

РУБИЛЬНИК ДОВЕРИЯ



Андрей ЖАРКЕВИЧ

эксперт Start X,
ведущий рубрики
BIS Journal

13 июня 2026 года в 04:10 по московскому времени GlobalSign, один из крупнейших удостоверяющих центров мира, начал поэтапный принудительный отзыв TLS-сертификатов у российских компаний. Почти сразу клиенты Т-банка получили SMS с предупреждением о возможных проблемах при входе на российские сайты. К утру тысячи доменов могли встретить посетителя предупреждением «соединение не защищено».

При этом не был взломан ни один алгоритм. RSA остался стойким, TLS — корректным, подписи — валидными. Сломалось не шифрование. Сломалось то, что десятилетиями принималось как данность, — независимость глобальной инфраструктуры доверия от политики. Выяснилось, что доверие, на котором держится весь защищённый интернет, можно отозвать под давлением отдельных государств, и криптография тут бессильна.

И это, как ни парадоксально, и есть человеческий фактор, только в глобальном масштабе. Не пользователь, передавший пароль фишинговому сайту, а люди, которые надавили на других людей, в чьих руках находится рубильник управления доверием.

В этой статье мы поговорим не столько о криптографии, сколько о людях вокруг неё. О том, как доверие, на котором строился защищённый интернет, стало рычагом внешней политики и о том, к чему это может привести.

ЧТО ПРОИЗОШЛО

За месяц с небольшим произошло три значимых события. Первые два подготовили почву, а третьим стал тот самый отзыв сертификатов 13 июня, с которого мы начали. В результате из рядовых новостей сложилась довольно тревожная история.

4 мая 2026 года вступили в силу обновлённые требования международного консорциума CA/Browser Forum — органа, который

задаёт правила выпуска публичных сертификатов. Проверка заявителей по санкционным спискам (OFAC SDN List и BIS Denied Persons List в США, плюс европейские аналоги) из рекомендательной стала обязательной. Удостоверяющим центрам прямо запретили обслуживать тех, кто в эти списки попал.

4 июня Let's Encrypt обновил пользовательское соглашение до версии 1.7. Теперь подписант отдельным пунктом гарантирует, что не находится под комплексными санкциями и экспортным контролем США. Не связанных с государством сайтов в России и Иране это пока не касается: в санкциях США есть отдельное послабление на базовые средства интернет-связи, к которым отнесли и сертификаты. А вот государственным структурам выдачу закрыли.

13 июня от слов перешли к делу: GlobalSign, принадлежащий японской GMO Internet Group и обязанный соблюдать санкции, после аудита своего портфеля запустил отзыв выданных сертификатов. Оценки масштаба бедствия расходятся сильно — от «менее 5% сегмента» в формулировке Минцифры до 15–20 тысяч доменов второго уровня и миллионов поддоменов в оценках участников рынка. Российская «дочка» японского УЦ заявила, что у неё «нет ни юридических, ни технических рычагов влияния на решения консорциума».

Рычагов нет не только у российского офиса. Их нет ни у одной из сторон, которых это решение касается.

НЕДОВЕРИЕ НА УРОВНЕ ЛЮДЕЙ

Мы привыкли думать, что доступность сайта — вопрос техники. Сервер жив, канал доступен, сертификат не просрочен, значит, всё работает. Санкционный отзыв ломает это представление: с сайтом всё в порядке, а браузер всё равно встречает посетителя предупреждением о небезопасности. Не потому, что что-то сломалось, а потому, что кто-то решил больше ему не доверять.

Проблема в том, что доверие браузера к сайту — не физическое свойство и не результат вычислений. Это чьё-то однажды принятое решение. А раз доверие — решение, то и недоверие — тоже. И формулируют это решение живые люди.

Это и есть человеческий фактор, только не там, где мы привыкли его искать. Не пользователь поленился и не админ забыл — наоборот, всё сделано аккуратно и по процедуре.

Эта процедура позволяет административным решением лишить сайт доверия, несмотря на то, что ни сервер, ни канал, ни шифрование не взломаны и технических причин для отказа в доверии нет.

ПОЧЕМУ РУБИЛЬНИК В ОДНИХ РУКАХ

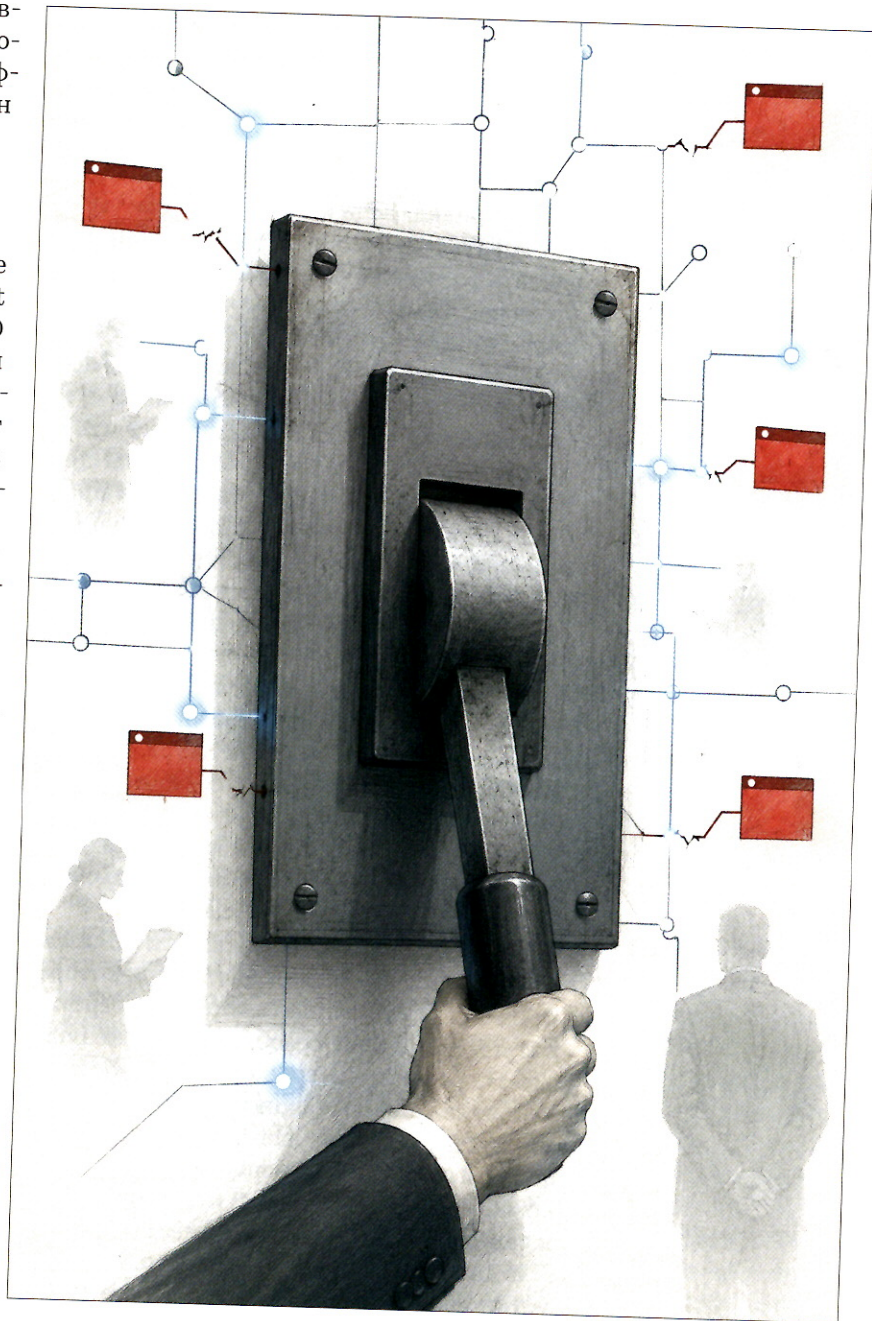
Сами удостоверяющие центры — это обычные частные компании в разных странах: DigiCert и Sectigo в США, GlobalSign под японской GMO Internet Group, Let's Encrypt под американской некоммерческой ISRG. Никакого надгосударственного статуса у них нет. Они выпускают сертификаты, но ценность сертификата не в самом файле, а в том, что браузеры ему доверяют. И это доверие УЦ не принадлежит.

Кому будет доверять браузер, определяет встроенный в него список доверенных удостоверяющих центров. Де-факто в мире есть четыре основных браузера и, соответственно, четыре таких списка, определяющих, кому можно доверять в вебе. Давайте перечислим их поимённо: Microsoft Edge, Apple Safari, Google Chrome и Mozilla Firefox. Три американские корпорации и американская же некоммерческая организация.

Чтобы значиться в списках, удостоверяющий центр обязан выполнять требования этих организаций, а они включают в себя соблюдение правил CA/Browser Forum и ежегодный аудит. Удаление УЦ из такого списка означает, что все выданные им сертификаты почти мгновенно превращаются в тыкву. И браузер выражает крайнюю степень недоверия всем сайтам, получившим сертификат в провинившемся УЦ.

У самого CA/Browser Forum властных полномочий нет, поскольку это не государственный орган, а отраслевое объединение, и его решения формально никого ни к чему не обязывают. Правила в нём принимают голосованием двух палат — удостоверяющих центров и браузеров. Но обязательными эти правила делают именно браузеры: они держат эти списки, поэтому соблюдать решения форума приходится всем, кто хочет в них остаться. Выйти из системы нельзя — ни обходного пути, ни апелляции для отдельной компании не предусмотрено.

Откуда тогда приоритет одной страны? В правилах его нет. Неравноправие нигде не записано, оно следует из географии. Списки доверенных центров ведут компании под юрисдикцией США. Американские санкции экстерриториальны — они дотягиваются до любой иностранной компании через сотрудников с гражданством США, техноло-



гии американского происхождения и, главное, через доллар. Любой, кто ведёт расчёты в долларах, рискует быть отрезанным от финансовой системы США, а к этому не готов почти никто.

Так и выходит, что в одних руках оказались сразу два рубильника — доверие и деньги. Евросоюз тоже вводит санкции, и формально GlobalSign ссылалась на обязательства перед ЕС. Но тон задаёт Вашингтон, потому что только у него оба рычага одновременно.

ЧЕМ ОПАСЕН ОБХОДНОЙ ПУТЬ

Что предлагают сделать, когда сертификат отозван и сайт не открывается? Самому скачать и установить на компьютер корневые

сертификаты Национального удостоверяющего центра. Пока это единичные инструкции для отдельных сайтов, но если отзывы сертификатов станут массовыми, может появиться соблазн превратить такой обходной путь в стандартное решение. И тут начинается зона риска. Ведь когда такие советы станут давать в масштабе страны, мы рискуем сделать то, чего не добились ни одна мошенническая кампания, — приучить миллионы людей вести себя небезопасно.

Годами индустрия выстраивала рефлекс: красное предупреждение браузера — это стоп-фактор. Не ходи дальше, тут что-то не так. На этот рефлекс потрачены десятилетия человеко-часов, миллионы предупреждений и немало болезненных уроков. А сейчас мы можем уничтожить его одной фразой: «красная плашка — это норм, просто санкции подкрались незаметно, смело жмите „Да“».

Разница с привычным человеческим фактором — в масштабе и в источнике. Раньше мы говорили про условного Петра, который не справился с шифрованием или поверил красивому лендингу. А тут к опасному поведению можно склонить миллионы граждан, причём сделает это не злоумышленник, а авторитетный голос государства.

Самое печальное, что риски эти не сиюминутные, а отложенные. Сайты, ради которых придётся устанавливать корневые сертификаты НУЦ, вполне безобидны и даже полезны. Но рефлекс не срабатывает выборочно. Человека, которого однажды научили игнорировать предупреждение и ставить сертификаты по указанию сверху, тем же способом обманут завтра, причём в ситуации, которая к санкциям отношения не имеет.

И даже это не вернёт главного. Массовая установка корневых сертификатов НУЦ в лучшем случае откроет сайты тем, кто послушно это сделал, — но глобальное доверие к самим сайтам так и останется отозванным. Пока есть время сделать нормальное безопасное решение, превращать обходной путь в норму — очень нехороший прецедент.

ПОДАРОК АТАКУЮЩЕМУ

И тут всплывает то, что превращает неудобство в прямую угрозу. Для пользователя сайт с отозванным из-за санкций сертификатом и фишинговый ресурс выглядят совершенно одинаково: красная плашка и кнопка «всё равно перейти». Подменил ли злоумышленник сертификат на пути к банку или его отозвали из-за санкций, человек не поймёт. А значит, любой повод нажимать

«да», который мы ему дадим, сработает на руку атакующему.

Фишинг и перехват трафика получают идеальную легенду. «Сертификат не распознан? Это из-за санкций, установите наш корневой сертификат и продолжайте». Фраза, которая, возможно, прозвучит с официальных трибун, сразу же превратится в инструмент мошенников. Человеческий фактор здесь не побочный эффект, а несущая конструкция: всё держится на том, что люди не видят разницы между отозванным сертификатом и атакой с подменой сертификата. А обходной путь, утверждённый в качестве нормы, эту слепоту только усилит.

ЕСТЬ ЛИ У РОССИИ СВОЙ ОТВЕТ?

У России на этот случай вроде бы есть туз в рукаве в виде Национального удостоверяющего центра, который бесплатно выдаёт сертификаты через «Госуслуги». Но выпуск сертификатов никогда и не был проблемой. Проблема в доверии. Мировые браузеры не доверяют НУЦ, а значит, и любому выданному им сертификату. Чтобы сайт с таким сертификатом открылся в обычном браузере, пользователю придётся вручную установить корневые сертификаты НУЦ, то есть пройти тем самым обходным путём, цену которого мы уже обсудили.

Есть и другое решение — использовать отечественные браузеры, где НУЦ в списке доверенных УЦ присутствует изначально. В самом деле, у нас же есть Яндекс Браузер, в котором российские сайты открываются без ошибок. Это выглядит более разумно, чем приучать каждого вручную устанавливать корневые сертификаты.

Но несмотря на все преимущества, Яндекс Браузер — это решение для своих. Иностранец не станет ставить российский браузер ради одного сайта, так что для внешней аудитории сайт с сертификатом НУЦ так и останется сломанным. Российский браузер — остров, а не мост.

Да и доверие никуда не вернулось, оно просто переехало: раньше пользователь должен был сам довериться НУЦ, теперь за него это сделал производитель браузера. Точка концентрации доверия не исчезла, сменился лишь тот, в чьих она руках. А заодно остаётся и человеческий фактор, только в более мягкой форме: «не открывается сайт — поставь специальный браузер». То есть пользователь закрепляет в сознании, что ошибка сертификата — это вопрос выбора программы, а не сигнал тревоги.

Так что российские браузеры снимают остроту, но не проблему. Доступ внутри стра-

ны они латают, но независимость доверия остаётся утраченной.

А В ПРИЛОЖЕНИЯХ КНОПКИ «ВСЁ РАВНО ПЕРЕЙТИ» НЕТ

Стоит упомянуть, что TLS-сертификатами пользуются не только браузеры. Мобильные приложения тоже проверяют сертификаты серверов. Так, к примеру, приложение онлайн-банка может убедиться, что подключилось к настоящему банку, а не к подставному узлу. Многие приложения идут дальше и заранее встраивают сертификат своего сервера в код. В этом случае соединение установится, только если на том конце правильный сервер.

Пока сертификаты числятся в доверенных, всё работает. Но стоит сертификат отозвать или заменить на выданный НУЦ, которому приложение и система не доверяют, соединение не установится. И здесь, в отличие от браузера, у пользователя нет спасительной кнопки «всё равно перейти». Приложение не покажет диалог и не предложит принять риск и продолжить, скорее всего, оно молча перестанет работать. Человек даже не поймёт, в чём дело — то ли приложение зависло, то ли белые списки включили.

СЕТЬ РАССЫПАЕТСЯ НА ОСКОЛКИ

Любой отзыв доверия бьёт по самой идее единой сети: Россия лишается доверия мировых центров, а остальной мир — доверия к российским сайтам. Между сегментами сети вырастает стена.

К сожалению, это не разовый сбой, а очередной этап давно идущего процесса. Сначала были геоблокировки: сайты стали ограничивать посетителей с IP из «неправильных» стран. Теперь к ним добавилось доверие, нарезанное по юрисдикциям. Глобальная сеть, которую задумывали единой, на глазах распадается на слабо связанные «суверенные» сегменты, у каждого из которых свой список тех, кому он верит. Внутри сегмента всё работает, на стыках — красная плашка.

Разделять и властвовать получается не всегда. Давить через сертификаты на Китай — крупнейший интернет-рынок планеты — никто не решается. Причина проста: под комплексными санкциями США, в отличие от России и Ирана, его нет. Точечные ограничения против отдельных компаний есть, но отозвать доверие целой стране, глубоко вплетённой в мировую экономику, означает ударить по самим себе. Китай слишком большой, чтобы безболезненно отрезать его.

К тому же Китай к такому развитию событий подготовился. В 2015 году Google и

Mozilla уже исключали из числа доверенных китайский центр CNNIC — тогда писали, что причиной стал выпуск сертификата, с помощью которого перехватывали трафик. Урок Пекин усвоил и сделал ставку на собственную криптографию и центры доверия. Сегодня у него, по сути, свой остров, отрезать который куда сложнее. А вот Россия пришла к тому же рубежу налегке.

ЧТО С ЭТИМ ДЕЛАТЬ

Полностью убрать политику из инфраструктуры доверия вряд ли удастся. Но смягчить ущерб для людей возможно.

Перечислю то, что кажется разумным:

- ♦ не строить пользовательский сценарий вокруг «проигнорируйте ошибку» — любой UX, легализующий обход предупреждений, работает против вас в долгосрочной перспективе;
- ♦ если выполнять миграцию на НУЦ, то с проверяемым каналом доставки — пользователь должен иметь возможность убедиться, что доверяет настоящему НУЦ, а не «скачивает откуда-нибудь»;
- ♦ продолжать учить людей, что предупреждение остаётся предупреждением — даже в эпоху деглобализации интернета красную плашку не стоит игнорировать;
- ♦ провести инвентаризацию внешних зависимостей от иностранных удостоверяющих центров, чтобы очередной отзыв доверия не застал врасплох и не толкнул к панической обходной инструкции, написанной на коленке;
- ♦ разделять публичный TLS и внутренний PKI — у них разные модели угроз и разная цена ошибки.

Криптографии в этом списке нет. Только люди и процессы вокруг неё.

ВМЕСТО ВЫВОДА

С математикой у нас всё хорошо. Алгоритмы по-прежнему стойкие, протоколы корректные, подписи работают без сбоев. Проиграть в этой истории мы можем не из-за стойкости или несuverенности шифра, а из-за того, что официально научим десятки миллионов человек не доверять сигналам тревоги.

Санкции на сертификаты бьют не по криптографии, а по рефлексам пользователей. И если в ответ мы приучим людей не верить предупреждениям браузера, дорожке всего обойдётся не сам отзыв, а страна, разучившаяся пугаться красной плашки. Отзыванные сертификаты заменят, доступ к сайтам наладят. А вот утраченный рефлекс назад уже не вернёшь.