Бизнес•Ателье

разработка и оптимизация сайтов на WordPress
бизнес-ателье.рф

Чек-лист по безопасности сайта

1. Обновление системы и плагинов

- ☐ Регулярные обновления CMS (обновления исправляют уязвимости в системе и обеспечивают безопасность)
- ☐ Обновление всех установленных плагинов и тем до последних версий
- ☐ Создание резервной копии перед обновлением

2. Использование HTTPS

- ☐ Проверка наличия SSL-сертификата (он шифрует данные между сайтом и пользователем, что защищает от перехвата информации)
- ☐ Настройка принудительного перенаправления HTTP на HTTPS (это предотвращает доступ к сайту через незащищённое соединение)
- ☐ Регулярная проверка срока действия сертификата

3. Сильные пароли и двухфакторная аутентификация (2FA)

- ☐ Проверка сложности паролей
- ☐ Включение 2FA для административных учётных записей
- ☐ Регулярная смена паролей для повышения безопасности

4. Ограничение доступа по IP

- ☐ Настройка доступа к административной панели только с доверенных IP-адресов
- ☐ Настройка плагина для фильтрации подозрительного трафика
- ☐ Ведение списка разрешённых и запрещённых IP-адресов

5. Регулярное резервное копирование

- ☐ Настройка автоматического резервного копирования данных сайта
- ☐ Проверка работоспособности восстановления из резервной копии
- ☐ Хранение резервных копий в безопасном месте

6. Защита от атак типа Brute Force

- ☐ Ограничение количества попыток входа в систему (это предотвращает попытки взлома через подбор паролей)
- ☐ Внедрение капчи на страницах входа и форм (помогает защититься от автоматических атак с использованием ботов)
- ☐ Использование временной блокировки для подозрительных IP-адресов

7. Проверка безопасности плагинов и тем

- ☐ Удаление неиспользуемых или устаревших плагинов и тем
- ☐ Проверка на наличие уязвимостей в используемых плагинах
- ☐ Использование только проверенных и популярных плагинов

8. Мониторинг и ведение журнала активности (логи)

- ☐ Настройка журналов активности для отслеживания изменений на сайте
- ☐ Включение уведомлений о подозрительных действиях (например, многократные попытки входа)
- ☐ Регулярный анализ логов для выявления аномалий

9. Ограничение прав доступа

- ☐ Пересмотр ролей и прав доступа для всех пользователей
- ☐ Ограничение доступа к файловой системе сайта (пользователи не должны иметь доступ к чувствительным файлам сайта)
- ☐ Применение принципа наименьших привилегий для пользователей

10. Защита базы данных

- ☐ Изменение стандартного префикса таблиц базы данных
- ☐ Регулярное резервное копирование базы данных
- ☐ Настройка сложного пароля для базы данных