email на privacy@company.ru с копией паспорта. Ответ в течение 30 дней».

НАРУШЕНИЕ

Раскрытие о трансграничной передаче (если есть Метрика/GA)

Уровень: важное · КоАП 13.11 ч.10 · штраф до 600 000 ₽

На сайте подключён Google Analytics, но в политике нет упоминания трансгран. передачи · найдено: google-analytics.com, googletagmanager.com

Что делать: Добавьте в политику раздел о трансграничной передаче ПД в указанные сервисы.

✕ Как это выглядит сейчас: На сайте стоит Google Analytics, но в политике нет упоминания трансграничной передачи в США.

✓ Как должно быть: В политике: «Google Analytics обрабатывает данные на серверах в США. Список стран: США, ЕС».

ВНИМАНИЕ

Оператор уведомил РКН об обработке ПД

Уровень: важное · КоАП 19.7

manual_review_required · Проверьте в реестре операторов pd.rkn.gov.ru

Что делать: Подайте уведомление через pd.rkn.gov.ru — без него оператор обязан только в порядке исключения.

ВНИМАНИЕ

Согласие на рассылку отдельно от согласия на обработку ПД

Уровень: важное · ФЗ-38 ст.18

Один чекбокс на ПД и рассылку — нужно разделить

Что делать: Сделайте маркетинговое согласие отдельным чекбоксом, не объединяйте с согласием на ПД.

ВНИМАНИЕ

Договор поручения обработки с процессорами (DPA)

Уровень: рекомендуемое · ФЗ-152 ст.6 ч.3

manual_review_required · Проверьте наличие DPA с email-сервисом и хостингом

Что делать: Подпишите DPA с подрядчиками (Beget, CRM) и перечислите их в политике.

OK

Политика обработки персональных данных опубликована

Уровень: критическое · КоАП 13.11 ч.1

OK

Цели обработки ПД прописаны

Уровень: важное · КоАП 13.11 ч.1

OK

Условия использования / оферта опубликованы

Уровень: рекомендуемое · ГК РФ ст.435

Технические (15)

НАРУШЕНИЕ

Базовые security headers (CSP, X-Frame, HSTS, Referrer)

Уровень: рекомендуемое · —

Не настроены CSP и Strict-Transport-Security · нет: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options

Что делать: Включите security-headers через helmet или конфиг nginx.

✕ Как это выглядит сейчас: Нет заголовков Content-Security-Policy, X-Frame-Options, Strict-Transport-Security.

✓ Как должно быть: CSP: default-src 'self'; X-Frame-Options: SAMEORIGIN; HSTS: max-age=31536000.

НАРУШЕНИЕ

Метрика/GA загружаются только после согласия

Уровень: критическое · КоАП 13.11 ч.6 · штраф до 150 000 ₽

Yandex Metrika и GA загружаются в <head> без проверки согласия · найдено: _ym, gtag('config'

Что делать: Включите блокировку аналитики до клика по «Принимаю» в cookie-баннере.

✕ Как это выглядит сейчас: В <head> сразу: <script src="mc.yandex.ru/metrika/tag.js"></script> — счётчик стартует до согласия.

✓ Как должно быть: Метрика подключается только в коллбэке after-consent: if (cookieConsent.granted) loadMetrika();

НАРУШЕНИЕ

Сервер для хранения ПД физически в РФ

Уровень: важное · ФЗ-152 ст.18 ч.5 · штраф до 600 000 ₽

IP сервера в Германии (Hetzner); в политике нет записи о трансграничной передаче · IP 88.99.x.x · страна: DE

Что делать: Перенесите хранение ПД на сервер в РФ (Beget, Timeweb, Yandex Cloud).

✕ Как это выглядит сейчас: Сервер хостится в US/EU, но ПД граждан РФ — без записи о трансграничной передаче.

✓ Как должно быть: Основная БД ПД на серверах в РФ (Selectel, Beget, Yandex.Cloud), либо корректная отметка о трансгран. передаче.

ВНИМАНИЕ

robots.txt закрывает приватные пути

Уровень: рекомендуемое · —

В robots.txt нет Disallow для /admin/ и /api/

Что делать: Добавьте Disallow для административных и личных кабинетов в robots.txt.

ВНИМАНИЕ

Сторонние скрипты учтены в политике

Уровень: рекомендуемое · КоАП 13.11 ч.1

Найдено 4 сторонних скрипта; в политике упомянуты только 2 · найдено: mc.yandex.ru, gtag, jivo.ru

Что делать: Перечислите все сторонние сервисы в политике ПД.

ВНИМАНИЕ

CMS и плагины обновлены (нет известных CVE)

Уровень: рекомендуемое · —

WordPress 6.1 (актуально 6.4); 2 плагина устарели

Что делать: Обновите CMS и критичные плагины до актуальных версий.

ОК

Сайт принудительно работает по HTTPS

Уровень: критическое · КоАП 13.11 ч.4

ОК

SSL-сертификат валиден и не истекает в ближайшие 30 дней

Уровень: критическое · КоАП 13.11 ч.4

SSL осталось 67 дн.

OK

Формы отправляют данные по HTTPS

Уровень: критическое · КоАП 13.11 ч.4

OK

В sitemap нет ссылок с ПД (email/телефон в query string)

Уровень: важное · КоАП 13.11 ч.4

OK

Админ-URL не торчат публично без 2FA

Уровень: критическое · КоАП 13.11 ч.4

OK

На HTTPS-страницах нет mixed-content (HTTP-картинок/скриптов)

Уровень: рекомендуемое · —

OK

В публичных файлах нет email/телефонов админов

Уровень: важное · КоАП 13.11 ч.4

OK

Listing директорий отключён

Уровень: важное · —

OK

Все страницы с формами доступны только по HTTPS

Уровень: критическое · КоАП 13.11 ч.4

Поведенческие (8)

НАРУШЕНИЕ

Чекбокс согласия не отмечен по умолчанию

Уровень: критическое · ФЗ-152 ст.9 ч.4 · штраф до 700 000 ₽

Чекбокс согласия отмечен по умолчанию (checked) · https://demo-shop152.ru/checkout

Что делать: Снимите атрибут checked — пользователь должен явно согласиться.

✕ Как это выглядит сейчас: <input type="checkbox" name="consent" checked> — галочка стоит по умолчанию.

✓ Как должно быть: <input type="checkbox" name="consent"> — пользователь сам ставит галочку (ст. 9 152-ФЗ требует активного согласия).

НАРУШЕНИЕ

Есть способ удалить аккаунт (видимая кнопка/инструкция)

Уровень: важное · КоАП 13.11 ч.5 · штраф до 5 000 ₽

В личном кабинете нет кнопки удаления аккаунта

Что делать: Добавьте кнопку удаления аккаунта в личный кабинет.

✕ Как это выглядит сейчас: В кабинете нет кнопки «удалить аккаунт» — пользователь не может реализовать право на забвение.

✓ Как должно быть: Профиль → «Удалить аккаунт» с подтверждением → данные стираются за 30 дней (ст. 21 152-ФЗ).

НАРУШЕНИЕ

Email для DSR-запросов виден на политике/контактах

Уровень: важное · КоАП 13.11 ч.5 · штраф до 5 000 ₽

На страницах /privacy и /contacts нет email для DSR

Что делать: Создайте алиас privacy@домен и опубликуйте его в политике.

✕ Как это выглядит сейчас: На страницах /privacy и /contacts нет email для запросов субъекта ПД.

✓ Как должно быть: В политике: «По запросам ПД пишите на privacy@company.ru» (обязательная видимая контактная точка).

ВНИМАНИЕ

При регистрации спрашивается возраст 14+

Уровень: рекомендуемое · ФЗ-152 ст.9 ч.1

При регистрации не спрашивается возраст 14+

Что делать: Добавьте возрастную проверку — для младше 14 нужно согласие законного представителя.

ВНИМАНИЕ

Описан способ отзыва согласия

Уровень: важное · ФЗ-152 ст.9 ч.5

В политике сказано про отзыв согласия, но без конкретного способа

Что делать: Опишите как и куда писать для отзыва согласия.

OK

Текст согласия читаем (≥12px, нормальный контраст)

Уровень: рекомендуемое · ФЗ-152 ст.9 ч.4

OK

Реквизиты юрлица/ИП опубликованы

Уровень: рекомендуемое · ФЗ-2300-1 ст.10

OK

В рассылках есть ссылка на отписку

Уровень: рекомендуемое · ФЗ-38 ст.18

О документе и юридический статус

Этот отчёт — автоматизированная техническая проверка публично доступных параметров сайта. Он не является заключением юриста и не заменяет аудит Роскомнадзора. Размеры штрафов указаны согласно действующей редакции КоАП РФ (ст. 13.11) и приведены как ориентир. Окончательный размер взыскания определяет надзорный орган.

Ограничения автоматической проверки

Сервис не даёт 100% гарантии обнаружения всех нарушений 152-ФЗ. Часть проверок может не сработать или дать ложноположительный/ложноотрицательный результат из-за специфики сайта: WAF/Cloudflare/anti-bot защиты, JS-рендеринга контента (SPA/SSR), нестандартной разметки форм и cookie-баннеров, закрытых разделов (личный кабинет, корзина, оформление заказа), кастомных решений согласия и динамической подгрузки аналитики. Также сканер видит только публичный фронтенд — внутренние процессы обработки ПД, договоры с подрядчиками, физическую/организационную защиту и серверную часть он не оценивает. Используйте отчёт как чек-лист и стартовую точку — финальную проверку и оценку соответствия должен делать DPO или юрист, специализирующийся на 152-ФЗ.