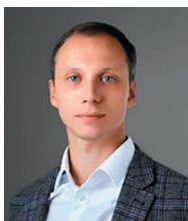




Явные и неочевидные последствия отзыва сертификатов SSL/TLS

8 мая 2026 года некоммерческий центр сертификации Let's Encrypt остановил выпуск сертификатов на два с половиной часа. Для малого и среднего бизнеса, использующего бесплатные сертификаты с автоматическим продлением через ACME, эта пауза прошла незаметно. При более длительном простое последствия могли быть иными: веб-серверы продолжили бы работать, а служебные соединения начали бы сбоить. Разбираем, на какие процессы в инфраструктуре возможности перевыпустить сертификат влияют сильнее всего и как отзыв одного корня может обрушить сразу несколько независимых систем.



text: Дмитрий Лившин, генеральный директор ООО «Сайбер Бизнес Консалтинг»

Что испытывает ИТ-инфраструктура при остановке Let's Encrypt

По данным Let's Encrypt, пауза 8 мая длилась около двух с половиной часов — выпуск был приостановлен из-за проблемы в схеме перекрестной подписи между корнями

Generation X и Generation Y. Для большинства пользователей пауза прошла незаметно: ACME-клиент перевыпускает сертификат заранее, за треть срока до истечения, запас в несколько недель перекрывает такой сбой.

Проблемы начинаются при простое длительностью в несколько

ДЛЯ ФИНТЕХА И СЛУЖБ ДОСТАВКИ ЭФФЕКТ ПОТЕРИ ДОВЕРИЯ — ТОЧЕЧНЫЙ: СТАРОЕ УСТРОЙСТВО ПЕРЕСТАЕТ ОТКРЫВАТЬ МОБИЛЬНЫЙ БАНК, ХОТЯ ПОЛЬЗОВАТЕЛЬ «НИЧЕГО НЕ ТРОГАЛ»

дней, и первыми их чувствуют не веб-серверы, а служебные соединения типа «машина-машина». Раньше всего ломается mTLS (mutual TLS — взаимная аутентификация) между микросервисами: сертификаты там живут всего несколько часов, ротация идет постоянно, без перевыпуска сервисы перестают аутентифицировать друг друга. Снаружи все работает, но внутренние вызовы не проходят. Следом падают CI/CD-пайплайны с обязательным TLS и интеграции с внешними API по клиентским сертификатам.

К тому же Let's Encrypt начал переход на 45-дневные сертификаты вместо 90-дневных: 13 мая 2026 года для TLS-сертификатов в режиме `ort-in` начался переход на 45 дней, а полный переход запланирован на февраль 2028 года. Это требует перевыпуска и установки вдвое чаще. Для крупных организаций с сотнями доменов и поддоменов автоматизация перестает быть удобством и становится обязательным условием — вручную такой массив становится неподъемным.

При этом при автоматизации масштабируются не только процессы, но и ошибки. Каскадный отказ реален, и типичный его источник — общий компонент. Если сотни серверов получают сертификаты через один ACME-клиент, один прокси или упираются в общий лимит запросов удостоверяющего центра — сбой такого звена обрушивает все разом, особенно при синхронном перевыпуске, когда все сертификаты нужно заменить

в один день: удостоверяющий центр упирается в `rate limit` и оставляет часть узлов без сертификата.

Разница между тестом и продакшеном — в балансировщике и CDN. На тесте все работает, а в «боевом» контуре ACME-клиент уже получил новый сертификат, но балансировщик продолжает отдавать старый, не перечитывая файл без перезагрузки, или CDN кеширует старую цепочку. Поскольку терминация TLS размазана по балансировщикам и точкам присутствия CDN, обновление при этом происходит не везде.

Отказ от кросс-подписи — угроза для старых устройств

Let's Encrypt прекратил поддержку кросс-подписи с DST Root CA X3 — цепочкой, которая удерживала на плаву старые Android-устройства еще в 2021 году, а длинная цепочка с перекрестной подписью перестала выдаваться в июне 2024-го. Теперь устройства на Android ниже 7.1.1, где набор корней не обновлялся, больше не доверяют собственным сертификатам Let's Encrypt (ISRG Root X1).

В России доля устаревших мобильных устройств выше среднего по Европе и миру. Для финтеха и служб доставки эффект потери доверия — точечный: старое устройство перестает открывать мобильный банк, хотя пользователь «ничего не трогал». Рост обращений носит устойчивый характер: жалобы концентрируются на конкретных старых версиях ОС и моделях смартфонов, ошибка стабильно

воспроизводится на конкретной прошивке и упирается именно в невозможность установить защищенное соединение. Это решается так: сервер собирает телеметрию о версиях клиентов, у которых обрывается TLS-рукопожатие, и использует заранее подготовленную матрицу соответствия «модель устройства + версия ОС — список поддерживаемых корневых сертификатов».

Отзыв сертификатов DigiCert и ложные срабатывания защиты

В апреле 2026 года DigiCert отзывал 60 EV-сертификатов для подписи кода (`code signing`) после целенаправленной атаки на службу поддержки. Злоумышленник через чат поддержки передал сотруднику замаскированный ZIP-файл, получил доступ к кодам инициализации и выпустил сертификаты от имени реальных клиентов DigiCert. Из 27 сертификатов, прямо связанных с атакой, 11 успели подписать вредоносное ПО Zhong Stealer, атрибутируемое группировке GoldenEyeDog/APT-Q-27.

Эффективность такого отзыва на практике ограничена. У DigiCert отзывали именно сертификаты `code signing`, так что вывод «файл перестанет запускаться» тут неточен, все упирается в метку времени. Если подпись заверена доверенной меткой до момента отзыва, то операционная система, скорее всего, продолжит считать ее действительной и после — на момент подписания сертификат был

ПРЕДУПРЕЖДЕНИЕ В БРАУЗЕРЕ — САМЫЙ БЕЗОБИДНЫЙ СЛУЧАЙ ОТЗЫВА TLS-СЕРТИФИКАТА: ЕСТЬ ЧЕЛОВЕК, ОН УВИДИТ ОШИБКУ И ОТРЕАГИРУЕТ. ВСЕ, ЧТО РАБОТАЕТ БЕЗ ЧЕЛОВЕКА В КОНТУРЕ, ОТКАЗЫВАЕТ «МОЛЧА»

легитимен. Рассчитывать, что отозванный сертификат гарантированно заблокирует уже подписанные файлы, нельзя. Конкретный образец вредоносного ПО быстрее заблокирует обновления антивирусных сигнатур и баз данных репутации, без оглядки на статус сертификата. По скорости у отзыва тоже нет гарантий: проверка через списки и OCSP кешируется, часть клиентов проверяет статус редко или никогда, поэтому окно доверия к скомпрометированному сертификату измеряется часами и днями.

Когда антивирус удаляет доверенные сертификаты

Самый показательный инцидент такого типа произошел в конце апреля 2026 года. Обновление сигнатур Microsoft Defender определило два легитимных корневых сертификата DigiCert как троян, и на некоторых системах они были автоматически удалены из хранилища доверенных корней. Взлома не было, но эффект оказался сопоставим с последствиями настоящей атаки: средство защиты само вырезало кусок инфраструктуры доверия и создало собственный радиус поражения.

Белый список сертификатов, которые антивирус не имеет права трогать, — мера правильная, но частная. Проблема глубже, в модели доставки обновлений. Сигнатуры нельзя ставить на критичную инфраструктуру мгновенно — их надо внедрять поэтапно: сначала на тестовой груп-

пе с наблюдением и только потом на всем остальном парке. Удаление объектов из доверенного хранилища тоже не должно выполняться молча — только с подтверждением. И отдельно нужен мониторинг целостности корневого хранилища: любое изменение набора доверенных корней, кто бы его ни внес (в том числе антивирус), обязано немедленно выдавать уведомление.

Молчаливый отказ инфраструктуры

Предупреждение в браузере — самый безобидный случай отзыва TLS-сертификата: есть человек, он увидит ошибку иотреагирует. Все, что работает без человека в контуре, отказывает «молча». mTLS между микросервисами перестает устанавливать соединение, пользователь видит общий сбой без какого-либо упоминания сертификата. VPN-концентратор рвет туннель, и это списывают на сбой сети. Защищенная почта по TLS копит в очереди письма, пока кто-то наконец не заметит задержку доставки. API-интеграции по клиентским сертификатам возвращают ошибку соединения, которую вызывающая сторона трактует как временную недоступность и молча продолжает попытки.

Обнаружение подобных отказов — самая большая операционная сложность. В логах разрыв на уровне TLS похож на обычный сетевой таймаут, сброс соединения или недоступность узла. Отличить отзыв можно, только

заранее собирая телеметрию: детальный код ошибки рукопожатия, мониторинг статуса отзыва и срока действия по всем сертификатам, а также контрольные тестовые сценарии интеграции. Без этого команда узнает об отзыве только из жалоб сотрудников, когда уже потеряны многие часы.

Secure Boot и истечение сертификатов Microsoft

Сроки действия сертификатов Microsoft Secure Boot, выпущенных в 2011 году, начали истекать летом 2026 года. КЕК CA 2011 (ключ обновления списков) истек 24 июня, UEFI CA 2011 — 27 июня, Windows Production PCA 2011 (подпись загрузчика) истечет 19 октября. Для корпоративных парков это означает, что устройства с устаревшей прошивкой перестанут получать критические патчи загрузки и списки отзыва вредоносного ПО (DBX) — базу сигнатур буткистов вроде BlackLotus и BootHole.

Сами устройства продолжают загружаться. Опасность в том, что без действующих сертификатов система перестает получать обновления списка запрещенного к загрузке кода. Парк оборудования, который больше не принимает DBX-обновления, — это фактически инфраструктура с отключенным контролем защиты загрузки и незакрываемым классом угроз.

Ни ФСТЭК, ни Банк России ситуацию типа «истек Secure Boot — значит, есть нарушение» так не определяют. Но на аудите уязвимость увидят.

Требования к защите конечных точек и к управлению уязвимостями подразумевают, что механизмы защиты находятся в актуальном, поддерживаемом состоянии. Аудитор посчитает это недостатком процессов управления уязвимостями и жизненным циклом, а в чувствительных сегментах — риском, требующим компенсирующих мер. Как минимум это приведет к замечанию.

Процесс обновления Secure Boot затрагивает самый нижний уровень — прошивку. На тысячах машин всплывает разнородность парка: разные вендоры и версии UEFI ведут себя по-разному, часть устройств не принимает новый ключ из-за особенностей заводской конфигурации UEFI. Типичный симптом — ошибка в журнале о том, что для устройства не найден подписанный платформенным ключом KEK. Само по себе корректное обновление к невозможности загрузки не ведет, но в связке с одновременным включением проверки в firmware или сырым обновлением UEFI «окирпичить» машину можно. Для удаленных станций это опасно вдвойне: при сбое на этапе загрузки физического доступа нет, а средства удаленного управления до старта системы могут быть недоступны. Массово такое не ставят сразу на все «железо» — только поэтапно, начиная с тестовой группы по каждой модели отдель-

но и со сверкой статуса по журналам. Обязательны свежие резервные копии и проверенный носитель восстановления, а границу обратимости отката следует заранее выяснить у вендора: часть шагов через настройки UEFI можно отменить, часть — нет.

НУЦ Минцифры в машинных интеграциях

На фоне санкций и ухода части иностранных удостоверяющих центров из России компании все чаще используют сертификаты НУЦ Минцифры. Но стандартный софт по умолчанию их не признает и работать с ним отказывается — поддержку таких сертификатов приходится встраивать и в окружение, и в код вручную.

Вот недавний кейс из нашей практики: на одном из проектов без видимой причины начали падать платежные сервисы. Диагностика показала, что проблема не только у нас, но и по всему Рунету. Оказалось, «Т-Банк» перевел свои сервисы на TLS-сертификат от НУЦ Минцифры. Корень этой цепочки — самоподписанный сертификат Russian Trusted Root CA, которого нет ни в стандартном наборе доверенных корней Debian, ни в библиотеке Certifi, ни в других популярных наборах. Для стандартной SSL-библиотеки он неотличим от обычного самоподписанного, которому никто до-

верия не дал. OpenSSL находит в цепочке корень, которому не доверяет, и рвет соединение. Возникают массовые ошибки.

Ситуацию усугубил поэтапный переход: сертификаты меняли по очереди, и сбой растянулся на 3–4 дня. Когда на одном узле цепочка уже была новой, а на соседнем — старой, диагностика превращалась в головоломку: часть вызовов проходила, часть нет, и причина была неочевидна.

Сервер secured-openapi.tbank.ru начал отдавать цепочку с самоподписанным корнем Russian Trusted Root CA. Те, у кого этого корня не было в доверенных, получали ошибку. Пришлось вручную добавить корень во все задействованные системы, изменить логику работы с цепочками и протестировать интеграции. Для поддержки это стало серьезным объемом внеплановой работы, возникшим совершенно внезапно.

Архитектуру стоит разделить по аудитории — она неизбежно становится гибридной. Для публичных сервисов, рассчитанных на российских пользователей, применение сертификатов НУЦ оправдано, а для машинных интеграций с зарубежными системами нужен коммерческий сертификат, принимаемый по умолчанию везде. Так что практический подход в том, чтобы иметь два набора серти-

ДЛЯ ПУБЛИЧНЫХ СЕРВИСОВ, РАССЧИТАННЫХ НА РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ, ПРИМЕНЕНИЕ СЕРТИФИКАТОВ НУЦ ОПРАВДАНО, А ДЛЯ МАШИННЫХ ИНТЕГРАЦИЙ С ЗАРУБЕЖНЫМИ СИСТЕМАМИ НУЖЕН КОММЕРЧЕСКИЙ СЕРТИФИКАТ, ПРИНИМАЕМЫЙ ПО УМОЛЧАНИЮ ВЕЗДЕ

СЕРТИФИКАТ — ЭТО ТА ТОЧКА, ГДЕ СХОДЯТСЯ ДОСТУПНОСТЬ, БЕЗОПАСНОСТЬ И СООТВЕТСТВИЕ ТРЕБОВАНИЯМ, И ЕЕ ОТКАЗ МОЛЧА РАСХОДИТСЯ ПО ВСЕЙ СИСТЕМЕ

фикатов: один для российского контура, другой для внешних интеграций.

Регуляторная ответственность

Российский регулятор (Банк России, ФСТЭК) требует шифрования каналов передачи данных. При отзыве или истечении сертификата организация формально перестает выполнять это требование, даже если разрыв длится всего несколько часов. Ответственности за то, что канал несколько часов был недоступен из-за истекшего сертификата, в явном виде не предусмотрено. Но есть два реальных типа последствий.

Во-первых, если в момент сбоя через незащищенный канал произошла утечка или инцидент — спрашивать за них будут, и там ответственность уже ощутимая. Во-вторых, регулярные истечения и отзывы сертификатов без их отлаженной замены аудитор справедливо прочтает незрелостью процессов управления.

Прямой запрет в политике ИБ на использование сертификатов без механизма оперативной замены разумен, но сформулировать его лучше как рабочее требование:

- у каждого сертификата есть владелец и определенный срок;
- автоматический перевыпуск действует с запасом;
- для всех сертификатов с назначением и зависимостями ведётся ведётся реестр;

- приближение срока мониторится с заблаговременным оповещением.

Тогда истечение срока действия одного из сертификатов перестает быть сюрпризом.

Скрытые зависимости и сегментация доверия

Многие IoT-устройства и сетевое оборудование имеют встроенные сертификаты с фиксированным сроком действия, но без функции автоматического обновления. Когда корень, которым они подписаны, отзывается или истекает, а механизма обновления нет, устройство не чинится штатно — оно перестает устанавливать доверенные соединения. Сотня датчиков, шлюзов или сетевых железок разом теряет связь с управляющим сервером, и починить это удаленно не получится: обновление корней либо не предусмотрено, либо требует физического доступа и перепрошивки. По трудозатратам это худший сценарий: руками и поштучно. Выявлять такие устройства нужно заранее, и единственный действенный способ — инвентаризация, подразумевающая полный реестр парка. По каждому классу устройств должно быть установлено, каким корням они доверяют, когда эти корни и встроенные сертификаты истекают и есть ли у них механизм обновления.

Второй пласт: сертификаты применяются не только для TLS, но и для подписи кода, документов (ЭЦП), аутентификации в системах контроля

доступа (smart-карты и токены). Один удостоверяющий центр или один корень нередко обслуживает сразу несколько разных по назначению зон. Пока все хорошо, такая экономия выглядит удобной. Но в момент компрометации или отзыва корня встают все процессы, которые на нем замкнуты. Единая точка доверия превращается в единую точку отказа.

Сегментация доверия здесь так же необходима, как и сегментация сети, но применительно к PKI (Public Key Infrastructure — инфраструктура открытых ключей). Разные по назначению зоны должны опираться на разные цепочки и по возможности на разные удостоверяющие центры. Тогда отзыв в одной зоне приводит только к локальному сбою. Решением становится уже упомянутый реестр, который показывает, какой корень какие процессы обслуживает.

Сертификат часто воспринимают как техническую формальность, мелочь, строчку в конфиге, о которой вспоминают раз в год. А это — та точка, где сходятся доступность, безопасность и соответствие требованиям, и ее отказ молча расходится по всей системе. Защищает ведь не сам сертификат, а зрелость процесса, который за ним стоит: инвентаризация, автоматизация с запасом, сегментация доверия и мониторинг, который оповещает о проблеме раньше, чем начнут жаловаться сотрудники. 📌