TLS в национальных доменных зонах: статистика, риски, импортозамещение

Никита Новиков

Менеджер проектов ООО «ТЦИ»

TLS — основа доверия в Интернете

Transport Layer Security обеспечивает два критически важных компонента безопасности: шифрование данных и подтверждение подлинности серверов. Без TLS современный интернет превратился бы в **открытую книгу для злоумышленников**.

Ключевой вопрос цифрового суверенитета: кому мы доверяем ключи от нашего цифрового пространства?

Рунет: доверие и суверенитет

Национальные зоны

Более 3 млн сайтов в доменах .RU, .РФ, .SU формируют основу российского Интернета

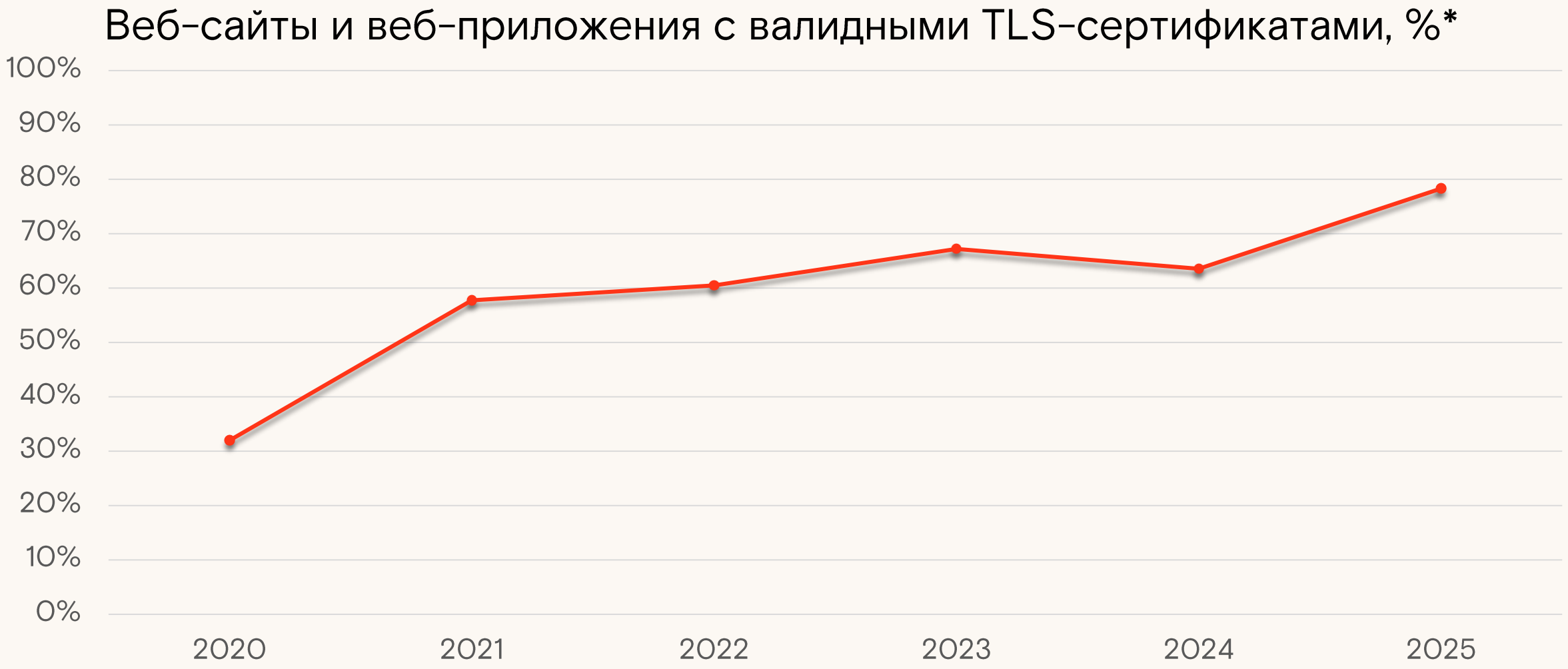
Внешняя зависимость

Более 99% TLS-сертификатов выданы иностранными центрами сертификации

Вопрос безопасности

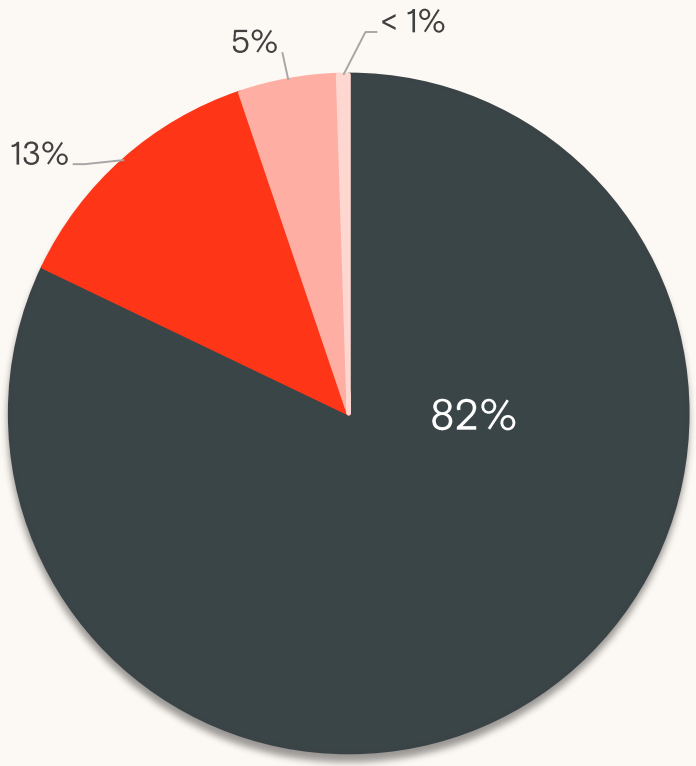
Импортозамещение в сфере TLS становится критически важной задачей национальной безопасности

Сколько сайтов защищено TLS



*Статистика в зонах .RU, .РФ и .SU по данным ресурса «Домены России» (statdom.ru)

Распределение по центрам сертификации



*Статистика за июль 2025 года в зонах .RU, .РФ и .SU по данным ресурса «Домены России» (statdom.ru)

Критическая концентрация

Три крупнейших иностранных центра сертификации контролируют **99% рынка** TLS-сертификатов в российском интернете.

Российские удостоверяющие центры занимают **менее 1%** рынка, что создает катастрофические системные риски для цифрового суверенитета.

Криптографические алгоритмы

77% –17%↓

Доминирующий алгоритм, проверенный временем

22% +17%↑

Быстрорастущая доля, эффективность и скорость

<1%

Используется преимущественно в государственном секторе

Безопасность Рунета в 2025 году

Позитивные тенденции

- 78% сайтов используют HTTPS
- Рост на 17% за три года
- Повышение культуры безопасности

Критические зависимости

- 99% сертификатов от зарубежных ЦС
- Концентрация доверия у трех центров
- Отсутствие резервных механизмов

Российский интернет становится более защищенным, но его безопасность критически зависит от **решений, принимаемых за пределами нашей юрисдикции**.

Cloudflare и Let's Encrypt: первый тревожный звонок

1

Июнь 2025

Введение ограничений Cloudflare для российских пользователей

2

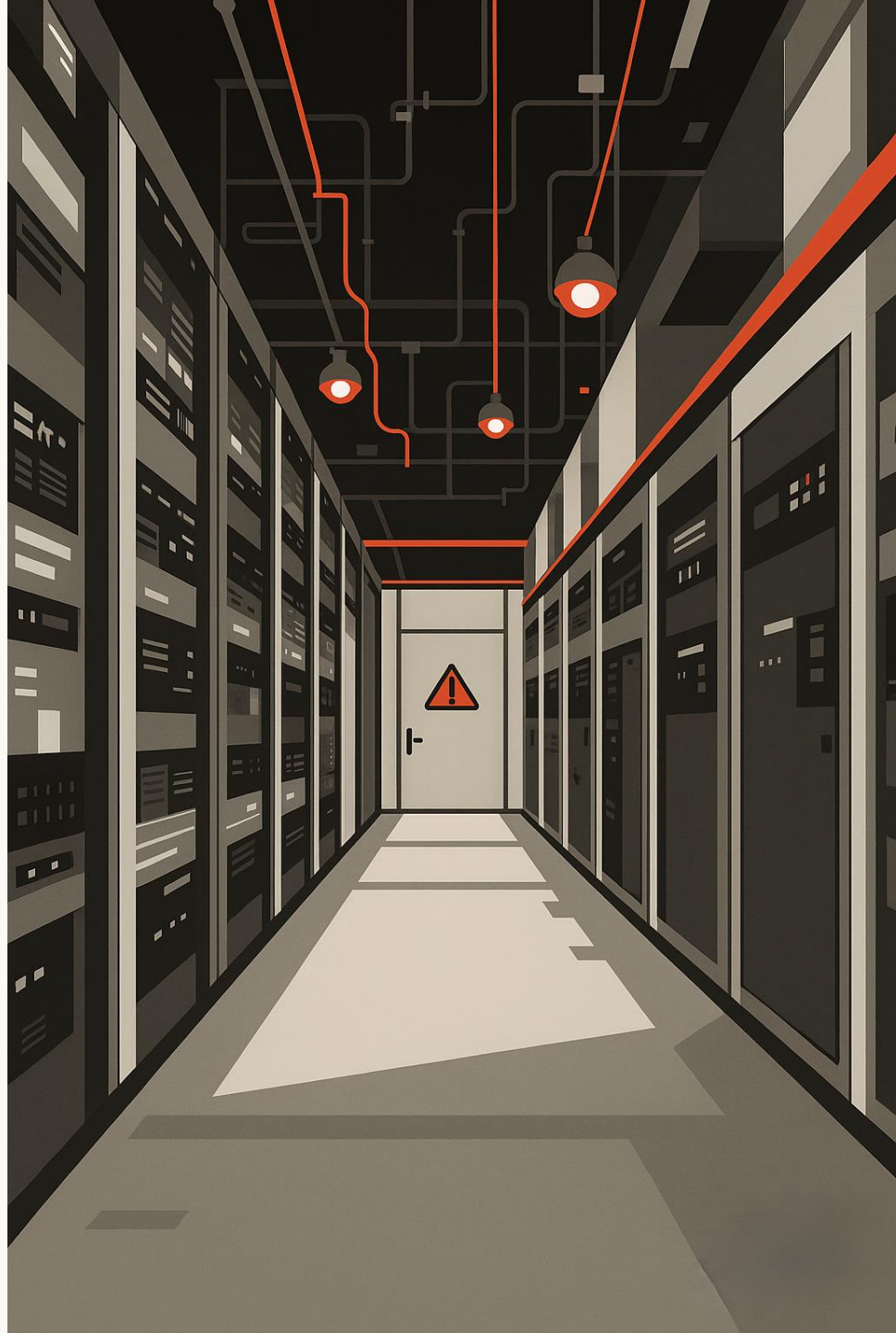
Критическая зависимость

82% сайтов Рунета полагаются на Let's Encrypt через Cloudflare

3

Системный риск

Угроза массового истечения сертификатов и потери HTTPS



90 дней до катастрофы

Короткий жизненный цикл = высокий риск

Современные сертификаты Let's Encrypt действуют всего 90 дней. Любой сбой в цепочке обновления превращается в системную угрозу для миллионов сайтов.

> Когда доверие централизовано, его потеря становится катастрофой для всей экосистемы.

Через 90 дней сайт остаётся без HTTPS

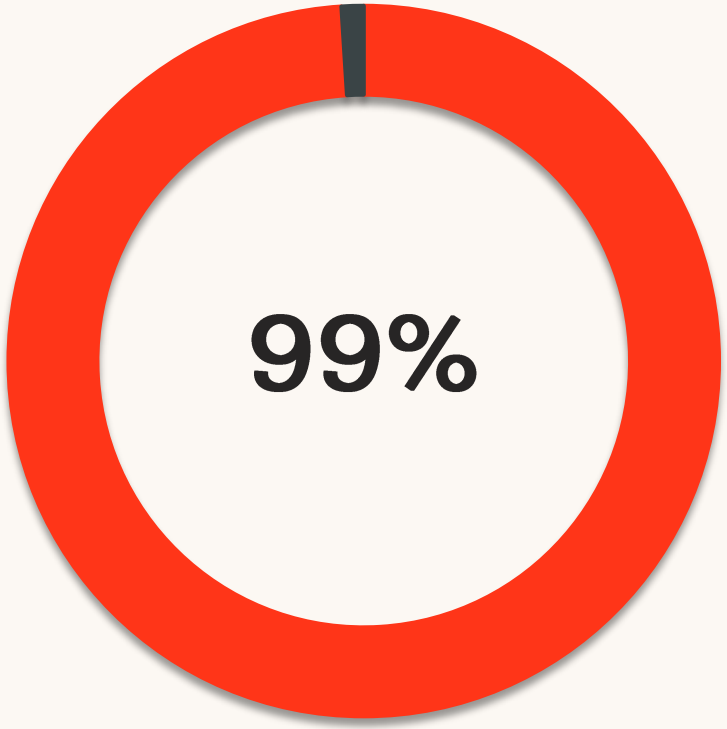
Сайт → Let`s Encrypt → ~~Cloudflare~~ → Браузер

Угрозы, с которыми мы уже сталкивались

Тип угрозы	Потенциальные последствия
Отзыв сертификатов	Мгновенная потеря доступа к защищенным сайтам
Санкции против ЦС	Блокировка всех сертификатов провайдера
Технические сбои	Массовое истечение без возможности обновления
Геополитическое давление	Ограничение доступа к критической инфраструктуре

События лета 2025 года с Cloudflare — очередной звонок. История показывает, что технологические зависимости быстро превращаются в инструменты давления.

Главный риск — зависимость



Доверия
находится под внешним контролем

Решение
извне может обрушить Рунет

⚠ Создание независимой инфраструктуры доверия — не вопрос удобства, а необходимое условие цифровой безопасности государства.

Сертификаты становятся всё короче

2015 — **3 года**
Традиционный срок действия SSL-сертификатов

2018 — **2 года**
Сокращение для повышения безопасности

2020 — **398 дней**
Текущий максимальный срок

2025 — **90 дней**
Стандарт Let's Encrypt

2026 — **200 дней**
Первая волна сокращения

2027 — **100 дней**
Вторая волна сокращения

2029 — **47 дней**
Целевой срок, DCV – 10 дней

Тренд — индустрия движется к максимальной автоматизации

Когда браузеры решают, чей сайт будет жить

На самом деле политику сроков определяет не CA/B Forum, а браузерные вендоры

- Google Chrome — фактический арбитр рынка
- Apple Safari следует стандартам Google
- Mozilla Firefox присоединяется к решениям
- При сроке 10 дней сбой означает мгновенную смерть сайта

Так кто на самом деле контролирует доступ в Интернет?

При коротких сроках действия любой сбой в системе автоматизации приводит к недоступности ресурсов

От разовых продаж к подписке

Раньше

Сертификат на 3 года

Разовая покупка

Минимальное обслуживание

Скоро

Обновление каждые 47 дней

Подписочная модель (квоты)

Постоянная зависимость

Центры сертификации перейдут от разовых продаж к модели MRR (Monthly Recurring Revenue), увеличивая предсказуемость доходов.

Интернет становится менее устойчивым

Растёт зависимость от автоматизации

Короткие сроки требуют безотказных систем обновления

Сбой равен потере доверия

Пользователи видят предупреждения браузера мгновенно

Решения принимаются за пределами РФ

Российские организации не участвуют в определении политик

Как автоматизируют выпуск сертификатов

Боты (certbot)

- Клиентские утилиты
- Работают по расписанию
- Требуют настройки сервера

ACME-протокол

- Стандартизированный подход
- Встроен в инфраструктуру
- Прозрачная автоматизация

⚠ Оба решения разработаны и контролируются зарубежными компаниями

ACME: удобство или риск?

Создан Google/Let's Encrypt

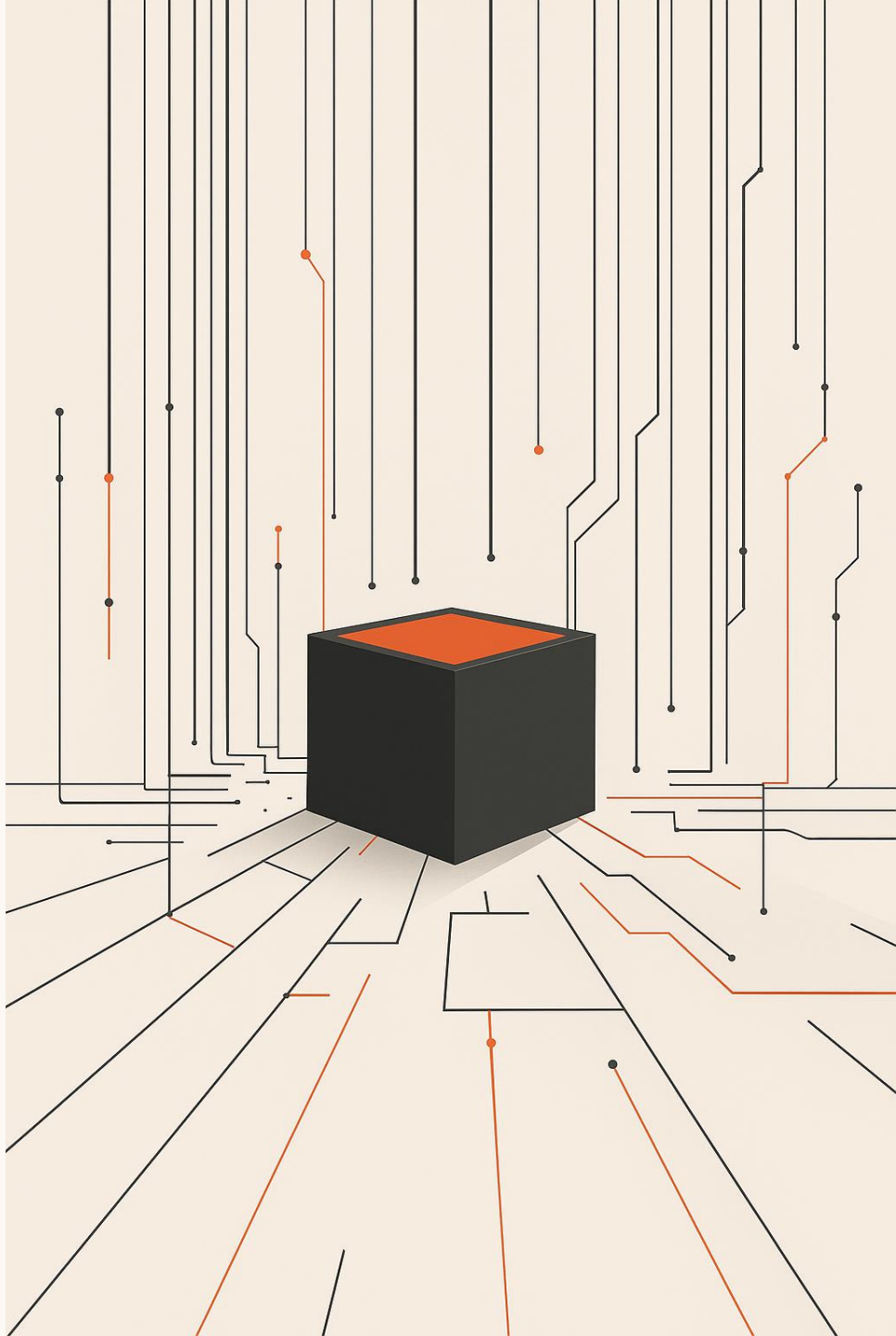
Спецификация и основные реализации от американских компаний

Go-библиотеки, непрозрачность

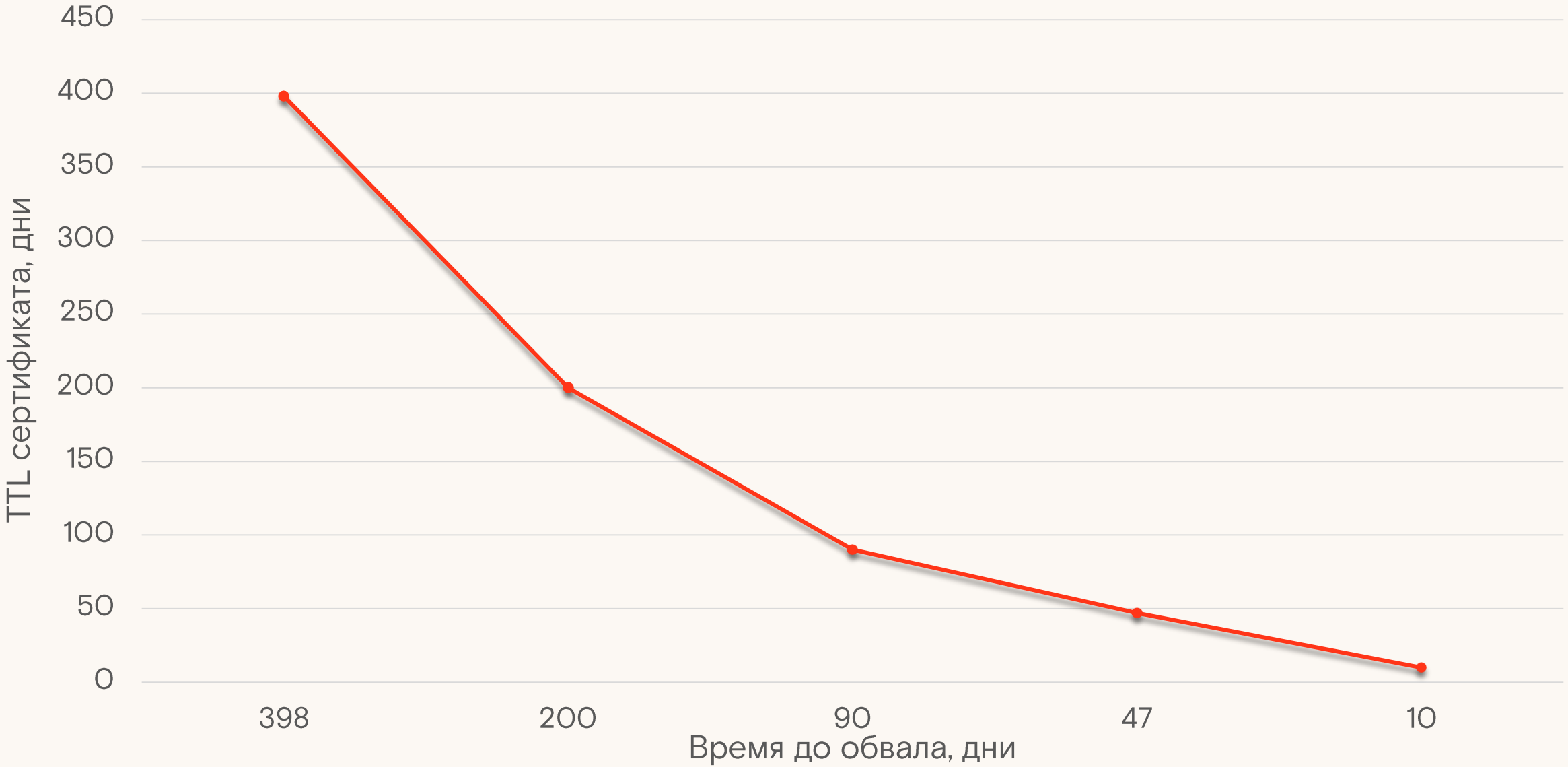
Исходный код доступен, но контроль разработки — у зарубежных команд

Недокументированные возможности

Теоретическая возможность внедрения и использования недокументированного функционала



Чем короче срок — тем выше цена сбоя



Что делать?

01

Отечественные certbot, ACME-клиенты и серверы

Разработка собственных реализаций протокола с открытым исходным кодом

02

Прозрачный код и полный контроль

Аудируемые решения без зависимости от зарубежных разработчиков

03

Интеграция с экосистемой

Встраивание в отечественные ОС, браузеры и хостинг-платформы

04

Оффлайн-выпуск для особых задач

Решения для изолированных инфраструктур и критически важных систем

Автоматизация нужна. Но она должна быть нашей

> **«TLS без автоматизации не живёт.
> И жить он должен в России!»**

Развитие отечественной экосистемы управления сертификатами — вопрос технологической независимости и национальной безопасности.

Архитектура российской PKI

НУЦ

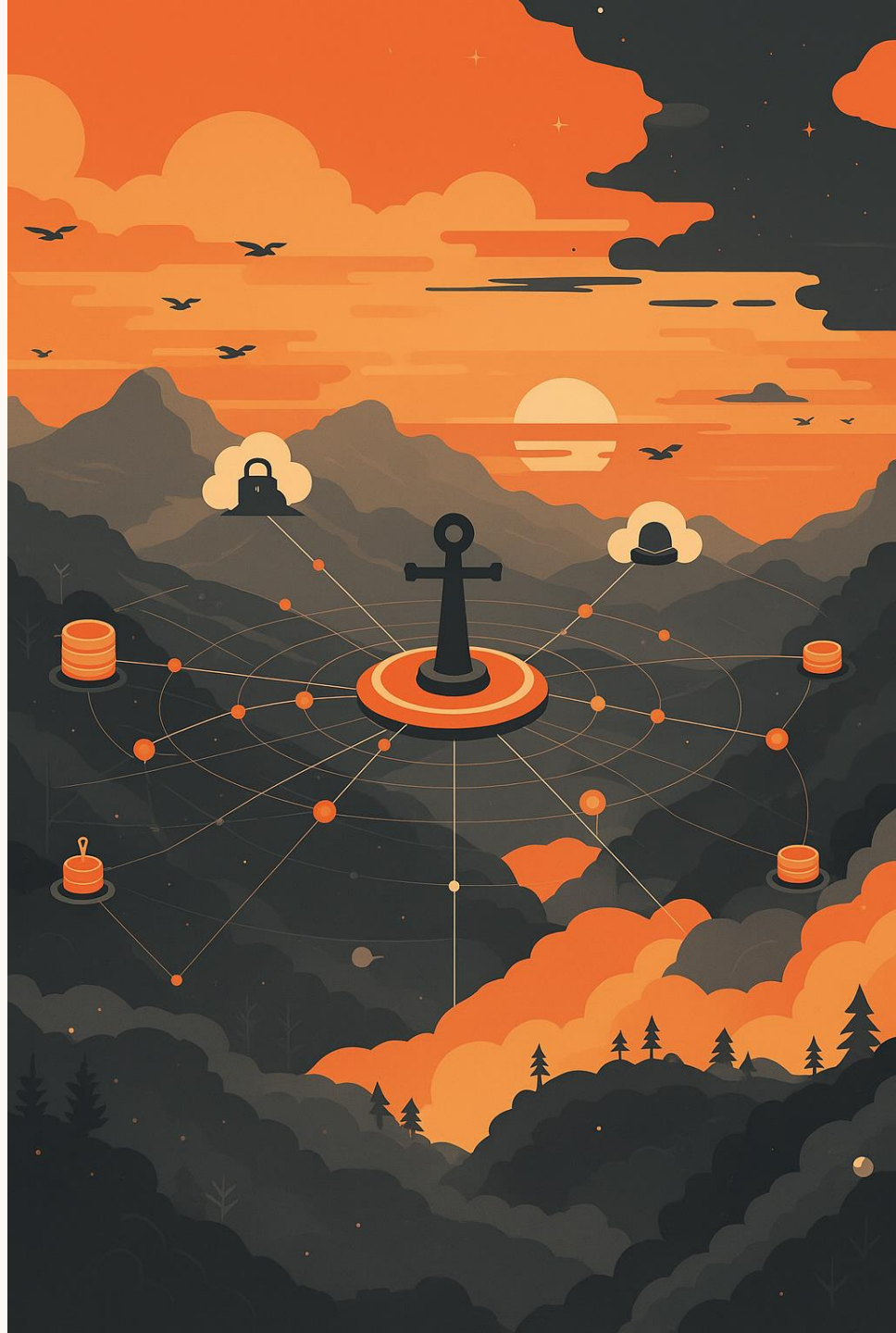
Государственный сектор, основа доверенной инфраструктуры

Частные ЦС

Коммерческие центры сертификации с ограниченной долей

ТЦИ

Ставка на инновации, автоматизацию процессов и поддержку комьюнити и пользователей



НУЦ: надёжно, но не быстро

Сильные стороны

- Государственные гарантии
- Высокий уровень доверия
- Приоритет госуслуг

Ограничения

- DV 90 дней, OV 365 дней
- Выпуск до 5 рабочих дней
- Ручная обработка заявок

Всего выпущено 17 000 сертификатов. Из них действуют сегодня около 5 000*

*По данным ресурса presert.ru

ТЦИ: инновации и автоматизация

Создан в 2022 году по модели Zero Trust

Максимальная автоматизация функций (генерация CSR, проверка домена, tcibot)

Выпуск сертификатов как ECDSA, так и ГОСТ для одного домена и Wildcard

Приоритет – защита сайтов юридических лиц, ИП и физических лиц

Сертификаты сроком на 90 и 365 дней. Срок выпуска – 5 минут

Выпуск сертификатов для электронной почты (S/MIME)

ТЦИ

ЦЕНТР СЕРТИФИКАЦИИ

Что дальше?

1

2026: Автоматизация и новые продукты

Реализация ACME, смена модели оплаты, сертификаты подписи кода

2

2027: Расширенные возможности

Сертификаты SAN, корпоративный TLS и S/MIME, сертификаты для VPN-авторизации

3

2028: Вызовы завтрашнего дня

Постквантовая криптография, сертификаты для программ-агентов

Импортозамещение в действии

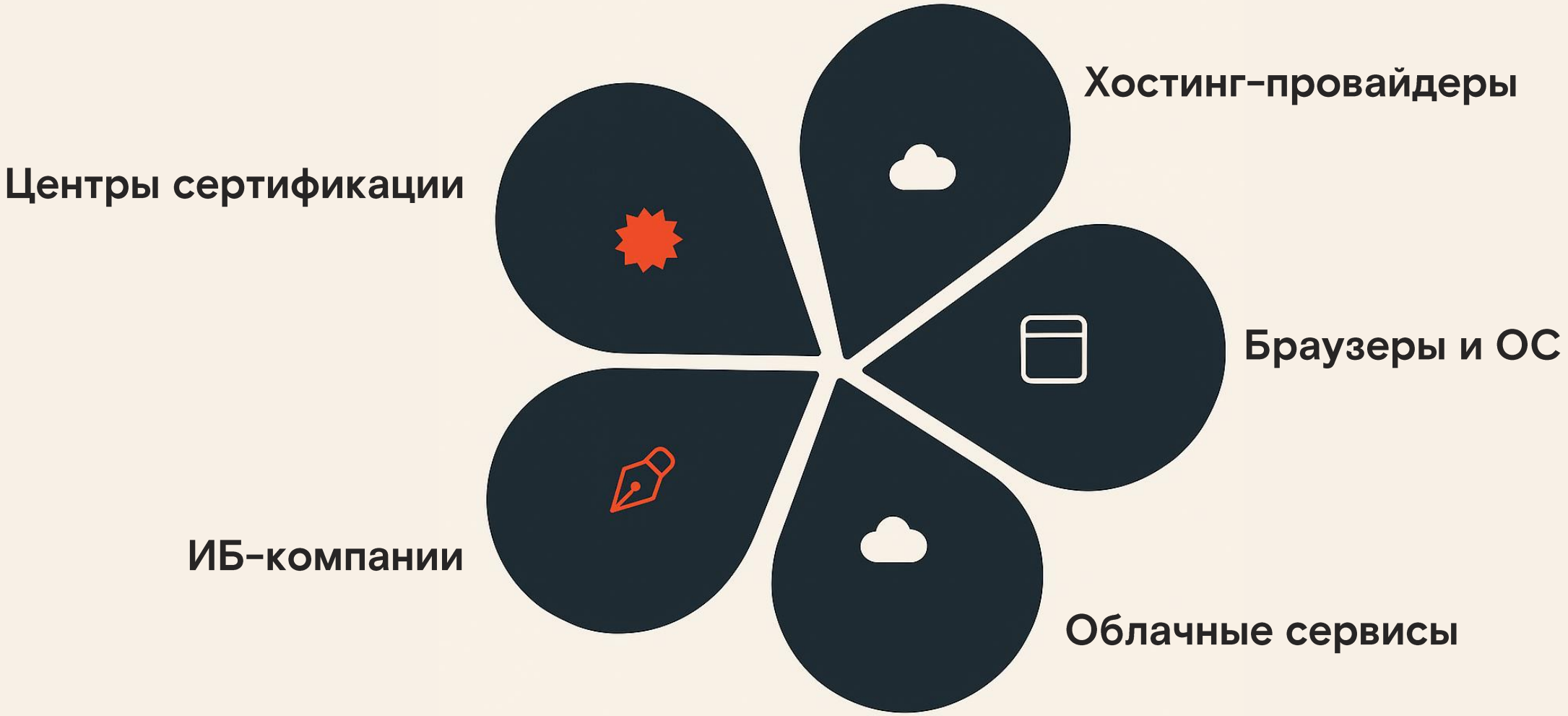
До российских ЦС

- ✗ Зависимость от иностранных ЦС
- ✗ Риски блокировки
- ✗ Длительные сроки выпуска
- ✗ Отсутствие контроля

После внедрения

- ✓ Локальный контроль процессов
- ✓ Высокая скорость выпуска
- ✓ Технологическая независимость
- ✓ Соответствие российским стандартам

Распределённая PKI — наше будущее



Присоединяйтесь к нам!

ТЦИ

Сайт Центра сертификации ТЦИ

tlscc.ru

Сервис аудита безопасности интернет-узлов

audit.statdom.ru

Никита Новиков

novikov@tcinet.ru