

ОБЕЗЛИЧЕННЫЙ ОТЧЁТ

Взлом и восстановление сайта на Joomla 3

Сайт туристической компании: разбор взлома, чистка файлов и базы, укрепление и открытие меньше чем через сутки после начала работ

Заказчик	туристическая компания, название скрыто по договорённости
Исполнитель	Евгений Крамсаков
Срок	2 дня, осень 2026 года
Платформа	Joomla 3, PHP, виртуальный хостинг

Отчёт обезличен. Я убрал название компании, адреса сайтов, учётные записи, сведения о хостинге и банке, номера счётчиков и всё, что относится к клиентам заказчика. Числа о данных клиентов округлены.

1. Коротко

Ко мне обратились владельцы сайта туристической компании. Сайт и админка не открывались: вместо них висела страница «WordPress: сайт на обслуживании», а телефоны перебрасывало на чужой сайт. Нужно было найти причину, вычистить сайт и вернуть его в работу.

Злоумышленник имел доступ к хостингу больше трёх месяцев и заразил все 11 сайтов на аккаунте. За два дня я разобрал взлом, вычистил сайт и базу данных, обновил движок и расширения, удалил лишнее и закрыл найденные лазейки. Две независимые проверки действующих закладок не нашли. Сайт открылся меньше чем через сутки после начала работ.

< 24 часов

от начала работ до открытия сайта

0 закладок

по итогам двух независимых проверок

18 копий

резервная копия перед каждым изменением

Что получил заказчик

- Работающий сайт на последней бесплатной версии Joomla 3 с обновлёнными расширениями.
- Базу данных без поддельных администраторов, лазеек в редакторе и подменённых прав.
- Отчёт: что произошло, что сделано и 22 рекомендации с уровнем срочности.
- Полный снимок заражённого аккаунта как доказательство и 18 резервных копий по ходу работ.

2. Что произошло

2.1. Что видели посетители

Любой адрес сайта, включая админку, отдавал поддельную страницу «WordPress: сайт на обслуживании» с кодом ошибки 503. Сайт работает на Joomla, эту страницу подложил злоумышленник: ночью он заменил ею 2954 файла сайта. На телефонах страница уводила посетителя на `urshort.com` и дальше на `muslmh.free-hosting.net`.

Ещё в 651 скрипт сайта злоумышленник вписал переброс мобильных посетителей на `ushort.dev`.

2.2. Как злоумышленник попал на сайт

Точный способ и дату проникновения я установить не могу: хостинг хранил журналы посещений только за последние две недели.

- На аккаунте хостинга, кроме основного сайта, работали ещё 10 сайтов: три тестовые копии основного сайта на старой Joomla 3.9.6–3.9.8 и семь сайтов и поддоменов, шесть из которых состояли из одних вредоносных файлов. Все они работали от имени одного пользователя хостинга, поэтому взлом любого из них открывал доступ к остальным.
- В тестовых копиях с ноября 2020 года лежал бэкдор `cache-db.php`, программа скрытого доступа.
- Временная папка основного сайта указывала в тестовую копию. Первые файлы активной атаки злоумышленник положил туда в июне 2026 года.
- На основном сайте стоял конструктор страниц SP Page Builder 3.7.8 с уязвимостью загрузки файлов. Все две недели, за которые сохранились журналы, его атаковали каждый день, до 53 попыток в сутки. Дважды сайт ответил на часть попыток кодом успеха.
- За семь недель до обращения антивирус хостинга нашёл 104 вредоносных объекта, почти все в тестовой копии. В тот же день кто-то перезаписал файлы движка копией 2021 года. Атаки после этого продолжились.

Когда	Событие
ноябрь 2020	В тестовых копиях сайта появляется бэкдор <code>cache-db.php</code> .
июнь 2026	Начало активной атаки: загрузки во временной папке тестовой копии.
июнь–сентябрь	Злоумышленник раскладывает веб-шеллы, заводит поддельных администраторов и профили редактора.
август	Антивирус хостинга находит 104 объекта; кто-то перезаписывает файлы движка копией 2021 года.
сентябрь	Ежедневные атаки на SP Page Builder.
ночь перед обращением	Злоумышленник подменяет 2954 файла заглушкой, сайт перестаёт работать.
День 1	Диагностика, полная копия аккаунта, честная страница «на обслуживании», замена сайта чистой копией.
День 2	Обновления, удаление лишнего, чистка базы, две проверки, открытие сайта.

2.3. Что злоумышленник оставил

В файлах

- Десятки веб-шеллов: программ, через которые сайтом управляют из браузера. Злоумышленник прятал их в папки со случайными именами.
- Загрузчики вредоносного кода в файлах с расширениями картинок и видео (`.ico`, `.jpeg`, `.m3u8`).
- Около 4400 служебных файлов `.htaccess`: они блокировали чужие программы и пропускали его собственные.
- Набор `ms_*`, который уводил посетителей на посторонние сайты.

В базе данных

- 4 поддельных главных администратора и 13 скрытых учётных записей в группе администраторов.
- 316 поддельных профилей визуального редактора JCE. 262 из них открывали редактор любому посетителю, 314 разрешали загружать файлы с программным кодом. Через них злоумышленник мог вернуться после любой чистки файлов.
- Изменённые права доступа: управлять плагинами и править два модуля мог любой посетитель.
- Включённое выполнение PHP-кода в расширении Sourcerer.

Одной чистки файлов здесь бы не хватило: через профили редактора и подменённые права злоумышленник вернулся бы на следующий день. Поэтому базу данных я разбирал так же подробно, как файлы.

2.4. Персональные и учётные данные

Злоумышленник мог запускать на сервере свой код и читать файл настроек сайта с паролем к базе данных. Значит, он мог прочитать и всю базу. В ней хранились около 17 тыс. адресов подписчиков рассылки, около 2,5 тыс. заявок из форм и около 3,3 тыс. комментариев с адресами почты. В файлах сайта открытым текстом лежали учётные данные магазина в системе эквайринга банка, а в настройках сайта лежал пароль почтового ящика.

Следов выгрузки данных я не нашёл, но журналы хостинга покрывали только последние две недели. Я рекомендовал заказчику сменить учётные данные эквайринга и почты и обсудить ситуацию с юристом: закон о персональных данных (152-ФЗ) в ряде случаев требует сообщить об инциденте в Роскомнадзор.

3. Что я сделал

3.1. Изоляция и сохранение улик

- Разбор я вёл в изолированном контейнере на отдельном сервере, без общих папок с рабочими компьютерами. Ни одного файла с сайта я не запускал.
- До любых изменений снял полную копию аккаунта хостинга (3,3 ГБ) и храню её как доказательство.
- В первые часы работ заменил заглушку злоумышленника честной страницей «Сайт на обслуживании» без скриптов и перенаправлений. Посетители видели её до открытия сайта, а я работал с сайтом со своего адреса.

3.2. Чистка файлов

- Заменил файлы сайта чистой копией годичной давности, которая лежала на хостинге, и сверил каждый файл по контрольной сумме. Из копии исключил программу выгрузки базы через браузер.
- По решению заказчика удалил остальные 10 сайтов аккаунта: тестовые копии и сайты, заражённые или созданные злоумышленником.
- Удалил вредоносные файлы вне папки сайта и заражённую копию сайта 2021 года.

3.3. Чистка базы данных

- Удалил 4 поддельных главных администратора, 13 скрытых учётных записей и 316 поддельных профилей редактора JCE.
- Вернул права доступа к значениям Joomla по умолчанию и выключил выполнение PHP в Sourcerer.
- Удалил 422 таблицы старых установок и вторую, ненужную базу данных.

3.4. Обновления

Перед каждым обновлением я делал резервную копию и сверял пакет с контрольной суммой производителя.

Компонент	Было	Стало
Joomla	3.9.23 (файлы), 3.9.28 (база)	3.10.12, последняя бесплатная версия ветки 3
Русский язык Joomla	3.9.23.1	3.10.12.1
PHP	7.1.33	7.4.30
Редактор JCE	2.9.1	2.9.99.11
Sourcerer	8.4.3	9.8.0 + Regular Labs Library вместо NoNumber Framework
Advanced Module Manager	7.14.1	9.9.0
Modules Anywhere	3.6.4	7.18.0
Akeeba Backup	7.4.0.1	8.4.0
Карта сайта	Xmap 3.0.0	OSMap 5.1.10

3.5. Что я удалил по решению заказчика

Больше двадцати расширений сайт не использовал или держал устаревшими, и риск от них перевешивал пользу.

Расширение	Почему
SP Page Builder	Через его уязвимость, скорее всего, и шла атака.
VirtueMart и модуль оплаты	Магазин уже не работал: от VirtueMart остались одни плагины. Модуль оплаты хранил учётные данные банка открытым текстом.
RSForm, AcyMailing, JComments	Формы, рассылка и комментарии: заказчик решил от них отказаться. Данные из них я сохранил в резервной копии.
Attachments	Нужные документы я вернул по прямым ссылкам.
eXtplorer	Файловый менеджер в админке: лишняя дверь на сервер.
Шесть расширений для cookie	Заменял одним современным баннером.
Froala, Instagram Stream, Gantry, RokNavMenu, JSpeed, плагин Google Tag Manager, NoNumber Framework, старые библиотеки Akeeba, мелкие плагины	Сайт ими не пользовался.

3.6. Что я исправил и добавил

- Поставил баннер о cookie (vanilla-cookieconsent 3.1.0) и вывел политику конфиденциальности в подвал по короткому адресу.
- Поставил карту сайта OSMap и добавил ссылку на неё в `robots.txt`.
- Вынес временную папку движка за пределы сайта. Раньше Akeeba сохранила бы следующую резервную копию в папку, открытую из интернета.
- Убрал из открытого доступа старый архив картинок на 120 МБ.
- Перевёл источники обновлений на защищённое соединение. Внешнюю библиотеку закрепил версией и контрольной суммой: подменённый файл браузер не выполнит.
- Вырезал из статей код старых виджетов с поддомена, который указывал на сторонний сервис. Сервис этот поддомен больше не обслуживает, его может перехватить посторонний.
- Убрал ссылки на старый домен компании, который больше не работает: его может зарегистрировать кто угодно.
- Нашёл 37 битых ссылок на картинки и документы. Семь файлов вернул из старого архива и из веб-архива, для остальных подготовил список для повторной загрузки.

3.7. Доступы

- Оставил одного администратора с новым случайным паролем из 24 символов. Старые учётные записи, включая запись прежней веб-студии, удалил.
- Сбросил все сессии, сменил секретный ключ Joomla и пароль базы данных.

3.8. Проверки

- Сверил все файлы сайта (около 11,6 тыс.) с чистыми источниками: официальными пакетами Joomla и расширений и годичной копией. Необъяснённых файлов не осталось.
- Провёл две независимые проверки на остаточные закладки: файлы, база данных, журналы, настройки хостинга. Действующего бэkdора ни одна не нашла. Вторая проверка нашла три слабых места в настройках: папку для резервных копий, источники обновлений без защищённого соединения и лишние права у компонента Check-in. Все три я исправил.
- Ночь между днями работ наблюдал за сайтом: файлы и база не менялись.
- После каждого изменения проверял 27 ключевых страниц сайта и админку.
- Анализ и рутинные операции я выполнял с помощью ИИ-агентов под своим контролем. Вторую проверку провёл отдельный агент на другой модели, независимо от первой.

3.9. Открытие сайта

Я открыл сайт на второй день. Узлы проверки в пяти странах получили ответ сайта за 0,4–1,4 секунды. Первый час после открытия я следил за изменениями на сайте и за попытками атак.

За этот час на сайт пришло 865 запросов. Google начал заново обходить сайт. Два сканера сделали 290 запросов в поисках веб-шеллов, чужих файловых менеджеров и уязвимых плагинов WordPress и на каждый получили ответ «страница не найдена». Страницу входа в админку открыли один раз, войти никто не пытался. За 20 проверок файлы, база данных и страницы сайта не изменились.

4. Рекомендации заказчику

Срочность: **Критично** в ближайшие дни, **Высокий** в течение месяца, **Средний** в течение квартала, **Низкий** по возможности. Ниже сокращённый список: 22 пункта из полного отчёта я свёл в 14.

№	Что сделать	Почему	Срочность
1	Сменить учётные данные эквайринга и пароль почтового ящика из настроек сайта.	Злоумышленник мог их прочитать.	Критично
2	Сменить пароль хостинга после окончания работ.	Пароль передавали подрядчику в переписке.	Критично
3	Включить двухфакторный вход в админку и поднять минимальную длину пароля до 12 символов.	Админка открыта всему интернету, сканеры открывают страницу входа.	Высокий
4	Обсудить с юристом возможный доступ к персональным данным.	152-ФЗ в ряде случаев требует уведомить Роскомнадзор.	Высокий
5	Перейти с Joomla 3 и PHP 7.4 на поддерживаемые версии.	Joomla 3 не получает исправлений с августа 2023 года, PHP 7.4 с ноября 2022-го. В Joomla 3.10.12 известны CVE-2024-21724 и CVE-2024-21726.	Высокий
6	Попросить хостинг проверить то, что не видно с аккаунта сайта.	Триггеры и события базы, системные настройки PHP, история входов в панель, FTP- и SSH-доступы.	Высокий
7	Настроить резервные копии вне хостинга и раз в квартал проверять восстановление.	Последняя полная копия перед взломом была полуторагодовой давности и лежала на том же хостинге.	Высокий
8	Проверить сайт в Яндекс.Вебмастере и Google Search Console.	Поисковики могли пометить сайт как опасный.	Средний
9	Удалить висячую DNS-запись старого поддомена.	Её может перехватить посторонний.	Средний
10	Назвать Яндекс.Метрику в политике cookie и обновить политику конфиденциальности.	Документы не называют Метрику, политику писали семь лет назад.	Средний
11	Раз в месяц обновлять Joomla и расширения, следить за изменениями файлов.	Сканеры приходят на сайт каждый день.	Средний
12	Ограничить срок хранения резервных копий с персональными данными.	Чем дольше копии лежат, тем больше риск утечки.	Средний
13	Добавить SPF-запись и удалить неиспользуемые настройки почтового сервера.	Письма с сайта попадают в спам, а старые настройки хранят пароль.	Низкий
14	Загрузить недостающие картинки, заменить старые расширения без обновлений.	Пустые места на страницах, расширения без исправлений безопасности.	Низкий

5. Как я работал

- **Сначала изоляция, потом действия.** Заражённые файлы разбирал только в отдельном контейнере, полный снимок аккаунта снял до первого изменения.
- **Резервная копия перед каждым шагом.** 18 копий за второй день, у каждой контрольные суммы, сверенные после переноса.
- **Проверка по контрольным суммам.** Каждый пакет обновления и каждый файл сайта я сверял с официальными источниками.
- **Решения за заказчиком.** Всё, что меняло возможности сайта (удаление расширений, сайтов, данных), я делал после явного решения заказчика.
- **Две независимые проверки и наблюдение.** Ночное наблюдение между днями работ и час после открытия.

Приложение. Признаки заражения

Для специалистов, которые ищут похожие следы у себя. Индикаторы относятся к злоумышленнику и не указывают на заказчика.

Тип	Значение
Заглушка	Поддельная страница «WordPress: Briefly unavailable for scheduled maintenance», 2954 копии одного файла (md5 начинается с 2cf9d01b), код 503 и Retry-After 3600
Домены перенаправлений	urshort.com, muslmh.free-hosting.net, ushort.dev, olurmuolur.xyz
Веб-шеллы	0day.php, anonfox.php, she11.php, priv0.php, cmd.php, ws.php, f35.php, b8.php (wpuploader), c95a05a87ad6.php, 837b97742cindex.php, 7814f5fb78index.php, filefuns.php (маркер BiaoJiOk)
Загрузки	cache.php с обфусцированной нагрузкой в .ico, .jpeg, .tiff, .m3u8 во вложенных папках (bin/bin/bin, css/css/css)
Набор ms_*	ms-home-gate.php, ms-bot-prepend.php, .ms_jp_quarantine, .ms_index.bak.php, .user.ini с auto_prepend
Бэкдоры	GIF89a+PHP с управлением через cookie; cache/cache-db.php (\$_COOKIE[ssid]); .nox-content (SEO-спам); php.ini с пустым disable_functions; маршрутизатор .htaccess в домашней папке
Учётные записи	lhfadmin, usiadmin, nxtadmin, evcadmin (дата регистрации 1970-10-10); adminstar, userhost, sudouser, joomla_support, assistant, joomsv, joomlaa440, mkzss, mkzsz, hugsys, sipotr, siput, siputi
Профили JCE	J#####, S####, H####, VulnScan3145, Jqcra, Shadow_... (316 штук, загрузка php/phtml, группа Public)
Атака на SP Page Builder	POST index.php?option=com_sppagebuilder&task=asset.uploadCustomIcon, User-Agent sppb-rce-пос