TLS в национальных доменных зонах и нормализация данных

Алексей Рогдев

Генеральный директор ООО «ТЦИ»

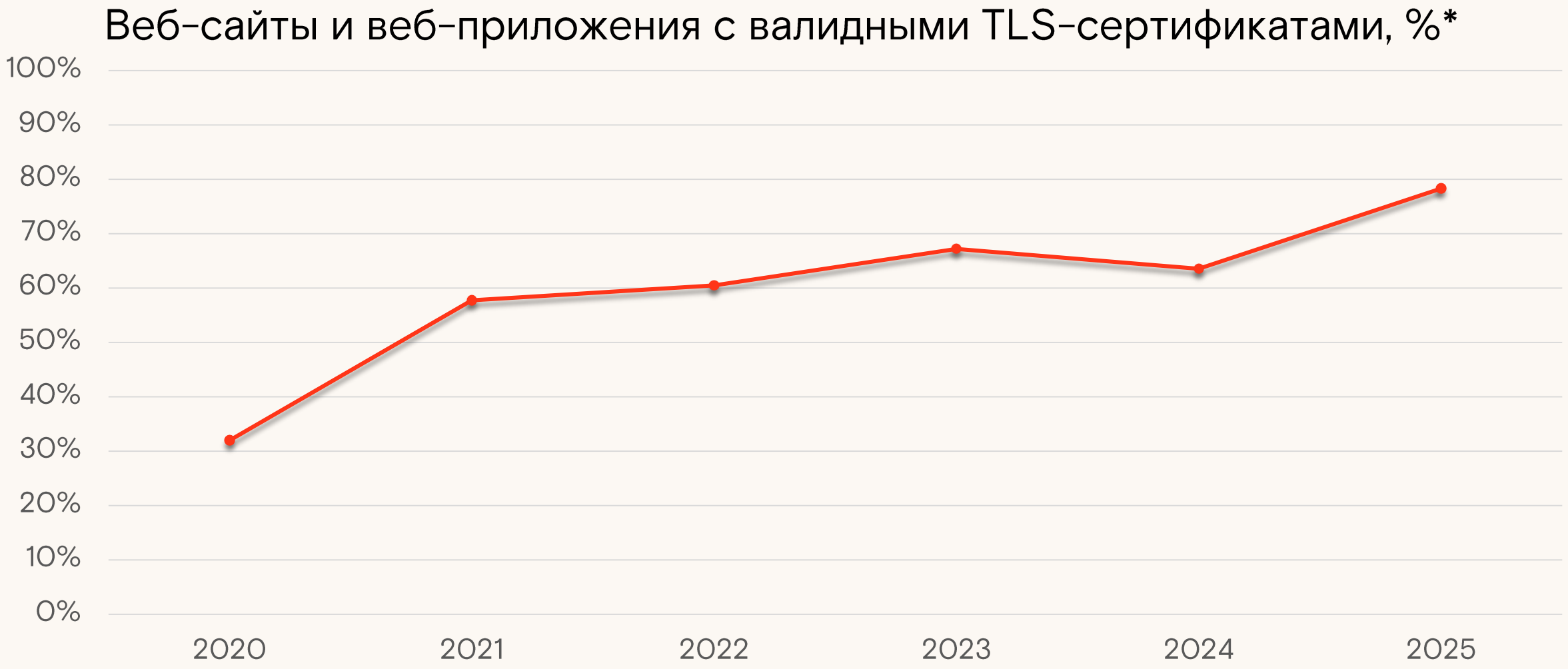
TLS — основа доверия в Интернете

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?

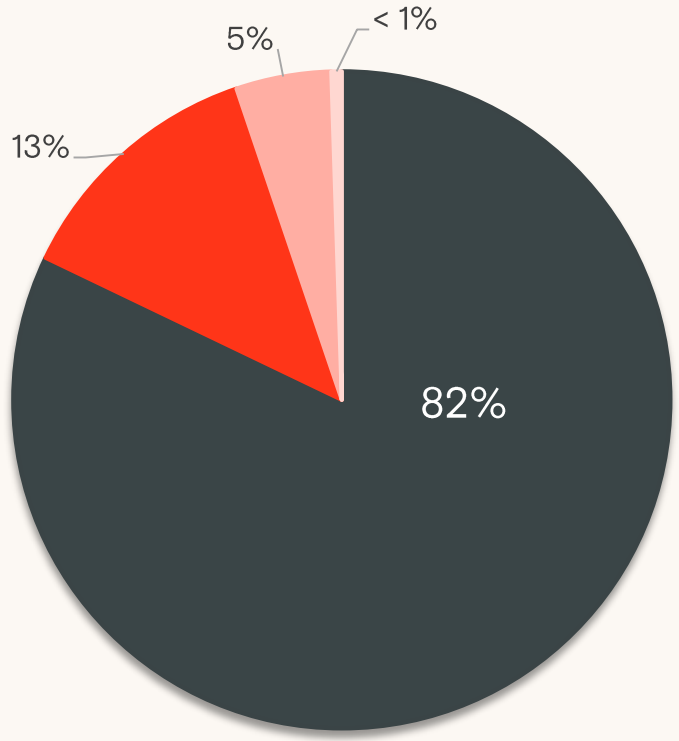


Сколько сайтов защищено TLS



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

Распределение по центрам сертификации



■ Let's Encrypt ■ Google Trust Services ■ GlobalSign ■ Другие

*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.

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

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

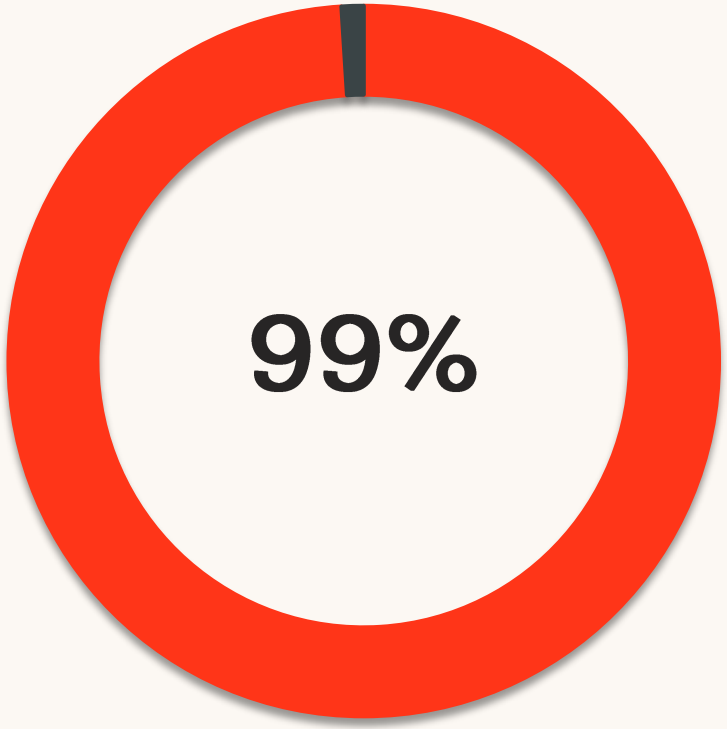
Сайт → Let`s Encrypt → ~~Cloudflare~~ → Браузер

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

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 экосистемы интернета.

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

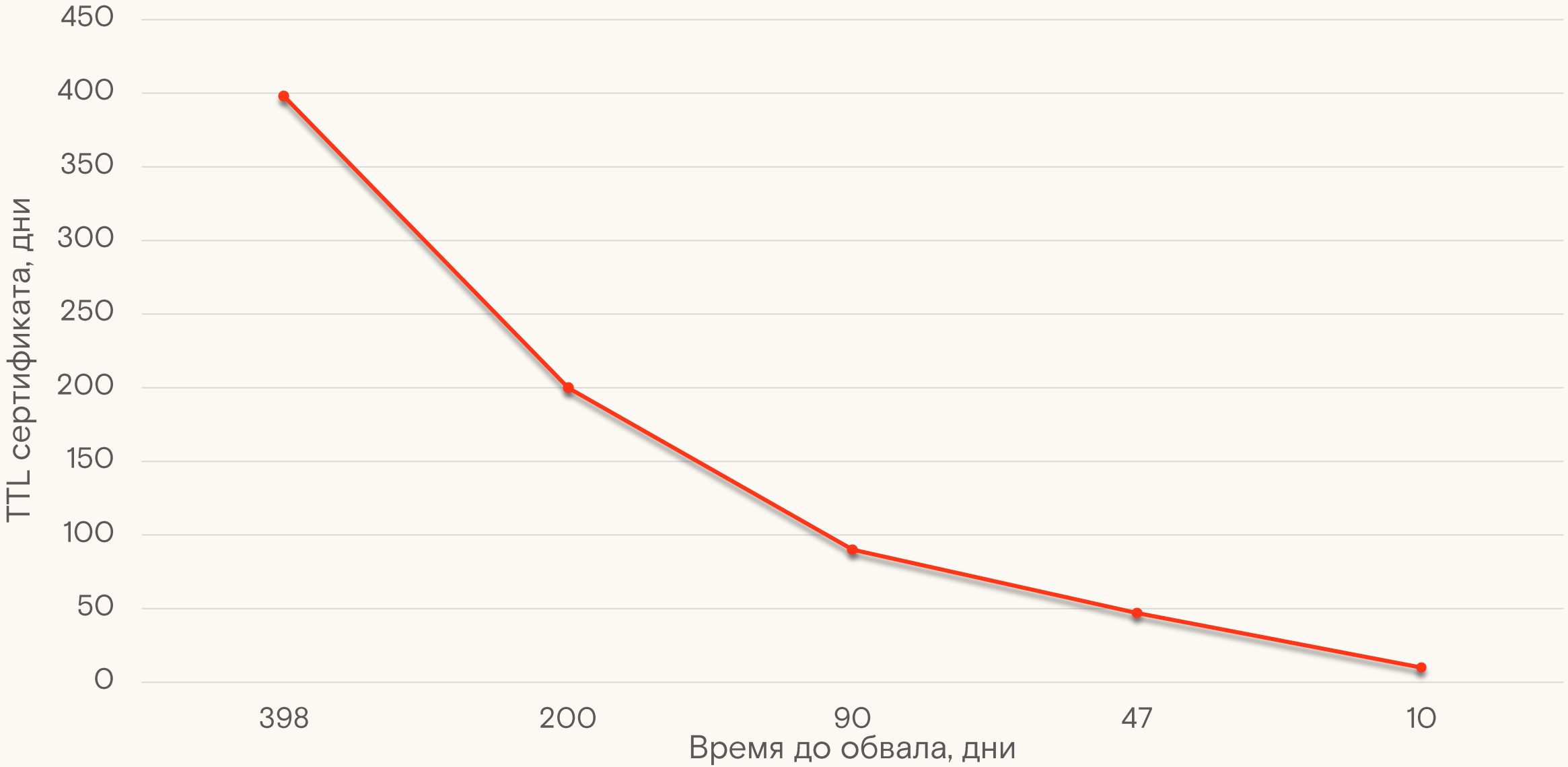
- Google Chrome — фактический арбитр рынка
- Apple Safari следует стандартам Google
- Mozilla Firefox присоединяется к решениям
- При сроке 10 дней сбой означает мгновенную смерть сайта

Так кто на самом деле контролирует доступ в Интернет?



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

Чем короче срок — тем выше цена сбоя



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

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

⚠ Оба решения разработаны и контролируются зарубежными компаниями

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



Архитектура российской PKI

НУЦ

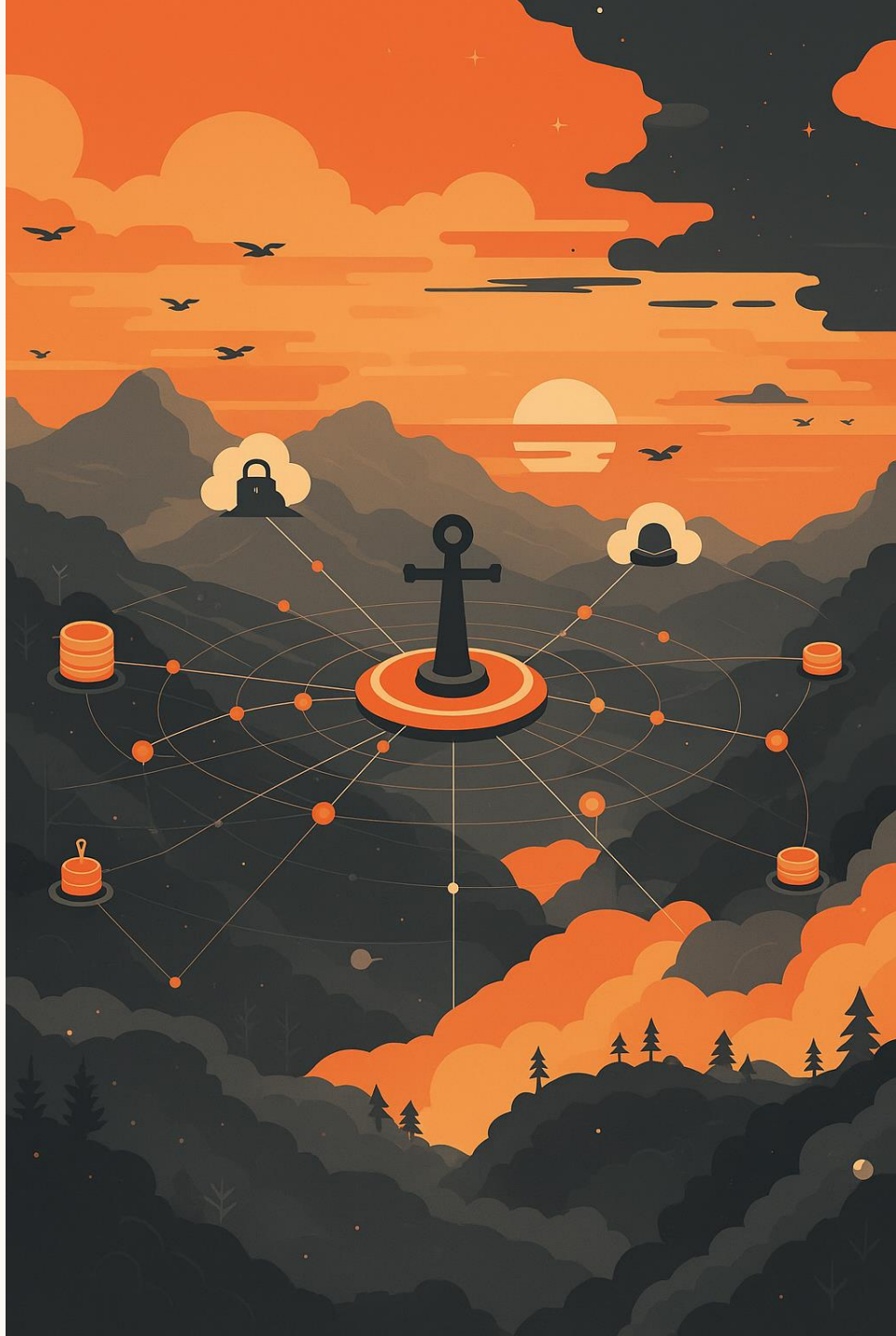
Государственный сектор, основа доверенной инфраструктуры

Частные ЦС

Коммерческие центры сертификации с ограниченной долей

ТЦИ

Ставка на инновации, автоматизацию процессов и поддержку комьюнити и пользователей



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

Импортозамещение в действии

До российских ЦС

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

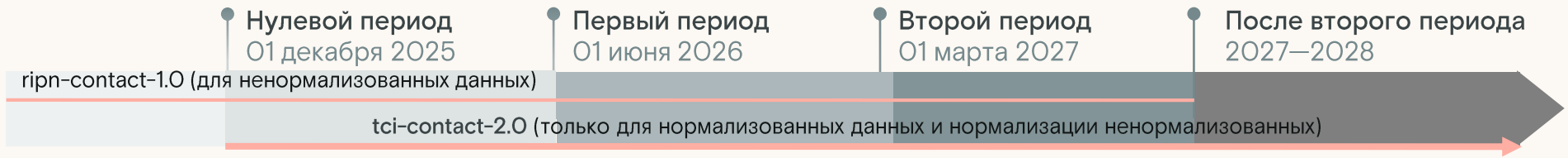
После внедрения

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



Обязательная верификация личности администраторов доменов через ЕСИА

Периоды нормализации данных



№	EPP запрос	Объект Contact	Переходные периоды				
			пред-0	0	1	2	пост-2
1	Create, update contact	Ненормализованный	✚	✚	—	—	—
		Нормализованный	—	✚	✚	✚	✚
2	Create domain	Ненормализованный	✚	✚	—	—	—
		Нормализованный	—	✚	✚	✚	✚
3	Update domain	Ненормализованный	✚	✚	◎	◎	—
		Нормализованный	—	✚	✚	✚	✚
4	Renew domain	Ненормализованный	✚	✚	✚	—	—
		Нормализованный	—	✚	✚	✚	✚
5	Transfer domain	Ненормализованный	✚	✚	—	—	—
		Нормализованный	—	✚	✚	✚	✚

0-й переходный период уже доступен в тестовой среде.
Каждый следующий период будет доступен в тестовой среде с момента старта нового периода.

✚ – разрешен — – запрещен

◎ – изменение атрибута домена registrant разрешено только на ID нормализованного объекта Contact. Изменение атрибута Authinfo запрещено. Изменение остальных атрибутов Domain разрешено.

ТЦИ

Спасибо за внимание.