Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Безопасность корпоративного сайта: наш инженерный чек-лист

Как мы строим защиту веб-периметра: TLS-контур nginx, CSP, изоляция CMS и бэкапы с проверкой

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Корпоративный сайт — единственный сервис компании, открытый в интернет 24/7: его круглосуточно сканируют боты на известные уязвимости CMS. Взлом сайта — это дефейс, фишинг-рассылки с домена компании, чёрные списки для корпоративной почты, а при общем сервере с 1С — вход во всю инфраструктуру. Мы закрываем периметр регламентом из шести технических контуров.

Почему это важно бизнесу

- Домен в чёрных списках = почта компании в спаме: КП не доходят до клиентов, продажи проседают на недели
- Взлом сайта, связанного с 1С или CRM, открывает базу заказов и контакты клиентов — риск по 152-ФЗ
- Простой сайта перед тендером — прямые потери лидов; восстановление после взлома дороже года сопровождения
- Дефейс и «баннер казино» на главной — репутационный ущерб, который клиенты видят раньше вас

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1.2/1.3

только эти версии TLS в ssl_protocols nginx; шифры ECDHE с AES-GCM и ChaCha20, без legacy-CBC

по докам nginx 1.28

90 дней

срок сертификата Let's Encrypt; certbot.timer продлевает автоматически за 30 дней до истечения

certbot 5.x / Let's Encrypt

1 год

max-age=31536000 в HSTS с includeSubDomains — браузер сам блокирует переход на HTTP

наш стандарт / RFC 6797

5 / 1 ч

порог fail2ban для админки CMS: 5 неудачных входов — бан IP на час (maxretry=5, bantime=1h)

fail2ban 1.1

24 ч

наш SLA на установку security-обновлений CMS и плагинов после выхода патча

наш стандарт

14 дней

глубина ежедневных бэкапов файлов и БД в двух независимых хранилищах (сервер + S3)

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

TLS-контур и заголовки безопасности на фронте nginx

Что настраиваем

Фронт nginx 1.28 (reverse-proxy перед CMS): сертификаты, протоколы и HTTP-заголовки для всех виртуальных хостов

Как мы это делаем

1. Выпускаем сертификат: certbot --nginx -d site.ru -d www.site.ru; проверяем systemctl status certbot.timer и ставим deploy-hook на перезагрузку nginx
2. Фиксируем ssl_protocols TLSv1.2 TLSv1.3, в ssl_ciphers — только ECDHE с AES-GCM/ChaCha20; включаем http2 on и ssl_session_cache shared:SSL:10m (OCSP stapling не нас…
3. Добавляем заголовки с флагом always: HSTS (max-age=31536000; includeSubDomains), X-Content-Type-Options nosniff, X-Frame-Options SAMEORIGIN, Referrer-Policy
4. CSP вводим в два шага: сначала Content-Security-Policy-Report-Only, неделю собираем нарушения, затем переводим политику в боевой режим
5. Контроль результата: оценка A+ на SSL Labs и A на securityheaders.com — фиксируем в паспорте сайта

РЕЗУЛЬТАТ

Сертификат больше никогда не «протухает внезапно»: продление и перезагрузка nginx полностью автоматические. Даже при внедрении чужого JS через уязвимость CMS браузер клиента не выполнит скрипт вне белого списка CSP — вторая линия защиты работает без участия сервера.

КЛЮЧЕВОЙ НЮАНС

add_header в nginx не наследуется: любой add_header внутри location отменяет все заголовки уровня server. Поэтому весь блок заголовков мы выносим в отдельный include и подключаем его в каждом location.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Изоляция CMS и харднинг админки WordPress/Битрикс

Что настраиваем

Отдельный VPS под сайт (никогда на одном сервере с 1С, файлами и почтой): PHP-FPM, MySQL/MariaDB, панель CMS

Как мы это делаем

1. Выносим сайт на отдельный VPS: перенос файлов и БД, смена DNS, неделя параллельной работы, затем удаление со старого сервера
2. Закрываем /wp-admin/ и /bitrix/admin/ по IP: allow офис + VPN, deny all; сверху limit_req (rate=10r/s, burst=20 nodelay) против перебора
3. fail2ban: jail на POST к wp-login.php и xmlrpc.php, maxretry=5, bantime=1h; источник — access-логи nginx
4. Включаем автообновления core и плагинов (wp-cli / подписка на обновления Битрикс), проактивную защиту Битрикс — в максимальный режим
5. Еженедельный аудит WPScan по списку установленных компонентов; отключённые плагины не храним — удаляем

РЕЗУЛЬТАТ

Брутфорс админки перестаёт быть угрозой: снаружи она отдаёт 403 ещё до формы логина. Окно уязвимости после выхода патча сокращается до 24 часов, а компрометация сайта не даёт злоумышленнику ничего, кроме изолированного VPS без доступа к 1С и файлам офиса.

КЛЮЧЕВОЙ НЮАНС

Отключённый плагин остаётся исполняемым PHP-кодом на диске и эксплуатируется напрямую по URL. Правило простое: не используется — удаляется физически, а не деактивируется.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Бэкап-контур с обязательным тестовым восстановлением

Что настраиваем

Файлы сайта + дамп БД; два независимых хранилища: локальный каталог бэкапов и S3-совместимое облако

Как мы это делаем

1. Ежедневно по cron: tar -czf файлов и mysqldump --single-transaction базы, ротация find -mtime +14 -delete
2. Копия в облако через rclone в S3-совместимое хранилище; у ключа доступа — права только на запись в свой бакет
3. Раз в квартал разворачиваем бэкап в staging и прогоняем чек-лист: главная, формы, корзина, вход в админку
4. Мониторинг доступности с интервалом 60 с и алертом инженеру в Telegram при простое дольше 1 минуты

РЕЗУЛЬТАТ

Восстановление после дефейса или шифровальщика — регламентная операция на 1-2 часа, а не проект на неделю. Квартальный тест гарантирует, что в бэкапе есть и файлы, и база, и что они реально разворачиваются в рабочий сайт.

КЛЮЧЕВОЙ НЮАНС

Ключ облачного хранилища на сервере не должен позволять удалять или читать бэкапы: иначе при компрометации сервера злоумышленник уничтожит и копии. Write-only-доступ закрывает это на уровне политики бакета.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **add_header пропадает в location**
  Директива в location отменяет заголовки уровня server. Держим все security-заголовки в одном include и подключаем его в каждом location.

- ✕ **TLS 1.0/1.1 «для совместимости»**
  Старые протоколы роняют оценку SSL Labs и открывают downgrade-атаки. Реальных клиентов на них давно нет — отключаем без исключений.

- ✕ **Сертификат обновился, nginx — нет**
  certbot renew без reload оставляет в памяти nginx старый сертификат до истечения. Ставим deploy-hook: systemctl reload nginx.

- ✕ **CSP сразу в боевом режиме**
  Жёсткая политика молча ломает метрику, шрифты и виджеты. Сначала Report-Only с разбором отчётов, enforce — после недели наблюдения.

- ✕ **Сайт на сервере с 1С**
  Взлом CMS даёт доступ ко всему хосту, включая базы 1С. Сайт живёт только на отдельном VPS или хостинге — наш обязательный минимум.

- ✕ **Деактивированные плагины**
  PHP-файлы плагина доступны по прямому URL даже в выключенном состоянии. Неиспользуемое удаляем физически и проверяем WPScan.

- ✕ **Бэкап рядом с сайтом**
  Копия на том же сервере гибнет вместе с ним при взломе или отказе диска. Вторая копия — только во внешнее хранилище с ограниченным ключом.

- ✕ **Админка защищена одним паролем**
  Формы логина CMS брутфорсят круглосуточно. Белый список IP + fail2ban + 2FA снимают проблему до того, как пароль вообще проверяется.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- HTTPS с автопродлением certbot, редирект 80→443, только TLS 1.2/1.3
- Автообновления core CMS и еженедельная установка обновлений плагинов
- Ежедневный бэкап файлов и БД с хранением 14 дней вне сервера

НОРМАЛЬНО

- Полный набор заголовков: HSTS, CSP, X-Content-Type-Options, Referrer-Policy
- Админка по белому списку IP + fail2ban (5 попыток — бан на час)
- Сайт на отдельном VPS, изолированном от 1С и файловых серверов
- Мониторинг доступности с шагом 60 с и алертом в Telegram

ХОРОШО

- CSP в enforce-режиме с отчётами о нарушениях и белым списком доменов
- Квартальное тестовое восстановление из бэкапа в staging по чек-листу
- Ежемесячный аудит WPScan / проактивная защита Битрикс + разбор логов
- WAF/анти-DDoS фронт перед сайтом и rate limiting в nginx

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SSL Labs даёт сайту оценку A/A+, а сертификат продлевается автоматически с reload nginx?
- [ ] Отключены ли TLS 1.0/1.1 и legacy-шифры (RC4, 3DES) в конфигурации веб-сервера?
- [ ] Отдаёт ли сайт HSTS, CSP и X-Content-Type-Options — проверяли на securityheaders.com?
- [ ] Обновления безопасности CMS и плагинов ставятся в течение 24 часов после выхода?
- [ ] Админка CMS доступна только с IP офиса/VPN, а брутфорс блокирует fail2ban?
- [ ] Сайт физически отделён от сервера с 1С, почтой и файловым хранилищем?
- [ ] Бэкап файлов и БД делается ежедневно и копируется во внешнее хранилище?
- [ ] Восстановление из бэкапа проверялось в тестовой среде за последний квартал?
- [ ] Есть ли мониторинг доступности с алертом инженеру в первую минуту простоя?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Экспресс-аудит безопасности сайта за 1-2 дня: TLS, заголовки, версии CMS, следы компрометации — с отчётом
- Перенос сайта с общего сервера на изолированный VPS: nginx, fail2ban, харднинг админки
- Сопровождение под ключ: обновления CMS за 24 ч, ежедневные бэкапы, мониторинг, реакция на инциденты 2-4 ч
- Лечение взломанных сайтов: зачистка веб-шеллов, восстановление из бэкапа, вывод домена из чёрных списков

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Модуль ngx_http_ssl_module и директива add_header (nginx.org — 1.28)

02 Certbot User Guide: renew, deploy-hook, systemd timer (eff-certbot.readthedocs.io — 5.x)

03 Let's Encrypt: срок действия сертификатов и переход отзыва на CRL (letsencrypt.org — 2026)

04 Content Security Policy и заголовки безопасности (developer.mozilla.org — 2026)

05 Hardening WordPress (Advanced Administration) (developer.wordpress.org — 6.8+)

06 Проактивная защита «1С-Битрикс: Управление сайтом» (dev.1c-bitrix.ru — 2026)

07 fail2ban: jails и фильтры для nginx (github.com/fail2ban — 1.1)

08 Регламент сопровождения сайтов ITfresh (внутренний шаблон) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.