TLS - средство защиты данных в интернете

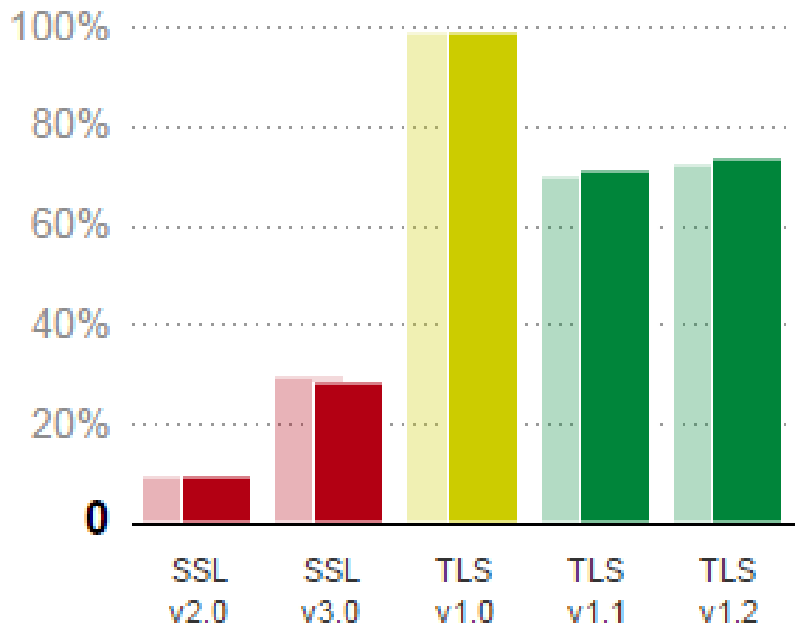
Dmitry Belyavskiy, TCI

Cybersecurity Форум
9 февраля 2016 г.
Москва

Technical Centre of Internet

TLS: история

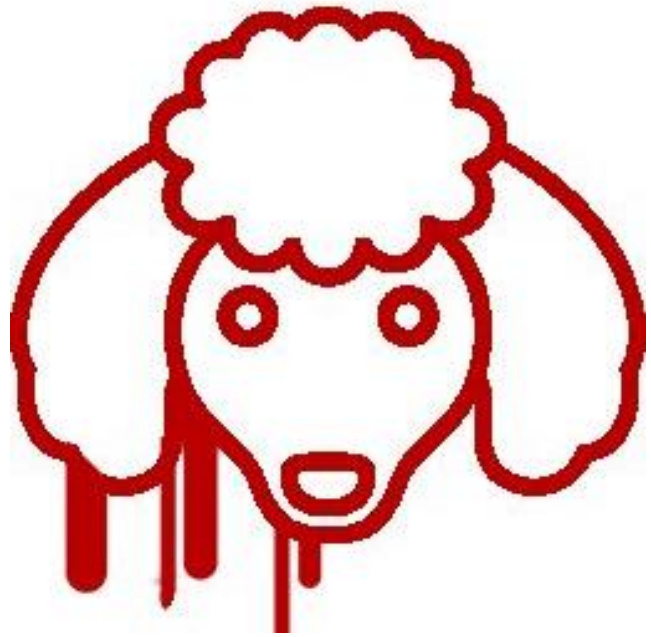
- SSLv2 устарел (RFC 6176)
- SSLv3 устарел (RFC 7568)
- TLS 1.0 – RFC 2246 (1999)
- TLS 1.1 – RFC 4346 (2006)
- TLS 1.2 – RFC 5246 (2008)



Источник: https://www.trustworthyinternet.org/ssl-pulse/

Уязвимости 2014-2016

- Heartbleed
- POODLE
- FREAK
- LogJam
- SLOTH



Продолжение следует…

Старые алгоритмы

- SHA1 устаревает
  - Freestart collision
- RC4 уже устарел

1024-bit RSA недостаточно!

Новые решения

- Эллиптические кривые
- Кривые Эдвардса
- Perfect Forward Secrecy
- ChaCha20
- Poly1305
- Certificate transparency

Зашифруемся!

- **Растёт доля шифрованного трафика.**
  - ***По данным MSK-IX – примерно треть*.**
- **Новые протоколы подразумевают защиту трафика**
- **Хостеры включают TLS по умолчанию**
  - ***Universal SSL***
- **DNS – последний нешифрованный протокол**
  - ***RFC 7626***

TldStat

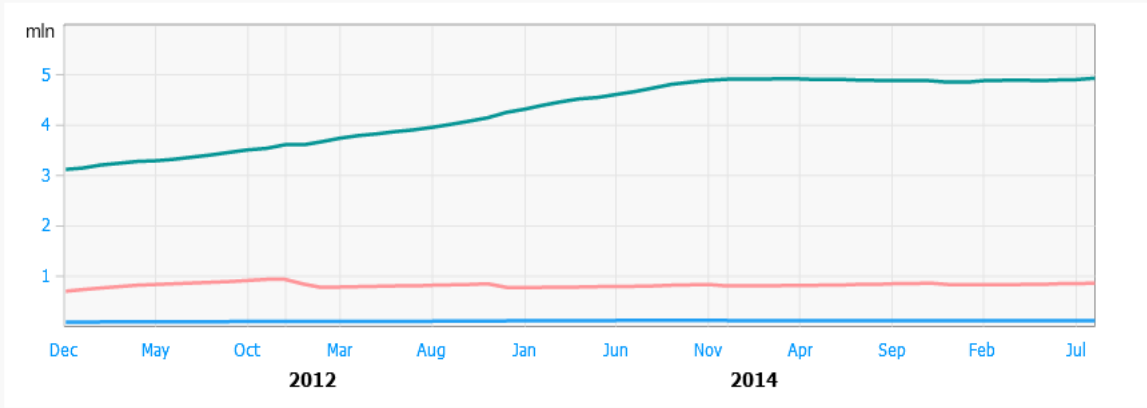
02 September 2015 (yesterday)

.RU
4 930 412 ▼ - 0,05 %
New domains in the current month: **12 070**

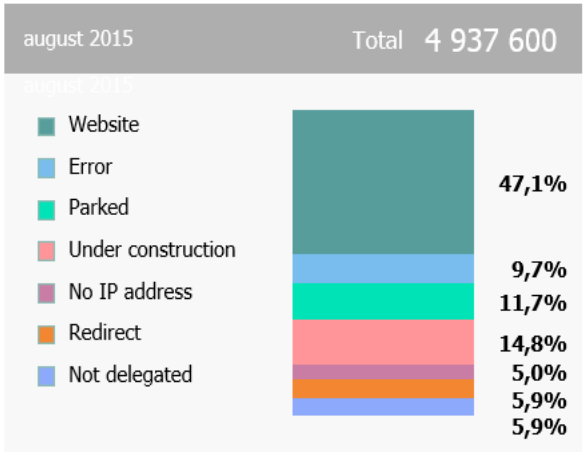
.РФ
863 492 ▲ + 0,06 %
New domains in the current month: **1 549**

.SU
118 316 ● 0 %
New domains in the current month: **177**

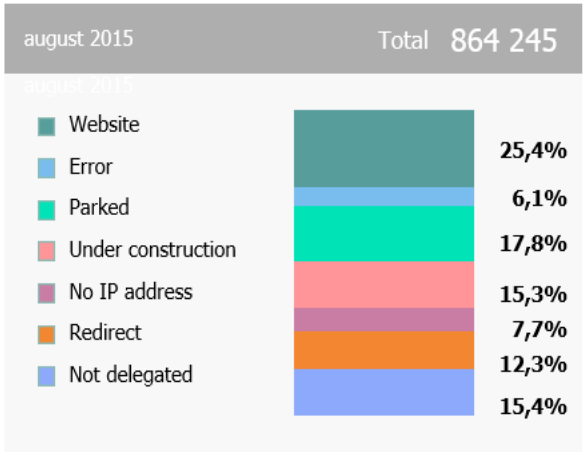
.RU/.РФ growth



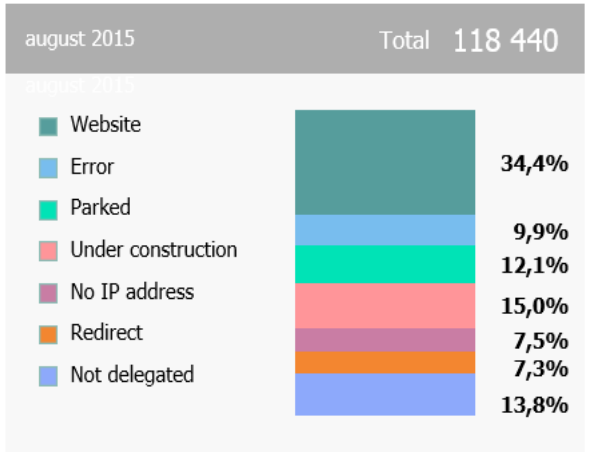
.RU domain names usage



.РФ domain names usage



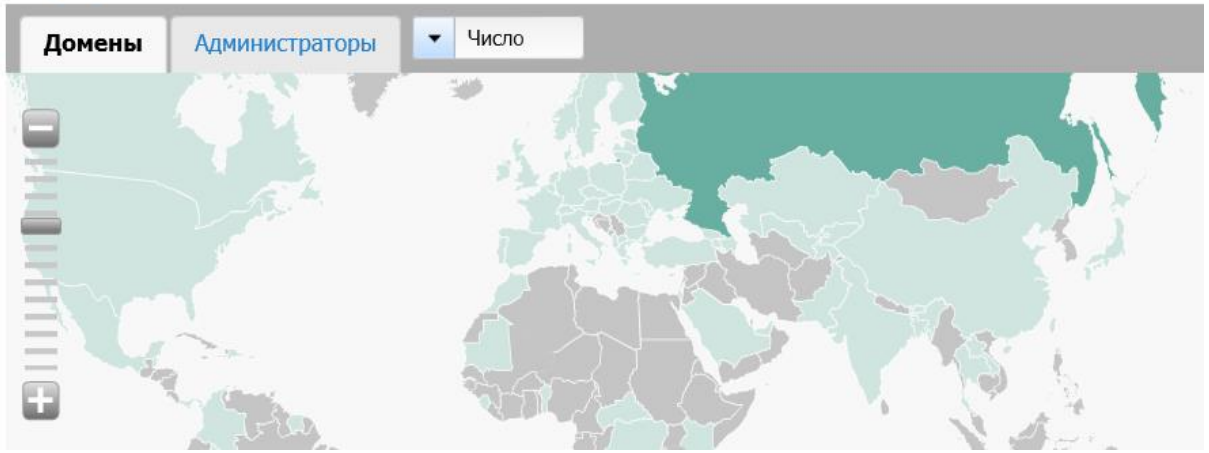
.SU domain names usage

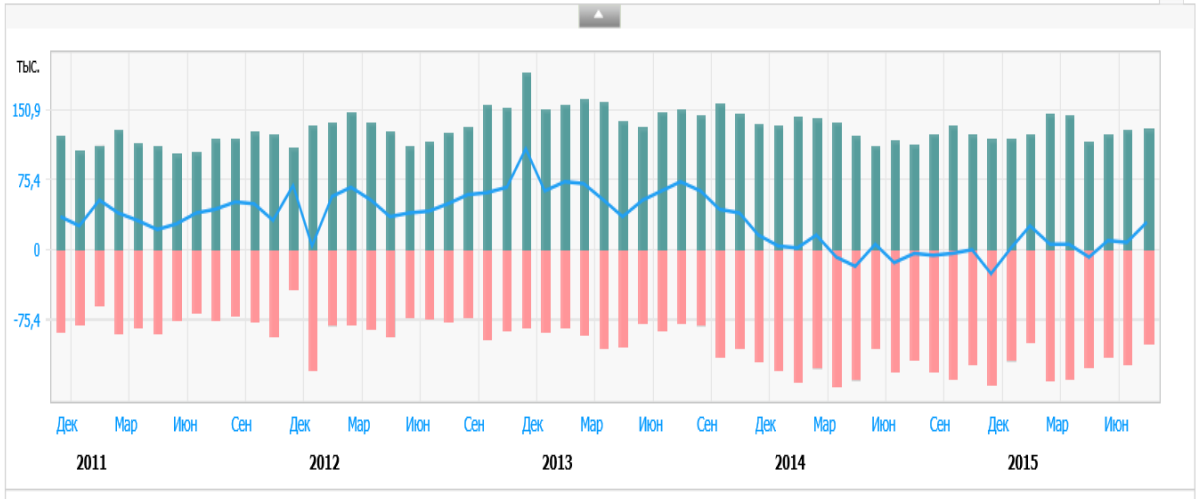


Source: http://statdom.ru/

TldStat

География





Source: http://statdom.ru/

За 01 сентября 2015 (вчера)

.RU
4 933 073 - 0,09 %
Новых с начала месяца: **5 458**

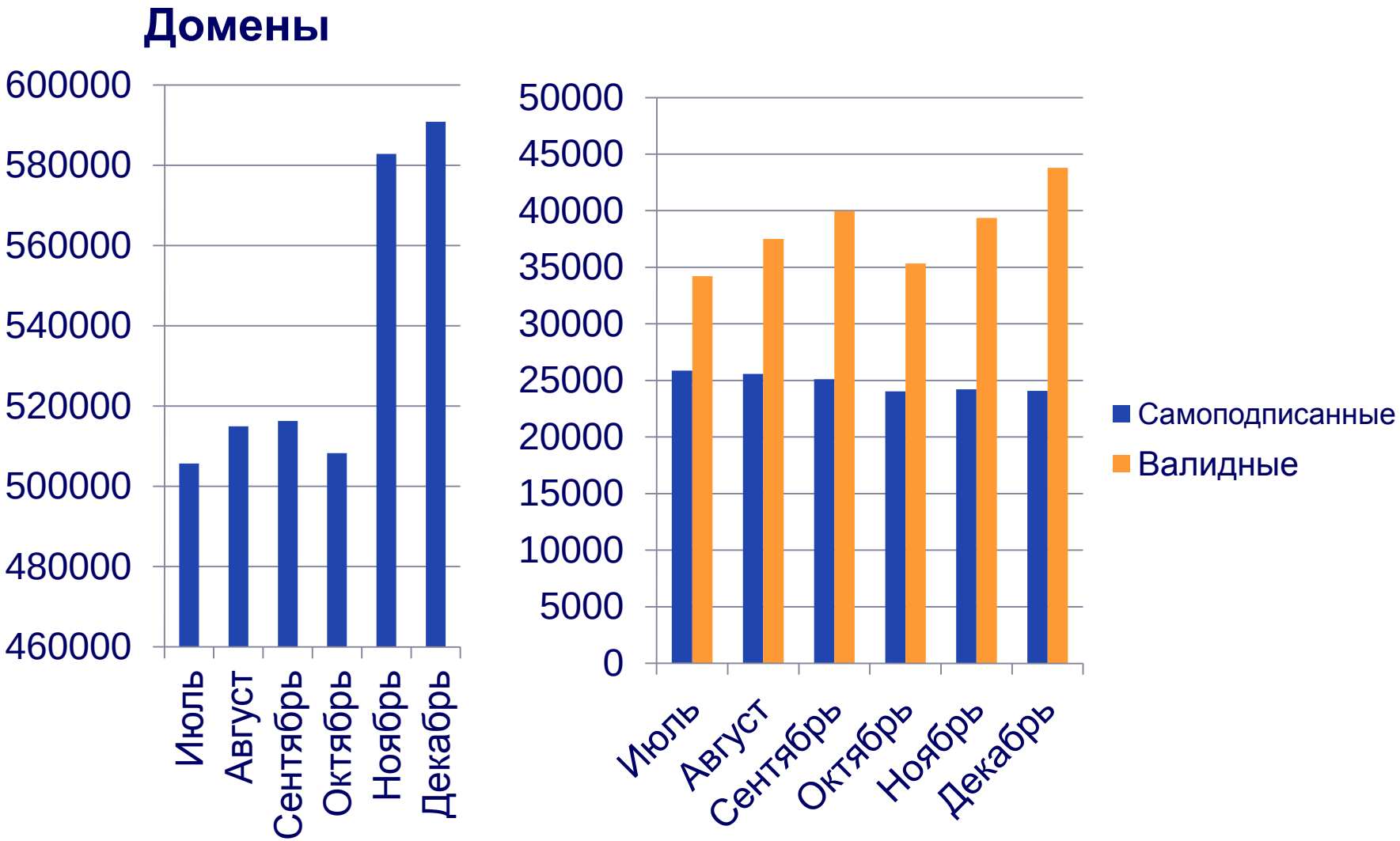
.РФ
862 997 - 0,14 %
Новых с начала месяца: **798**

.SU
118 311 - 0,11 %
Новых с начала месяца: **110**

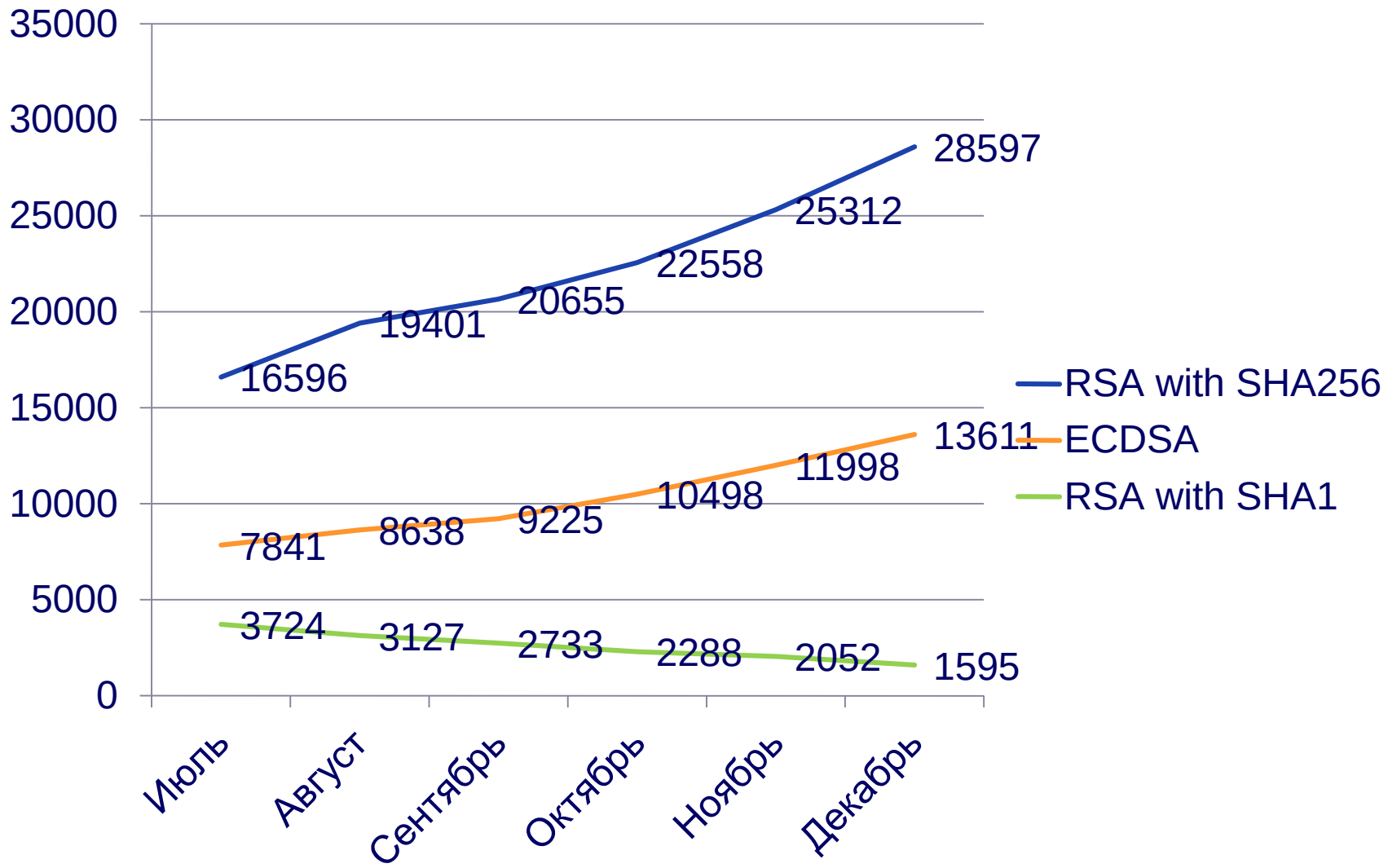
Использование доменов .RU

Требующие про	Продлённые, число	Продлённые, доля
353 294	**244 597**	**69,23 %**
113 118	49 552	43,81 %
55 215	37 221	67,41 %
40 611	31 694	78,04 %
32 937	26 529	80,54 %
28 876	24 799	85,88 %

.RU – общая статистика



.RU - алгоритмы



Интересные факты

- Все EC сертификаты - от Cloudflare
- ~50% сертификатов бесплатны
- ~450 EV сертификатов
- >90% RSA сертификатов 2048+bits
- <10 RSA сертификатов 1024 bits

Промежуточные выводы

- **Российская практика соответствует рекомендациям**
- **Можно обсчитывать больше**
  - **MX, ciphersuites,…**
- **Можем обследовать зону на предмет угроз**

Что думают пользователи

- **TLS – это про шифрование**
  - Нет. Аутентификация сторон важнее.
- **Зелёный замочек вас спасёт**
  - Нет. Домены с похожими названиями+бесплатный сертификат = фишинг

Чего надо бояться

- **MITM-атаки**
  - Национального уровня (.KZ)
  - Уровня провайдера
  - Уровня отдельного хакера
- **Параноидальные браузеры**
  - SHA-1
- **Мобильные приложения**
  - Ошибки проверки сертификатов
- **Странные наборы корневых УЦ**

Вопросы?

Email:

beldmit@tcinet.ru