Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Просроченный SSL-сертификат: маленький файл, большие убытки

Почему сертификаты «слетают», чего это стоит бизнесу и как автоматизация снимает проблему

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сайт, веб-доступ к 1С, почта и личный кабинет держатся на SSL-сертификатах — файлах с конечным сроком действия. Истёк один — и браузер встречает клиентов красным «Подключение не защищено»: заявки и платежи падают, репутация страдает. Вдобавок зарубежные УЦ отзывают сертификаты российских компаний по санкционным ограничениям. Корень проблемы — не технология, а ручное продление...

Почему это важно бизнесу

- Красное предупреждение браузера останавливает клиента на входе: до сайта не доходят ни заявки, ни оплаты
- Просрочка ломает не только сайт: почту на телефонах сотрудников, веб-доступ к 1С для бухгалтерии, платёжные шлюзы
- Зарубежный УЦ может отозвать оплаченный сертификат по санкциям за одну ночь — деньги потеряны, замену нужно поднять за часы
- С 15 марта 2029 года максимальный срок публичных TLS-сертификатов — 47 дней: ручное продление физически перестанет успевать
- Let's Encrypt с 4 июня 2025 года не шлёт письма об истечении — без собственного мониторинга о просрочке первыми узнают клиенты

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

90 дней

срок действия сертификата Let's Encrypt — без настроенного автопродления просрочка гарантирова…

letsencrypt.org, Why ninety-day lifetimes

30 дней

до истечения certbot renew продлевает сертификат; systemd-таймер запускает проверку дважды в с…

certbot.eff.org, User Guide

47 дней

максимальный срок публичных TLS-сертификатов с 15 марта 2029 года (200 дней — с 2026-го, 100 —…

cabforum.org, Ballot SC-081v3

0 писем

Let's Encrypt прекратил email-уведомления об истечении сертификатов 4 июня 2025 года — контрол…

letsencrypt.org, Expiration Notification Service Has Ended

50 в неделю

лимит выпуска сертификатов на один регистрируемый домен у Let's Encrypt — учитывайте при массо…

letsencrypt.org, Rate Limits

14 и 7 дней

до истечения — пороги алертов в нашем регламенте мониторинга; второй алерт эскалируется дежурн…

регламент мониторинга ITfresh

РЕАЛИЗАЦИЯ 1 ИЗ 3

Автопродление «настроено» — и молча падало два месяца

Что настраиваем

Наш сценарий: интернет-магазин на nginx, сертификаты Let's Encrypt через certbot

Как мы это делаем

1. Certbot настроен с проверкой HTTP-01 через webroot; год всё продлевается автоматически, о сертификатах никто не вспоминает
2. Сайт переезжает на новый сервер: путь webroot меняется, конфиг продления в /etc/letsencrypt/renewal/ остаётся старым
3. certbot renew дважды в сутки падает с ошибкой валидации — 404 на /.well-known/acme-challenge/ — но логи никто не читает
4. Через 90 дней сертификат истекает в пятницу вечером: у клиентов красное «Подключение не защищено», заявки останавливаются

РЕЗУЛЬТАТ

Выходные без заявок и оплат: покупатели уходят с красного предупреждения, часть пишет в поддержку «у вас вирус». Саму причину устранили за 15 минут — но два дня трафика и рекламного бюджета не вернуть.

КЛЮЧЕВОЙ НЮАНС

«Настроено» не значит «работает». После любого переезда или смены конфигурации — certbot renew --dry-run, плюс внешний мониторинг срока сертификата, который не зависит от самого сервера.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Сертификат обновился, а почта отдавала старый

Что настраиваем

Наш сценарий: почтовый сервер компании на Postfix и Dovecot

Как мы это делаем

1. Certbot исправно продлевает сертификат: свежий файл появляется в /etc/letsencrypt/live/ каждые 60 дней
2. Postfix и Dovecot читают сертификат один раз при старте и месяцами держат в памяти старую копию
3. Старая копия истекает: телефоны сотрудников перестают забирать почту, клиенты видят предупреждения о сертификате
4. Диагноз ставится не сразу: на диске сертификат валидный; расхождение показала проверка openssl s_client -connect на порту 993

РЕЗУЛЬТАТ

Полдня почта «не работает» у всей компании, а поиск идёт не там: файл на диске свежий, истёкший сертификат отдаёт сама служба. Потеряны часы работы всех сотрудников и доверие к ИТ.

КЛЮЧЕВОЙ НЮАНС

Продление — это два шага: получить файл и заставить службу его перечитать. Deploy hook обязателен: --deploy-hook с reload nginx, Postfix и Dovecot — и мониторить срок именно на порту, а не на диске.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Отзыв зарубежным УЦ: оплаченный год сгорел за ночь

Что настраиваем

Наш сценарий: компания с платным wildcard-сертификатом зарубежного УЦ

Как мы это делаем

1. УЦ уведомляет: из-за санкционных ограничений сертификаты российских клиентов будут отозваны, деньги не возвращаются
2. На одном сертификате висят сайт, API и личный кабинет — после отзыва браузеры покажут ошибку всем клиентам одновременно
3. За вечер выпускаем Let's Encrypt: HTTP-01 для сайта, DNS-01 через API DNS-провайдера для wildcard на поддомены
4. Параллельно оформляем резервный сертификат НУЦ Минцифры для критичных сервисов и документируем процедуру переключения

РЕЗУЛЬТАТ

Переключение завершили до часа отзыва — клиенты ничего не заметили. Стоимость платного сертификата списана в убыток, зато исчезла зависимость всей инфраструктуры от решения одного зарубежного УЦ.

КЛЮЧЕВОЙ НЮАНС

Платный зарубежный сертификат для российской компании — единая точка отказа с санкционным риском. Автоматизированный Let's Encrypt плюс резерв НУЦ Минцифры снимают эту зависимость.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Выпустили вручную и забыли

Сертификат Let's Encrypt живёт 90 дней. Без автопродления просрочка гарантирована — вопрос лишь, заметите вы её раньше клиентов или нет.

✕ Автопродление есть, но не работает

Скрипт ломается после переезда сайта, смены путей или веб-сервера. Без certbot renew --dry-run и контроля результата продление молча падает месяцами.

✕ Нет мониторинга сроков

Let's Encrypt закрыл email-уведомления об истечении в июне 2025 года. Алерты за 14 и 7 дней по всем доменам — единственная страховка, и стоит она коп…

✕ Сертификат обновлён, сервис — нет

Новый файл лежит на диске, а nginx, Apache или почтовый сервер держат в памяти старый. Нужен deploy hook с reload службы после каждого продления.

✕ Учтён только основной сайт

Почта, веб-публикация 1С, API, панели управления тоже работают на сертификатах. Именно «невидимые» сервисы просрочиваются чаще всего.

✕ Всё держится на одном человеке

Уволился админ или сменился подрядчик — никто не знает, где сертификаты и как они продлеваются. Нужна документация на каждый домен.

✕ Ставка только на зарубежный платный УЦ

Санкционный отзыв обнуляет оплаченный год за одну ночь. Нужен автоматизированный бесплатный вариант и резервный сертификат НУЦ Минцифры.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Инвентаризация всех доменов и сервисов, работающих по HTTPS: сайт, почта, веб-1С, па…
- Автопродление через certbot или acme.sh: таймер дважды в сутки, продление за 30 дней…
- Deploy hook: автоматический reload nginx, Apache и почтовых служб после продления

НОРМАЛЬНО

- Мониторинг сроков всех сертификатов с алертами за 14 и 7 дней до истечения
- Wildcard-сертификат по DNS-01 через API DNS-провайдера для поддоменов и внутренних с…
- Документация на каждый домен: где сертификат, как обновляется, кто отвечает
- certbot renew --dry-run после каждого переезда, смены путей или веб-сервера

ХОРОШО

- Единый дашборд сроков по всем доменам и сервисам компании
- Резервный ACME-УЦ и сертификат НУЦ Минцифры на случай отзыва или недоступности основ…
- Полная автоматизация под 47-дневные сертификаты — график CA/Browser Forum к марту 20…
- Внешний независимый мониторинг HTTPS: проверка сертификата на порту сервиса, алерт д…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаете ли вы точное число доменов и сервисов с HTTPS в вашей компании?
- [ ] Продлеваются ли все сертификаты автоматически, без участия человека?
- [ ] Получите ли вы уведомление за 14 дней до истечения любого сертификата?
- [ ] Перезапускаются ли веб-сервер и почта автоматически после продления?
- [ ] Проверяли ли вы автопродление после последнего переезда сайта или смены подрядчика?
- [ ] Есть ли документация: где лежат сертификаты, как обновляются, кто отвечает?
- [ ] Есть ли план на случай отзыва сертификата зарубежным УЦ по санкциям?
- [ ] Закрыты ли HTTPS не только сайт, но и веб-1С, почта и панели администратора?
- [ ] Готова ли инфраструктура к сокращению срока сертификатов до 47 дней?

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).

- Аудит: найдём все домены и сервисы с SSL — сайт, почту, веб-1С, панели — и проверим срок каждого
- Внедрение Let's Encrypt с автопродлением и deploy hook на nginx, Apache, IIS, Bitrix, почте и веб-1С
- Мониторинг сроков с алертами в Telegram за 14 и 7 дней до истечения — по всем доменам компании
- Резервный план под санкции: сертификаты НУЦ Минцифры и запасной ACME-УЦ для критичных сервисов
- Абонентское сопровождение: продление, контроль и документация — сертификаты больше не ваша забота

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 Why ninety-day lifetimes for certificates? — документация Let's Encrypt (letsencrypt.org — 2025)

02 Challenge Types: HTTP-01, DNS-01, TLS-ALPN-01 — документация Let's Encrypt (letsencrypt.org — 2025)

03 Rate Limits — лимиты выпуска Let's Encrypt (letsencrypt.org — 2025)

04 Expiration Notification Service Has Ended — Let's Encrypt (letsencrypt.org — 2025)

05 Certbot User Guide: renew, --deploy-hook, systemd-таймер (certbot.eff.org — 2025)

06 acme.sh — официальная wiki: dnsapi, reloadcmd (github.com/acmesh-official — 2025)

07 RFC 8555 — Automatic Certificate Management Environment (ACME) (datatracker.ietf.org — 2019)

08 Ballot SC-081v3: Introduce Schedule of Reducing Validity and Data Reuse Pe… (cabforum.org — 2025)

09 Configuring HTTPS servers: ssl_certificate, ssl_certificate_key (nginx.org — 2025)

10 Национальный удостоверяющий центр: получение TLS-сертификата (gosuslugi.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.