Памятка: что сделать после взлома сайта

Сайт вычистили. Дальше – восемь шагов, которые остаются за владельцем и его программистом. Распечатайте и отмечайте сделанное.

> **Чистка не защищает от повторного взлома.** Если не закрыть то, через что вошли, злоумышленник вернётся тем же путём. Поэтому шаги ниже – не «по желанию».

1 Сменить все пароли

Считайте украденным всё, до чего взломщик мог дотянуться, а не только пароль администратора сайта.

- [ ] администраторы сайта (1С-Битрикс, WordPress и другие системы)
- [ ] FTP, SFTP, SSH
- [ ] личный кабинет хостинга или сервера
- [ ] база данных
- [ ] панель управления сервером
- [ ] почта администраторов
- [ ] учётные записи разработчиков, у которых был доступ
- [ ] ключи и токены для обмена с другими системами

До смены выпишите, где эти пароли и ключи прописаны: обмен с 1С, CRM, оплата, доставка, почта сайта. После смены впишите туда новые – иначе обмен остановится.

2 Проверить пользователей сайта

- [ ] удалить незнакомых пользователей
- [ ] сверить список администраторов
- [ ] проверить группы и права
- [ ] убедиться, что не осталось скрытых учётных записей

3 Проверить доступы к серверу

Это работа для программиста или администратора сервера.

- [ ] SSH-ключи: нет ли чужих
- [ ] пользователи FTP и SFTP
- [ ] задачи по расписанию (cron)
- [ ] подозрительные процессы
- [ ] лишние учётные записи на хостинге

4 Обновить всё, что установлено

- [ ] ядро сайта (1С-Битрикс, WordPress)
- [ ] PHP
- [ ] модули, плагины, расширения
- [ ] шаблон
- [ ] сторонние компоненты

Если в стороннем модуле или шаблоне есть известная уязвимость – поставить свежую версию или закрыть уязвимость другим способом.

5 Настроить резервные копии

- ☐ копия делается сама, каждый день
- ☐ хранится несколько версий, а не одна последняя
- ☐ копии лежат отдельно от сервера сайта
- ☐ раз в несколько месяцев — пробное восстановление из копии

Файл backup.zip — ещё не резервная копия. Копия есть только тогда, когда из неё удалось поднять сайт.

6 Защитить учётные записи

- ☐ вход администраторов с кодом из приложения или СМС (двухфакторная защита)
- ☐ доступ в админку только с нужных адресов
- ☐ у каждого свой логин вместо общего admin
- ☐ каждому — только те права, которые нужны для работы

7 Наблюдать первые недели

Если что-то из списка появилось снова — вход остался открыт. Переадресацию и спрятанные чужие ссылки каждый день ищет наша охрана сайта и пишет в Telegram: la-chatte.com/services/ohrana-sajta/, 3 000 ₽ в месяц, первая проверка бесплатно.

- ☐ подозрительные файлы
- ☐ новые пользователи
- ☐ изменения в файлах сайта
- ☐ незнакомые задачи по расписанию
- ☐ переадресация на чужие адреса
- ☐ всплески нагрузки
- ☐ рассылка спама с сайта
- ☐ новые страницы и ссылки в поиске

8 Записать, что произошло

Пригодится при повторном случае, смене подрядчика и для вопросов от клиентов.

Когда обнаружили _____

Что именно обнаружили _____

Что сделали _____

Какие доступы могли быть украдены _____

Какие пароли сменили _____

Какие уязвимости закрыли _____

Дата последней проверки _____