MIDNIGHT WEBS

БЕСПЛАТНЫЙ МАТЕРИАЛ · ЧЕК-ЛИСТ ПО БЕЗОПАСНОСТИ

Чек-лист безопасности перед запуском сайта

Большинство взломанных сайтов малого бизнеса пострадали не от хитрых атак. На них работал устаревший плагин, повторно использованный пароль или незащищённая админка. Этот чек-лист собирает около 40 проверок, которые закрывают такие бреши до запуска.

Обновлено в ноябре 2026 | 12 мин чтения | проверок: 48

ДЛЯ КОГО	ЧТО ОХВАТЫВАЕТ	КАК ИСПОЛЬЗОВАТЬ
Владельцы, менеджеры проектов и разработчики, готовящие запуск	8 областей: от доступа к аккаунтам до проверок в день запуска	Назначьте каждому пункту ответственного и срок; «!» отмечает пункты, которые нельзя пропускать

С ЧЕГО НАЧАТЬ

Если у вас всего час, пройдите разделы 1, 2 и 5. Двухфакторный вход, заблокированный домен и проверенная резервная копия предотвращают самые дорогие сбои.

ОТМЕТЬТЕ КВАДРАТ, КОГДА ГОТОВО · ОБЯЗАТЕЛЬНО = МАКСИМАЛЬНЫЙ ЭФФЕКТ

01 Аккаунты и доступ

Слабые или повторно используемые пароли остаются самым частым путём на сайты малого бизнеса: злоумышленники просто пробуют пароли, утёкшие из других сервисов. Начните с доступа; это и самая дешёвая часть списка.

- [ ] ОБЯЗАТЕЛЬНО **Включите двухфакторную аутентификацию везде, где это важно**
  Хостинг, регистратор домена, админка CMS, почта и аналитика. Лучше приложение-аутентификатор или passkey, чем SMS, которые можно перехватить через подмену SIM-карты.

- [ ] ОБЯЗАТЕЛЬНО **Используйте менеджер паролей и сгенерированные пароли**
  Случайные пароли от 16 символов, уникальные для каждого сервиса. Актуальные рекомендации NIST ставят длину и уникальность выше принудительных правил сложности.

- [ ] **Выдайте каждому человеку личную учётную запись**
  Общие логины не позволяют понять, кто что изменил, и убрать одного человека, не затронув остальных.

- [ ] **Применяйте принцип минимальных прав**
  Редактору нужна роль «Редактор», а не «Администратор». Оставьте администраторами только тех, кому это действительно нужно, в идеале двух-трёх человек.

- [ ] **Удалите ушедших людей и неиспользуемые аккаунты**
  Проверьте хостинг, регистратора, аккаунты Google/Meta, платёжные сервисы и список пользователей CMS. Подрядчики прошлых проектов — обычный «хвост».

- [ ] **Запишите, кому принадлежит каждый аккаунт**
  Домен, хостинг и платёжные аккаунты должны быть оформлены на компанию, а не на личную почту подрядчика. Храните коды восстановления в менеджере паролей.

КАК ПРОВЕРИТЬ

Откройте адрес админки в приватном окне: он должен запросить пароль и второй фактор. Просмотрите список пользователей и найдите незнакомые имена.

02 Домен, DNS и HTTPS

Домен управляет всем остальным. Если его перехватят, под контролем окажутся ваш сайт, почта и репутация.

- [ ] ОБЯЗАТЕЛЬНО **Заблокируйте домен и защитите аккаунт у регистратора**
  Включите блокировку переноса (registrar lock), 2FA и автопродление. Просроченный домен может зарегистрировать любой, в том числе тот, кто будет выдавать себя за вас.

- [ ] ОБЯЗАТЕЛЬНО **Отдавайте все страницы по HTTPS с автоматическим продлением**
  Браузеры требуют его для платежей и форм. Сроки жизни сертификатов сокращаются (индустрия договорилась о переходе на 200 дней с марта 2026 года, затем на 100 и 47 дней), так что ручное продление не выживет.

- [ ] **Настройте постоянный редирект (301) с HTTP на HTTPS**
  И выберите одну каноническую версию адреса — с «www» или без, чтобы сайт не существовал в двух местах.

- [ ] **Опубликуйте SPF, DKIM и DMARC для деловой почты**
  Без них мошенники могут рассылать письма от имени вашего домена, а Gmail и Yahoo могут отправлять ваши настоящие письма в спам. Начните DMARC с `p=none` и отчётов, а затем переходите к quarantine или reject, когда отчёты станут чистыми.

- [ ] **Удалите DNS-записи, которыми вы не пользуетесь**
  Старые записи, указывающие на отменённые сервисы, могут занять злоумышленники (subdomain takeover). Проверьте записи A, CNAME и MX по одной.

- [ ] **Добавьте HSTS, когда всё работает по HTTPS**

  Начните с короткого max-age, например 300 секунд, проверьте все поддомены, затем увеличьте до года. «preload» добавляйте, только если уверены, что все поддомены останутся на HTTPS.

КАК ПРОВЕРИТЬ

Проверьте домен в SSL Labs (ssllabs.com/ssltest) и выполните `dig TXT yourdomain.com` и `dig TXT _dmarc.yourdomain.com`, чтобы убедиться, что записи почты существуют.

03 Платформа, ПО и настройки сервера

Злоумышленники сканируют интернет в поисках известных уязвимостей в старом ПО. Большинство успешных атак используют брешь, для которой исправление уже было опубликовано.

- [ ] ОБЯЗАТЕЛЬНО **Обновите CMS, темы, плагины и серверные пакеты до запуска**

  Затем запланируйте обновления — для плагинов не реже раза в неделю. Включите автоматические обновления безопасности там, где платформа это позволяет.

- [ ] **Удалите всё, чем не пользуетесь**

  Отключённые плагины и темы всё равно можно взломать. Меньше компонентов — меньше обновлений и меньше поверхность атаки.

- [ ] **Уберите демо-контент, тестовых пользователей и учётные записи по умолчанию**

  Пользователь «admin» или «test» со слабым паролем — первое, что пробуют автоматические скрипты.

- [ ] ОБЯЗАТЕЛЬНО **Убедитесь, что приватные файлы не открыты**

  Попробуйте yourdomain.com `/.env`, `/.git/config`, `/backup.zip` и `/phpinfo.php`. Все должны отдавать 404 или 403, но не содержимое. Храните секреты, ключи API и дампы базы вне публичной папки.

- [ ] **Отключите листинг каталогов и редактирование файлов в админке**

  В WordPress добавьте `define('DISALLOW_FILE_EDIT', true);` в wp-config.php, чтобы украденный администраторский вход не позволял править код напрямую.

- [ ] **Добавьте стандартные заголовки безопасности**

  `X-Content-Type-Options: nosniff`, `Referrer-Policy`, защита от clickjacking (frame-ancestors или X-Frame-Options) и, когда будете готовы протестировать, Content-Security-Policy. Проверьте результат на securityheaders.com или в Mozilla Observatory.

КАК ПРОВЕРИТЬ

Составьте список всех плагинов и тем с версиями и сравните с последним релизом разработчика. Всё, что не обновлялось больше года, стоит заменить.

04 Формы, вход и платежи

Каждое поле, куда можно вводить текст, — точка входа. Считайте любой ввод враждебным, пока сервер его не проверил.

- [ ] ОБЯЗАТЕЛЬНО **Проверяйте и очищайте данные на сервере**
  Проверки в браузере нужны только для удобства; их может обойти кто угодно. Используйте параметризованные запросы против SQL-инъекций и экранируйте вывод против внедрения скриптов.

- [ ] ОБЯЗАТЕЛЬНО **Защитите публичные формы от спама и злоупотреблений**
  Используйте альтернативу CAPTCHA вроде Cloudflare Turnstile, скрытое поле-ловушку (honeypot) и ограничение частоты, чтобы боты не заваливали почту и не исчерпывали лимит отправки.

- [ ] **Добавьте защиту от CSRF и безопасные cookie**
  Сессионные cookie должны быть Secure, `HttpOnly` и `SameSite=Lax` (или Strict). Это не даёт другим сайтам незаметно выполнять действия от имени вошедшего пользователя.

- [ ] **Ограничьте загрузку файлов**
  Разрешайте только нужные типы, проверяйте реальный тип и размер, переименовывайте файлы и по возможности храните их вне публичной папки.

- [ ] **Собирайте только необходимое**
  Каждое лишнее поле — это данные, которые нужно защищать и удалять по запросу согласно GDPR. Если вы не используете телефон, не спрашивайте его.

- [ ] **Поручите платёжному провайдеру работу с данными карт**
  Используйте размещённую у провайдера оплату или поля (Stripe, PayPal, шлюз вашего банка), чтобы номера карт не попадали на ваш сервер. Это сводит требования PCI к минимуму.

КАК ПРОВЕРИТЬ

Отправьте каждую форму с очень длинной строкой, апострофом и `<b>bold</b>`. Данные должны быть приняты или чётко отклонены, а форматирование ни в коем случае не должно отображаться на странице.

05 Резервные копии и восстановление

Резервные копии защищают не только от хакеров, но и от неудачных обновлений, случайных удалений и проблем хостинга. Копия, которую вы ни разу не восстанавливали, — лишь надежда.

- [ ] ОБЯЗАТЕЛЬНО **Автоматизируйте ежедневное копирование файлов и базы данных**
  Храните историю за 14–30 дней, чтобы можно было вернуться к состоянию до начала проблемы, а не только к вчерашнему вечеру.

- [ ] ОБЯЗАТЕЛЬНО **Храните одну копию в другом месте**
  Правило 3-2-1: три копии, на двух типах носителей, одна вне основной площадки. Копия в том же хостинг-аккаунте исчезнет вместе с ним.

- [ ] **Шифруйте копии с персональными данными**
  Данные клиентов в резервной копии остаются данными клиентов по GDPR.

- [ ] **Восстановите копию в тестовой среде до запуска**
  Засеките время. Это ваше реальное время восстановления; большинство владельцев узнают его во время аварии.

- [ ] **Напишите памятку по восстановлению на одну страницу**
  Кто может восстановить, где лежат копии, как войти и кому звонить на хостинге. Храните копию, не зависящую от самого сайта.

КАК ПРОВЕРИТЬ

Возьмите вчерашнюю копию, восстановите её на тестовой версии и проверьте, что страницы, изображения и заявки из форм на месте.

06 Мониторинг и реагирование на инциденты

Взломанные сайты часто работают незамеченными неделями. Мониторинг сокращает это время до минут.

- [ ] ОБЯЗАТЕЛЬНО **Настройте мониторинг доступности с оповещениями**
  Бесплатные сервисы вроде UptimeRobot или Better Stack проверяют сайт каждые 1–5 минут и сообщают, когда он перестал отвечать.

- [ ] **Следите за сроком действия сертификата и домена**
  Настройте оповещения за 30 и за 7 дней до истечения и отправляйте их двум людям.

- [ ] **Подключите Google Search Console и проверяйте раздел «Проблемы безопасности»**
  Google сообщит, если найдёт вредоносный код или взломанный контент, зачастую раньше ваших посетителей.

- [ ] **Журналируйте неудачные входы и изменения в админке**
  Просматривайте их после запуска и настройте оповещение о повторяющихся неудачах с одного адреса.

- [ ] **Отправляйте оповещения в ящик, который кто-то читает**
  Уведомление безопасности, которое приходит бывшему сотруднику, мониторингом не является.

- [ ] **Подготовьте краткий план реагирования на инциденты**
  Кого вызывать, как перевести сайт в режим обслуживания, как сбросить все пароли и кто сообщает клиентам. По GDPR о нарушении безопасности персональных данных нужно уведомить надзорный орган в течение 72 часов с момента, когда вы узнали.

КАК ПРОВЕРИТЬ

Ненадолго остановите сайт в тестовой среде или направьте монитор на неверный адрес. Убедитесь, что оповещение пришло, и узнайте, кому именно.

07 Конфиденциальность и юридические основы

Сбор данных создаёт обязательства. Сайт, который собирает меньше и понятно объясняет, безопаснее и легче защищается.

- [ ] ОБЯЗАТЕЛЬНО **Опубликуйте политику конфиденциальности, соответствующую действительности**
  Перечислите, что вы собираете, зачем, кто получает данные (аналитика, почтовый сервис, платёжный процессор) и как долго вы их храните.

- [ ] ОБЯЗАТЕЛЬНО **Запрашивайте согласие на cookie до загрузки необязательных**
  Аналитика, реклама и пиксели отслеживания не должны загружаться, пока посетитель не согласился, если у вас есть посетители из ЕС или Великобритании. Обязательные cookie (вход, корзина) согласия не требуют.

- [ ] **Заключите соглашения об обработке данных с провайдерами**
  Почтовым сервисам, аналитике и хостингу, обрабатывающим персональные данные жителей ЕС, нужно соглашение DPA; большинство провайдеров предлагают принять его онлайн.

- [ ] **Ссылайтесь на политики там, где собираются данные**
  Рядом с формами, подпиской на рассылку и при оформлении заказа.

- [ ] **Проверьте реквизиты компании и контактную информацию**
  Юридическое название, регистрационный номер, адрес и номер плательщика НДС, где применимо. Во многих странах они обязательны на коммерческих сайтах.

КАК ПРОВЕРИТЬ

Откройте сайт в чистом приватном окне и в инструментах разработчика (вкладка Network) посмотрите, что загружается до нажатия «Принять».

08 Проверки в день запуска

Финальная проверка доказывает, что сайт работает на реальных устройствах, с реальными данными и реальными почтовыми серверами.

- [ ] ОБЯЗАТЕЛЬНО **Протестируйте каждую форму и убедитесь, что сообщение приходит**
  Проверьте и папку «Спам». Адреса отправителя и reply-to должны использовать ваш собственный домен.

- [ ] ОБЯЗАТЕЛЬНО **Проверьте оформление заказа от начала до конца**
  Небольшой реальный платёж, письмо-подтверждение и возврат. Затем удалите тестовые заказы.

- [ ] ОБЯЗАТЕЛЬНО **Уберите « `noindex` » и пароли тестовой среды**
  Забытый тег `noindex` оставляет новый сайт вне Google. Проверьте, что в `robots.txt` нет « `Disallow: /` ».

- [ ] **Добавьте редиректы 301 со всех старых адресов**
  Если вы заменили существующий сайт, сопоставьте старые страницы новым, чтобы позиции, закладки и ссылки продолжали работать.

- [ ] **Проверьте страницы 404, битые ссылки и изображения**
  Просканируйте сайт бесплатным инструментом вроде Screaming Frog (до 500 адресов бесплатно) и исправьте все ошибки.
- [ ] **Отправьте карту сайта**
  В Google Search Console и Bing Webmaster Tools.
- [ ] **Проверьте на настоящем телефоне и при медленном соединении**
  Используйте мобильный интернет, а не офисный Wi-Fi.
- [ ] **Сделайте финальную резервную копию и запишите время запуска**
  Если что-то пойдёт не так, можно будет откатиться к заведомо рабочему состоянию.

КАК ПРОВЕРИТЬ

Попросите человека, который никогда не видел сайт, выполнить главную задачу (связаться с вами, купить что-то) на своём телефоне, пока вы наблюдаете.

Источники и дополнительное чтение

OWASP Cheat Sheet Series
https://cheatsheetseries.owasp.org/

NIST SP 800-63B: руководство по цифровой идентификации (пароли)
https://pages.nist.gov/800-63-4/sp800-63b.html

Mozilla Observatory (проверка заголовков безопасности)
https://developer.mozilla.org/en-US/observatory

Google: требования к отправителям почты (SPF, DKIM, DMARC)
https://support.google.com/a/answer/81126

Нужна помощь?

Midnight Webs проектирует, защищает и поддерживает сайты для малого бизнеса. Расскажите, что нужно, и мы подготовим план работ.

midnightwebs.com/ru/estimate

Читать онлайн: midnightwebs.com/ru/resources/website-launch-security-checklist