TLDCON-2021

TLS и Рунет
TLS and RUnet

Александр **Венедюхин**
ТЦИ

ТЦИ

План
Plan

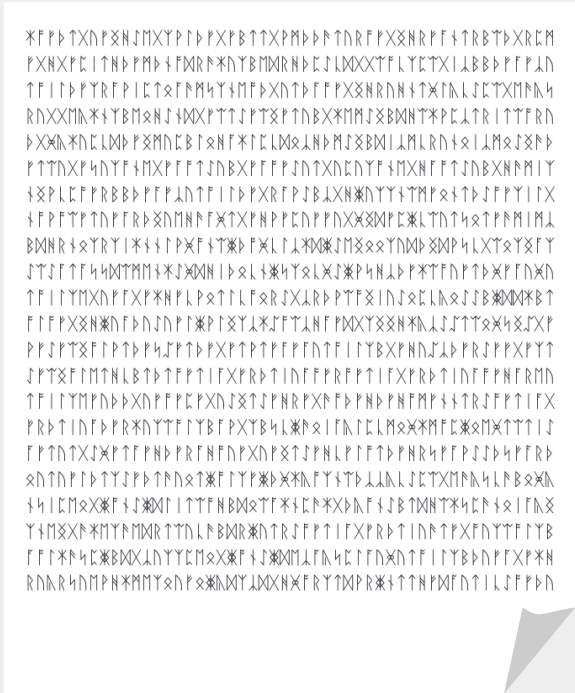
TLS/HTTPS

TLS+DNS

(ESNI/ECH, DoT/DoH)

DNS + TLS:

1. Выпуск сертификата – для доменного имени;
   Certificate issuance – domain name in Subject;
2. Проверка права управления – через DNS:
   Ownership validation – through DNS
   2.1. большинство способов проверки – полагаются на DNS;
   most validation methods are based on DNS;
3. Безопасность DNS
   DNS security

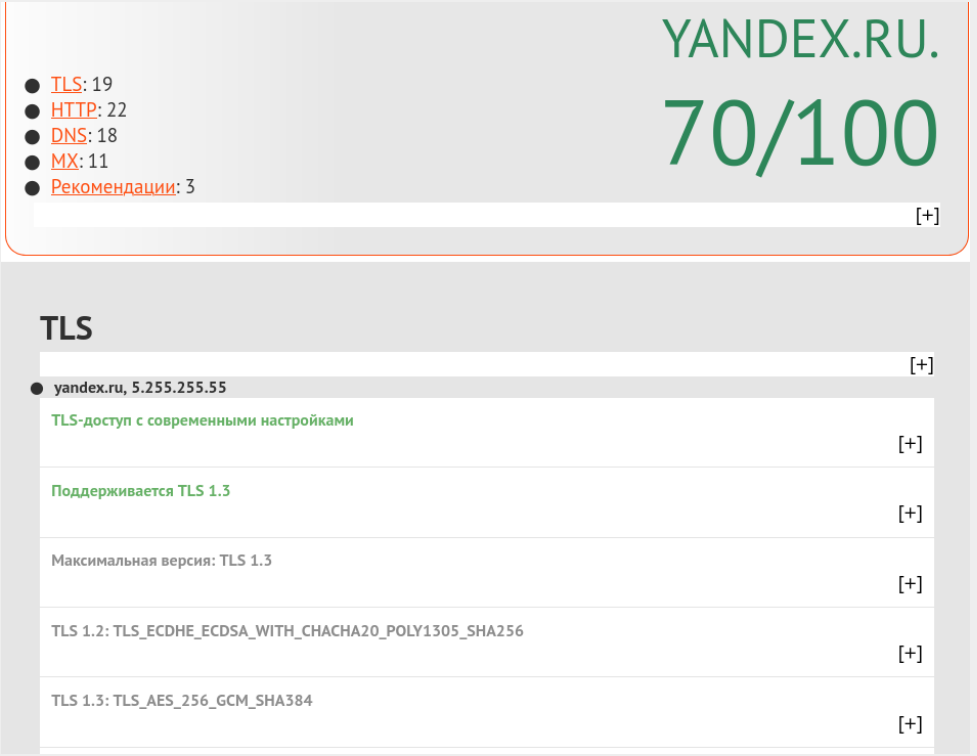


ТЦИ

Modern web *is* HTTPS (TLS)

TLS: email, DNS, etc.

ESNI/ECH, DoT/DoH



https://audit.statdom.ru/?p=yandex.ru.

ТЦИ

Статистика
Stats

Узлы, адресуемые доменами второго уровня (.RU)
Nodes in second-level names (.RU)

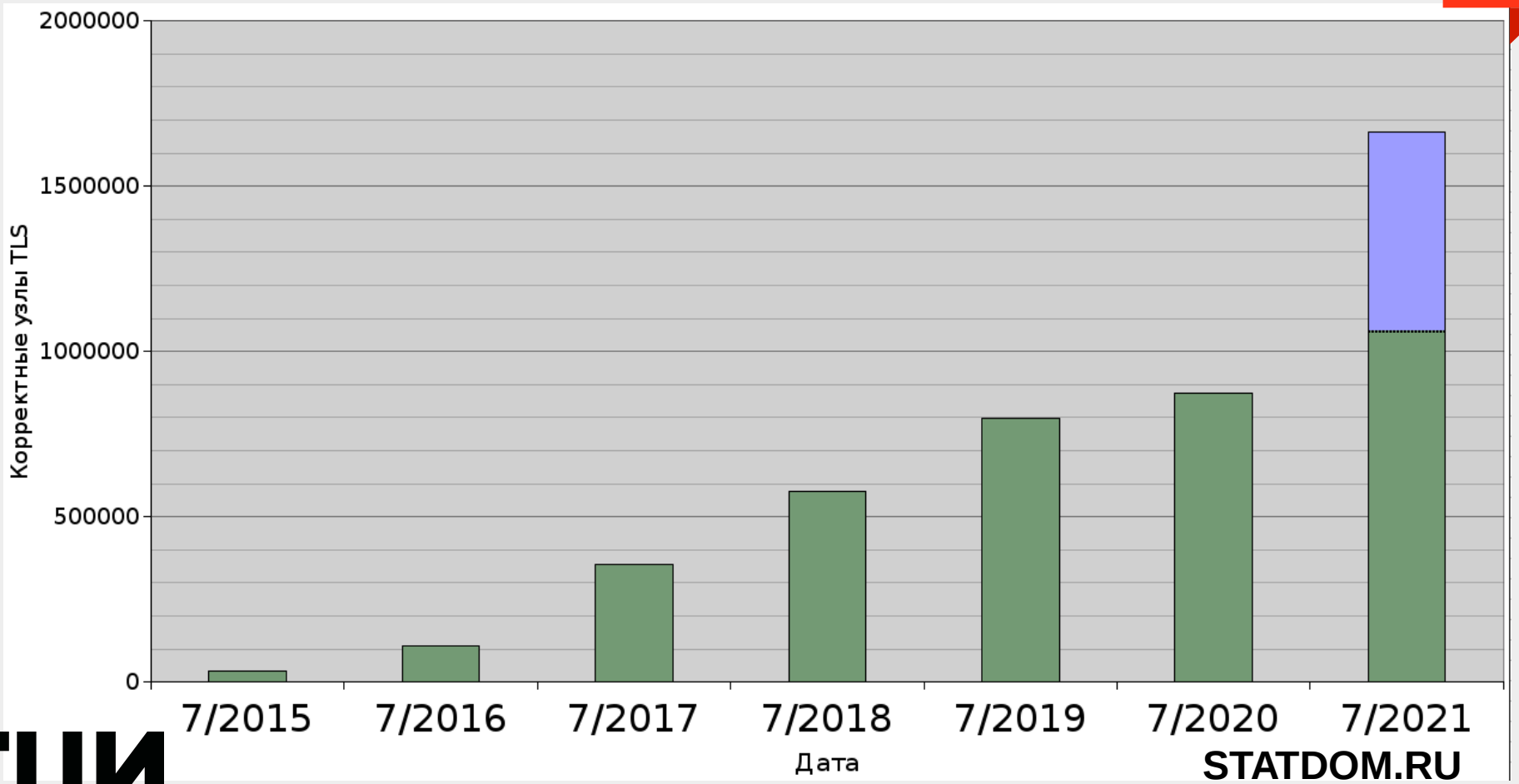
TLS-сессия на 443/tcp
TLS session on 443/tcp

TLS-сертификаты с сервера
TLS certificates from server

STATDOM.RU

ТЦИ

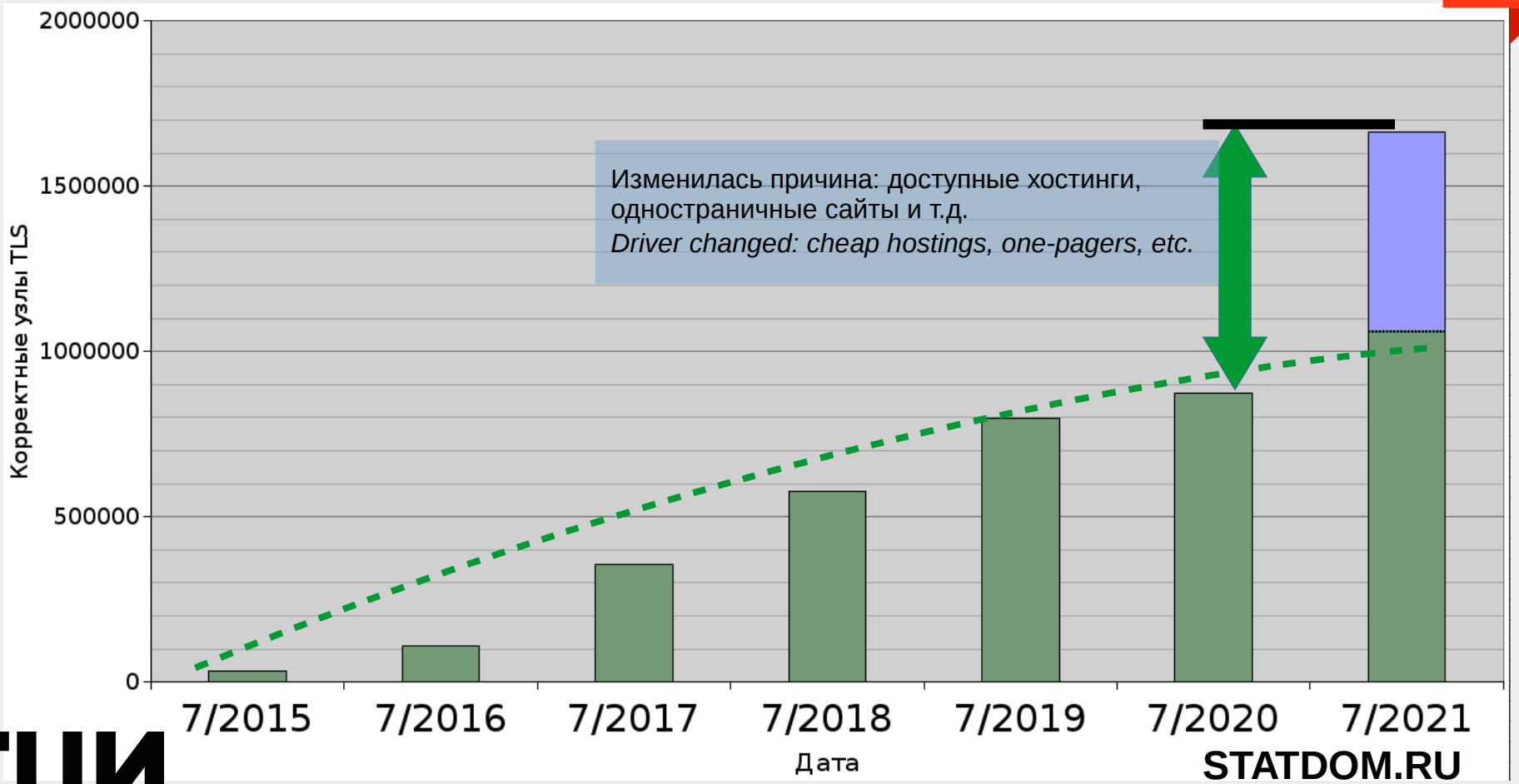
Рост
Growth



ТЦИ

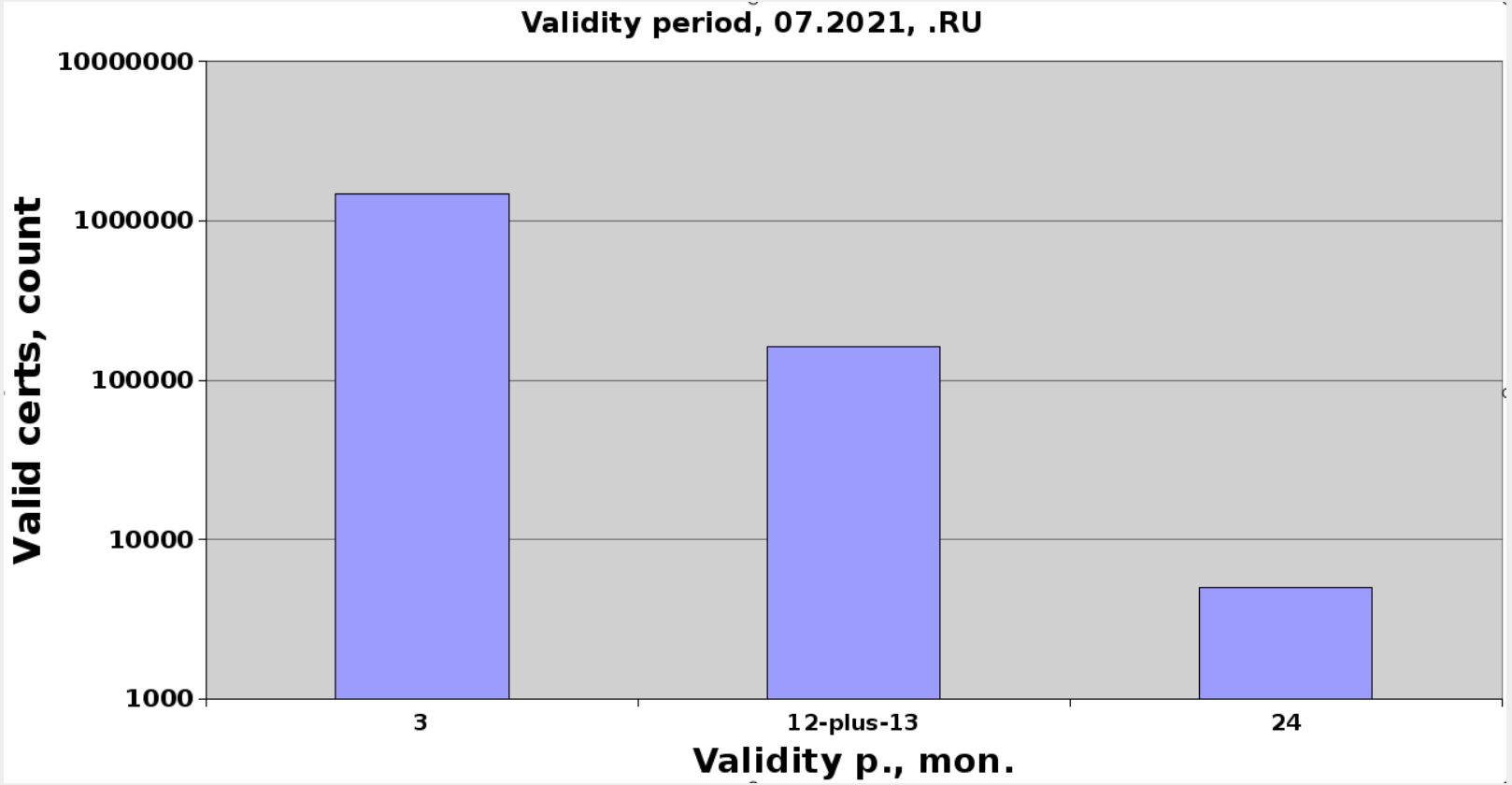
Рост
Growth

Изменение методики
Method change



ТЦИ

Короткий срок
Short term



ТЦИ

STATDOM.RU

TLS-узлы, веб
TLS nodes, web
*(07/**2021**, .RU)*

~1.7 × 10⁶

УЦ CA	
Let's Encrypt:	**~ 1.4 × 10⁶** (~85%)
Sectigo (Comodo)	~65000
GlobalSign	~45000
cPanel, Inc.	~34000

07/2021, STATDOM.RU

ТЦИ

ESNI/ECH (TLS), RU

Для сокрытия метаинформации (SNI);
To hide metainformation (SNI);

07.2021
.RU
ESNI (TXT record)

290569 зон/zones

ESNI – (экспериментальная) поддержка Firefox скоро завершится
soon will be retired from Firefox (experimental)

DNS-over-TLS, DNS-over-HTTPS

Google, Cloudflare – хорошо известные провайдеры в Рунете
well known providers in Runet

Поддержка на стороне сервера встречается редко
Implementations seldom seen server-side

Есть в браузерах
Browsers support it

Противодействие активным атакам и прослушиванию
Active attacks and monitoring mitigation

ТЦИ

Диспозиция
Disposition

ГОСТ-криптография:

открытая, есть открытые реализации (OpenSSL);
сейчас встречается на “специальных” сайтах;
может использоваться на всех сайтах, но мешают трудности с браузерами (пример: “Яндекс.Браузер” с CSP).

GOST crypto:

free, open source implementations exist (OpenSSL)
nowadays common on “special” websites;
could be implemented on all websites, if not “inhibited” by browser-related obstacles (e.g. Yandex.Browser with CSP).

Диспозиция
Disposition

Сертификаты с коротким сроком действия (3 мес.)
Short-term certificates (3 m.)

Let’s Encrypt

Преобладает единственный УЦ
Single CA predominates

RSA, not ECDSA

DoT and DoH – massively popularized

07/2021, STATDOM.RU

ТЦИ

ТЦИ

Открытый сервис аудита безопасности и корректности настроек интернет-узлов (Beta.6.8)

Сервис позволяет проверить технические параметры интернет-узла, адресуемого заданным именем хоста. Проверяются параметры DNS, TLS, HTTP(HTTPS), MX (электронная почта). Для начала проверки введите имя узла в формате name.tld (например, tcinet.ru).

facebook.com

ТЦИ

СПАСИБО ЗА ВНИМАНИЕ!

Александр **Венедюхин**
https://tcinet.ru/