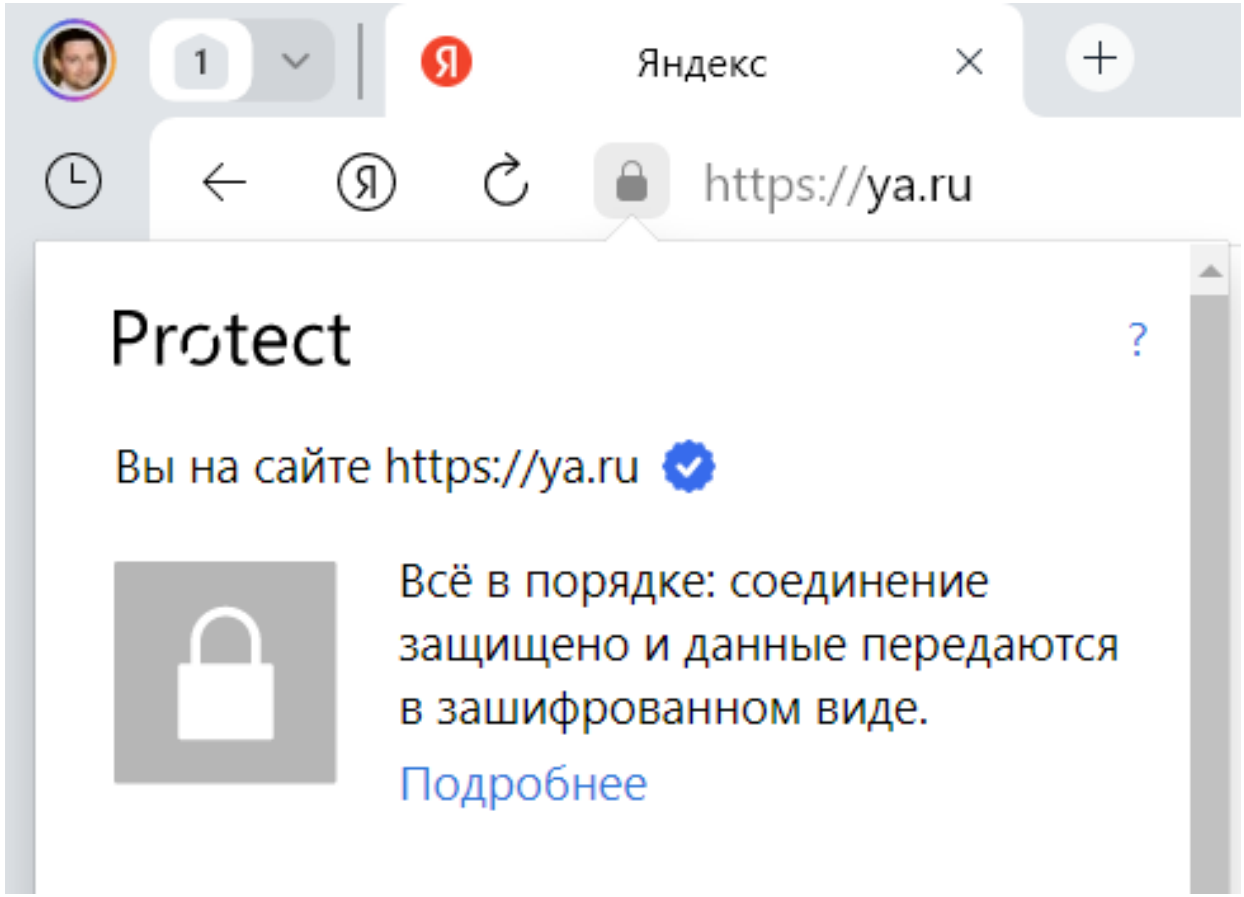
«Соединение защищено». Достижения и задачи в области защищенного доступа к веб-сайтам в России

Смышляев Станислав Витальевич, д.ф.-м.н.
заместитель генерального директора КриптоПро

КРИПТОПРО

Защищенные соединения в Интернете: TLS



NETSCAPE

SSL 2.0 (1995) → SSL 3.0 (1996)

IETF

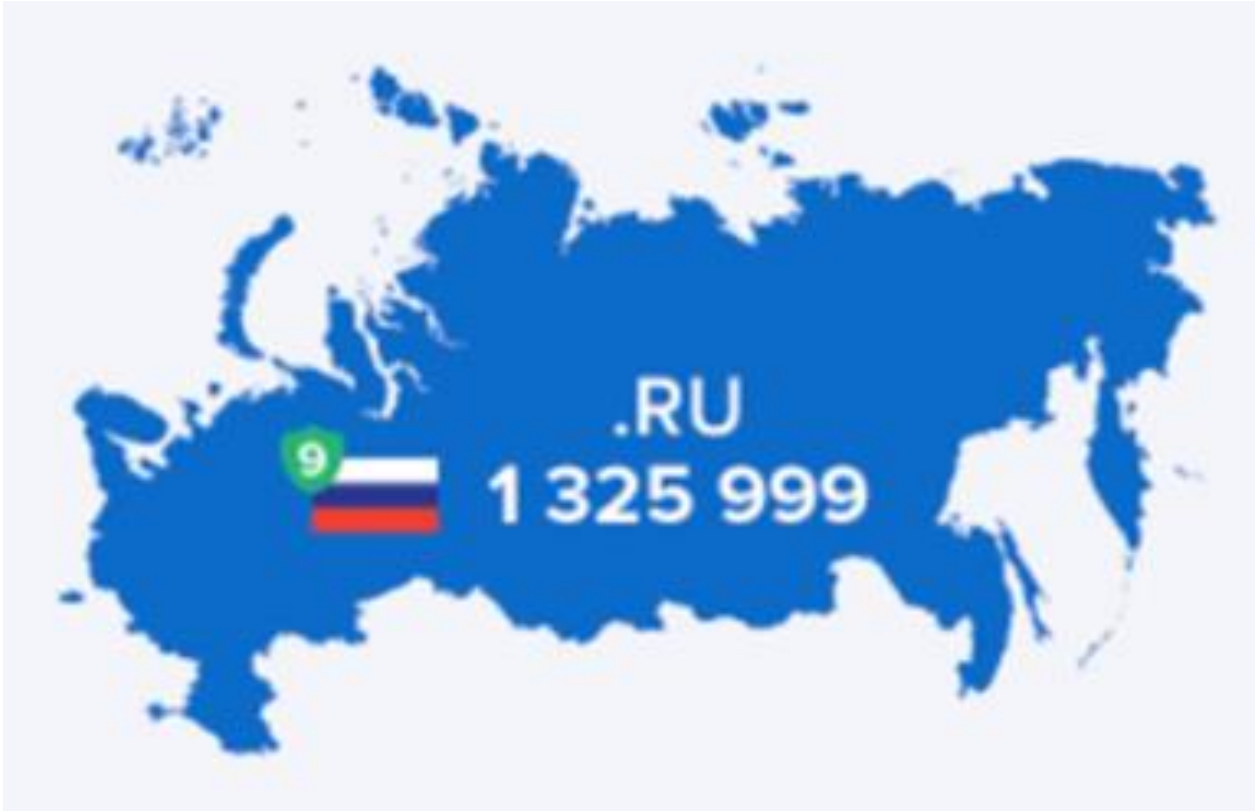
TLS 1.0 (1999) → TLS 1.1 (2006) → TLS 1.2 (2008)

TLS 1.3 (2018)

TLS 1.3

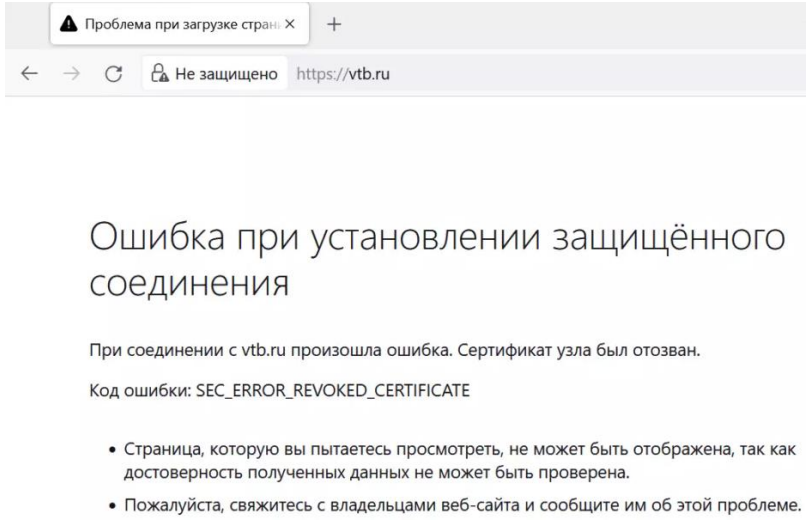
Топ-5 УЦ по количеству выпущенных сертификатов в зоне .RU

- Let's Encrypt (960 000)
- CloudFlare (110 000)
- DigiCert (85 000)
- GlobalSign (75 000)
- Sectigo (55 000)



Отзыв и прекращение выдачи TLS-сертификатов

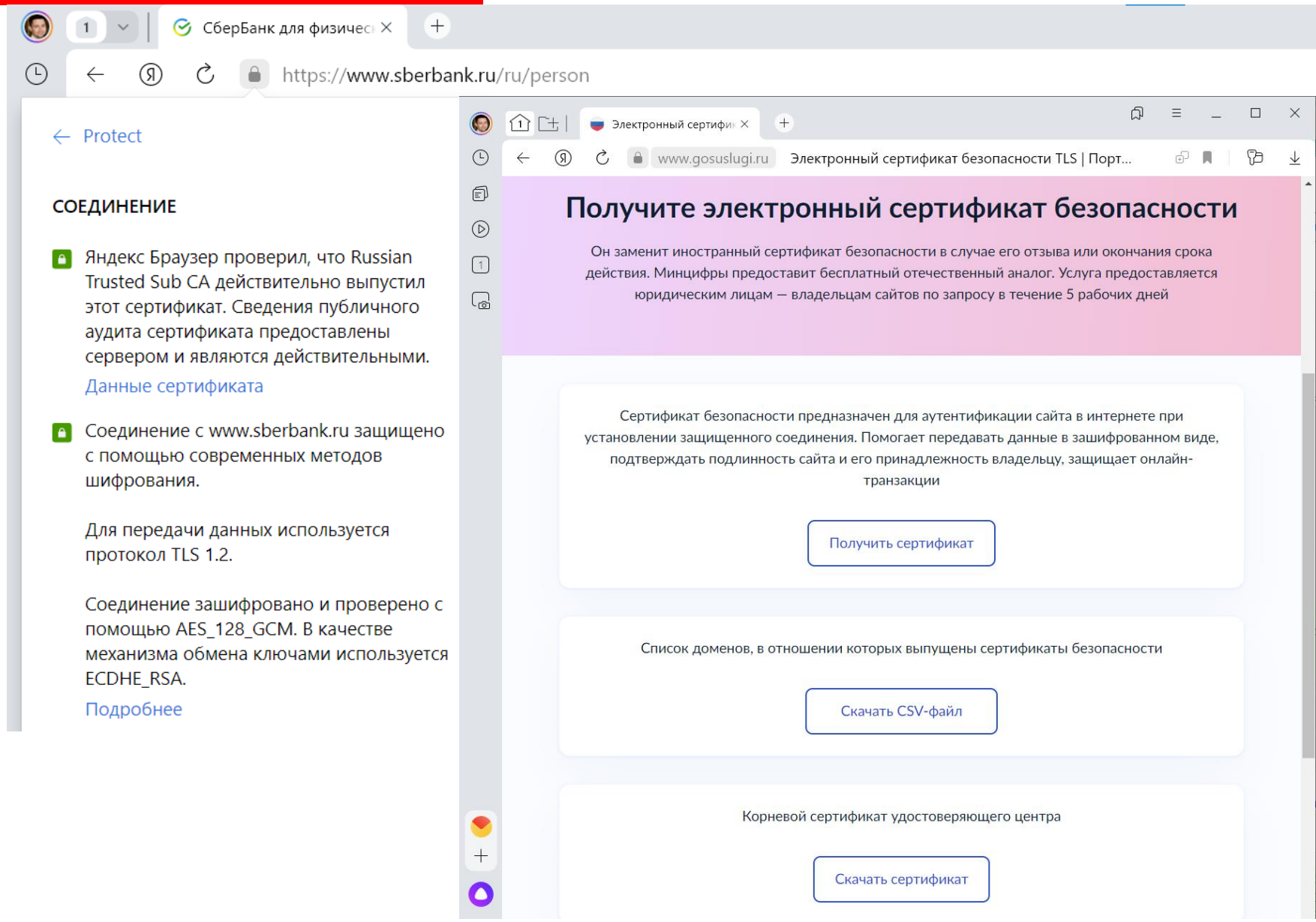
- 2017 – Утрата доверия Google к сертификатам от Symantec
- 2018 – Отозван сертификат Общественной палаты РФ
- 2022 – Отозваны сертификаты у ВТБ, ЦБ, ПСБ, Сбербанка, Минобороны
- 2022 – Прекращена выдача сертификатов для Рунета со стороны УЦ Sectigo (бывш. Comodo), DigiCert, Thawte, Rapid, GeoTrust



- 2022 – введен в действие НУЦ для выдачи RSA-сертификатов

НУЦ RSA и Certificate Transparency

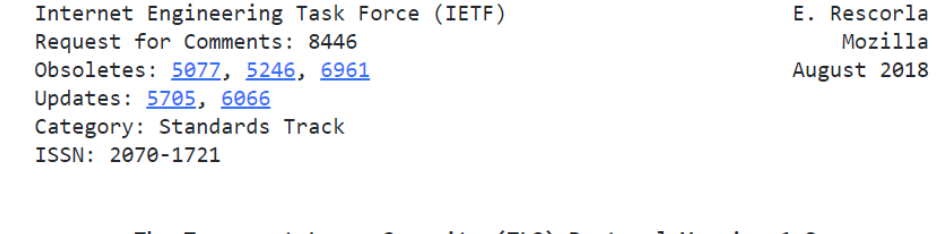
- Certificate Transparency: публичный лог выпущенных сертификатов, защищенный от искажений
- Выпуск и распространение корневого сертификата НУЦ
- Получение сертификатов веб-сайтов через ЕПГУ



Два вектора развития TLS в России

SSL/TLS с RSA

- RFC
- Поддержка со стороны браузеров
- Удостоверяющие центры
- Серверные решения (шлюзы)
- Массовость

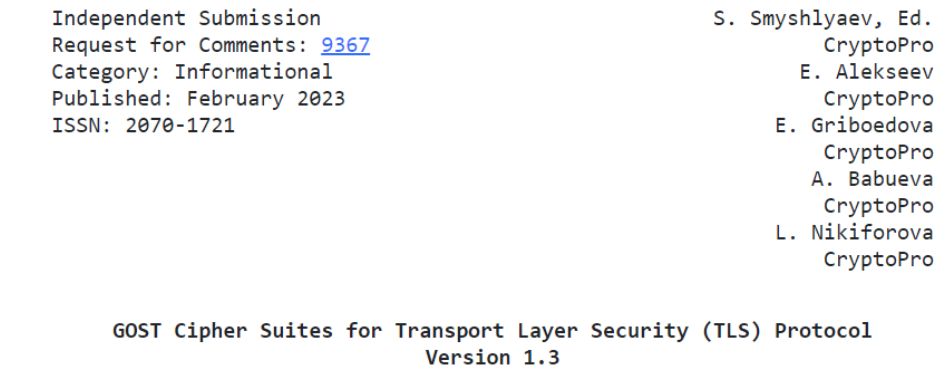


Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

TLS с ГОСТ

- RFC
- Поддержка со стороны браузеров
- Удостоверяющие центры
- Серверные решения (шлюзы)
- Выполнение требований законодательства в части криптографической защиты



Independent Submission — S. Smyshlyaev, Ed. CryptoPro
Request for Comments: 9367 — E. Alekseev CryptoPro
Category: Informational — E. Griboedova CryptoPro
Published: February 2023 — A. Babueva CryptoPro
ISSN: 2070-1721 — L. Nikiforova CryptoPro

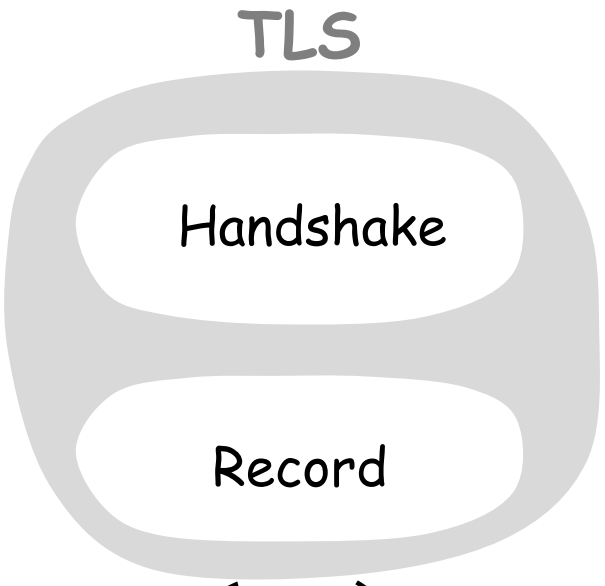
GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.3

КРИПТОПРО

Законодательное обеспечение ГОСТ TLS

- **2016.** Поручение Президента (Пр-1380) про переход ОГВ на российскую криптографию
- **2017.** Программа «Цифровая экономика РФ»
- **2018.** Дорожные карты по переходу на ГОСТ в Рунете
- **2020.** Пилотный проект по использованию российских алгоритмов и шифрсредств в ГИС
- **2023.** Ожидается принятие НПА по Национальному УЦ

Криптонаборы TLS с ГОСТ




```
TLS_GOSTR341112_256_WITH_28147_CNT_IMIT
TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC
TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC
```

```
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S
```

TLS 1.2 с ГОСТ

- ✓ Р 1323565.1.020-2020
- ✓ RFC 9189
- ✓ Идентификаторы в реестре IANA

TLS 1.3 с ГОСТ

- ✓ Р 1323565.1.030-2020
- ✓ RFC 9367
- ✓ Идентификаторы в реестре IANA

КРИПТОПРО

Криптонаборы TLS с ГОСТ

Важно: криптонаборы с ГОСТ для обеих версий стойкие,
нет необходимости переходить именно на 1.3, у обеих версий есть преимущества.

TLS 1.2 с ГОСТ

- Отсутствие известных уязвимостей
- Анализ стойкости в подробных моделях нарушителя
- Механизмы регулярной смены сессионных ключей:
  - Снижение требований к реализации и порядку размещения СКЗИ в условиях необходимости противодействия атакам по побочным каналам
  - Возможность безопасного функционирования в условиях слабодоверенного окружения.
- Обеспечение совместимости с СЗИ, осуществляющими расшифрование трафика с целью обнаружения атак

TLS 1.3 с ГОСТ

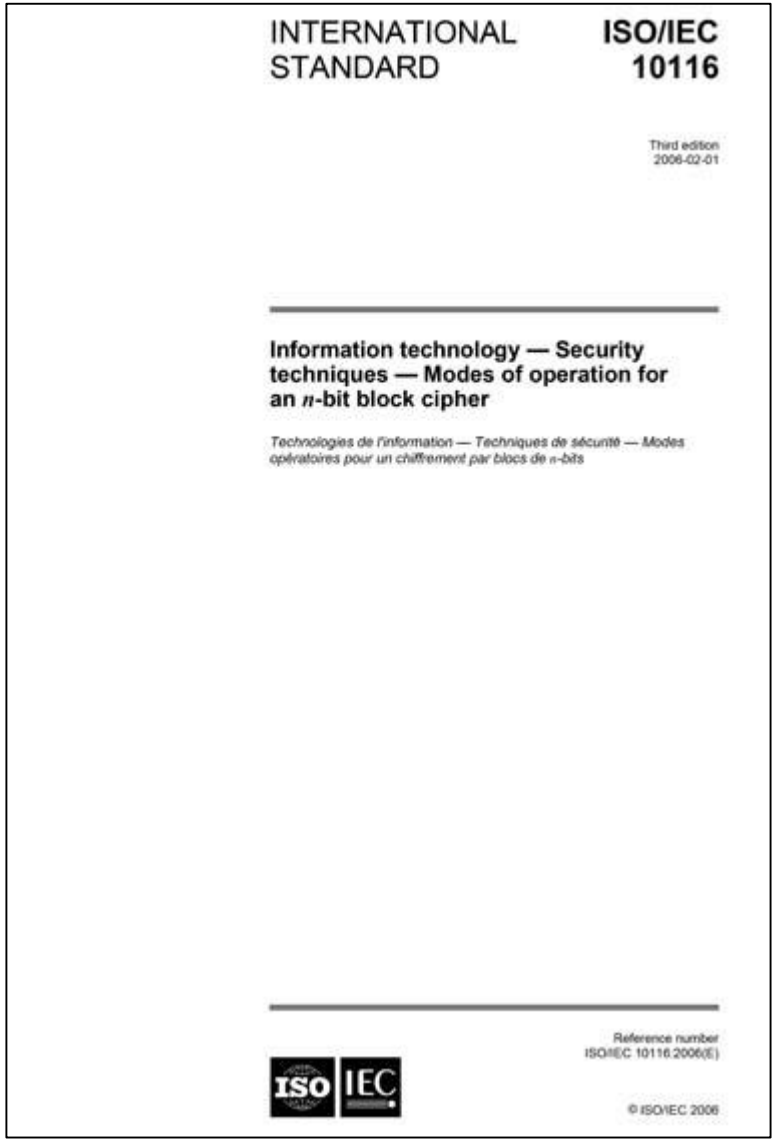
- Отсутствие известных уязвимостей
- Анализ стойкости в подробных моделях нарушителя
- Свойство PFS (Perfect Forward Secrecy) на сервере:
  - Отсутствие последствий для конфиденциальности ранее переданных данных в случае компрометации сервера
  - В ряде случаев – снижение требований к защите долговременных ключей от явной компрометации
- Улучшение производительности в случае высоконагруженных серверов

Стандартизация: IETF и ISO

- **RFC 9189**, «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2», **March 2022**.
  Stanislav Smyshlyaev, Dmitry Belyavskiy, Evgeny Alekseev.
- **RFC 9367**, «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.3», **February 2023**. Stanislav Smyshlyaev, Evgeny Alekseev, Ekaterina Griboedova, Alexandra Babueva, Lidiia Nikiforova.

- **RFC 8645**, «Re-keying Mechanisms for Symmetric Keys», August 2019; CFRG. Stanislav Smyshlyaev, Ed.
- **RFC 9058**, «Multilinear Galois Mode (MGM)», June 2021.
  Stanislav Smyshlyaev, Vladislav Nozdrunov, Vasily Shishkin, Ekaterina Griboedova.

- **ISO/IEC 10116:2017/AMD 1:2021 «Information technology — Security techniques — Modes of operation for an n-bit block cipher»**
  - Дополнение к международному стандарту ISO/IEC 10116:2017, содержащее описание режима шифрования CTR-ACPKM.


INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits

Reference number
ISO/IEC 10116:2006(E)

© ISO/IEC 2006

FSE 2023: CTR-ACPKM, криптоанализ

Attacking the IETF/ISO Standard for Internal Re-keying CTR-ACPKM

Orr Dunkelman, Shibam Ghosh, Eran Lambooij

University Of Haifa

- FSE 2023 (23 марта): Орр Дункельман и др., анализ CTR-ACPKM (применяется в TLS 1.2 с ГОСТ).
- Аннотация:
  - We show that the internal re-keying suffers from an entropy loss in successive repetitions of the re- keying mechanism. We show some attacks based on this issue. The most prominent one has time and data complexities of O(2k/2) and success rate of O(2−κ/4) for a k-bit key – 2^{64} смен ключа для ключа 256 бит.
  - We show that a malicious block cipher designer or a faulty implementation can exploit the ACPKM (or the original CPKM) mechanism to significantly hinder the security of a protocol employing ACPKM (or CPKM). Namely, we show that in such cases, the entropy of the re-keyed key can be greatly reduced.

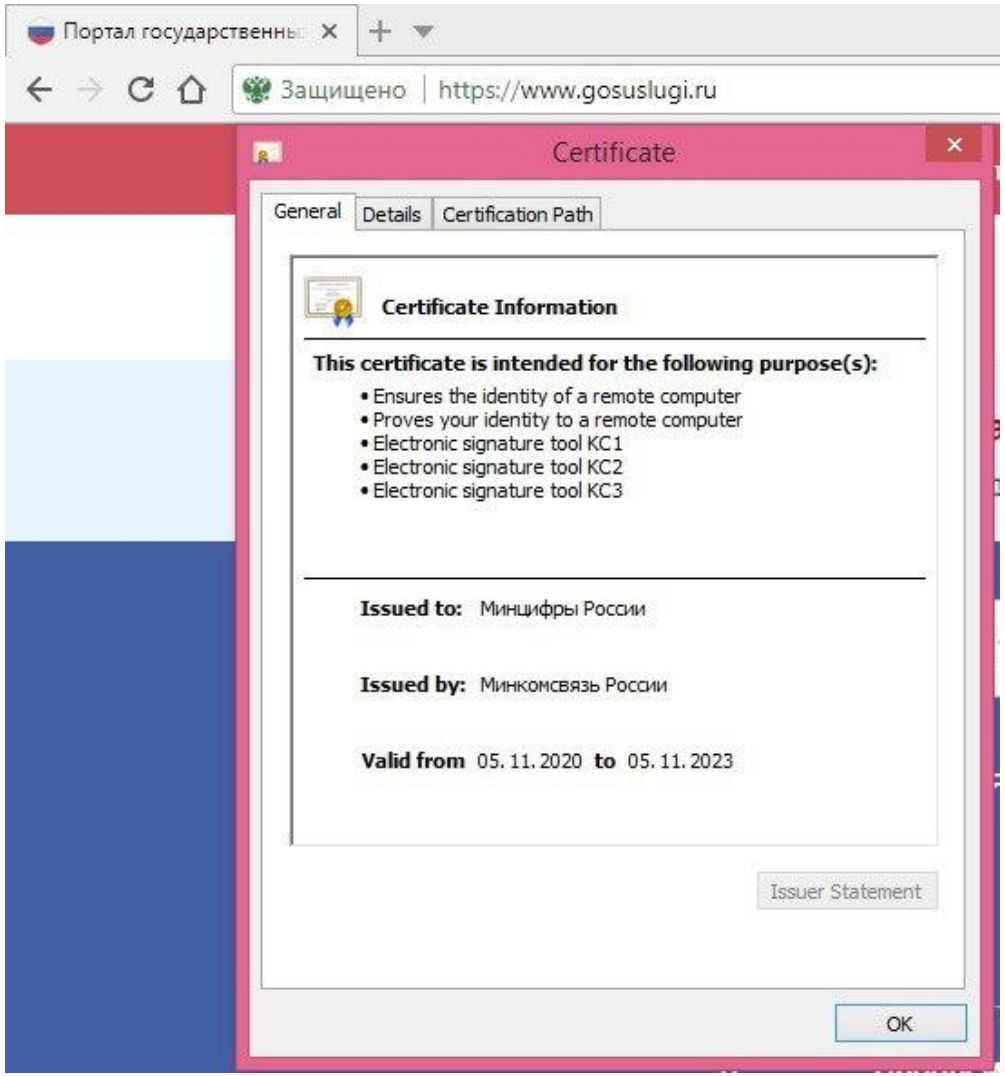
Замечание 1.4. Для итерационных алгоритмов выработки производных ключей типа «CryptoPro Key Meshing», выходами которых являются результаты отдельных тактов, взятых с произвольным фиксированным периодом $k \in \mathbb{N}$, распределение (1.9) случайной величины $\tau_{f^k}(x)$ задает распределение периода бесповторного использования производных ключей, сформированных на основе некоторого долговременного ключа, соответствующего $x \in S$.

- В.О. Миронкин, 2015, цикл работ («О некоторых вероятностных характеристиках алгоритма выработки ключа «CryptoPro Key Meshing» и другие работы, в т.ч. диссертация): с учетом фундаментальных свойств случайных отображений необходимо вводить ограничения на количество преобразований CPKM/ACPKM до полной смены ключа.
  Пример: 4 смены ключа в TLS 1.2 с Кузнечиком, 16 смен ключа в TLS 1.2 с Магмой.
- Неверные утверждения Дункельмана и пр. об отсутствии ограничений на длину блока используемого шифра в стандартах.
- Оценки стойкости для CTR-ACPKM не только не опровергнуты, но, напротив, косвенно подтверждена их точность.

Поддержка ГОСТ TLS на веб-сайтах (примеры)

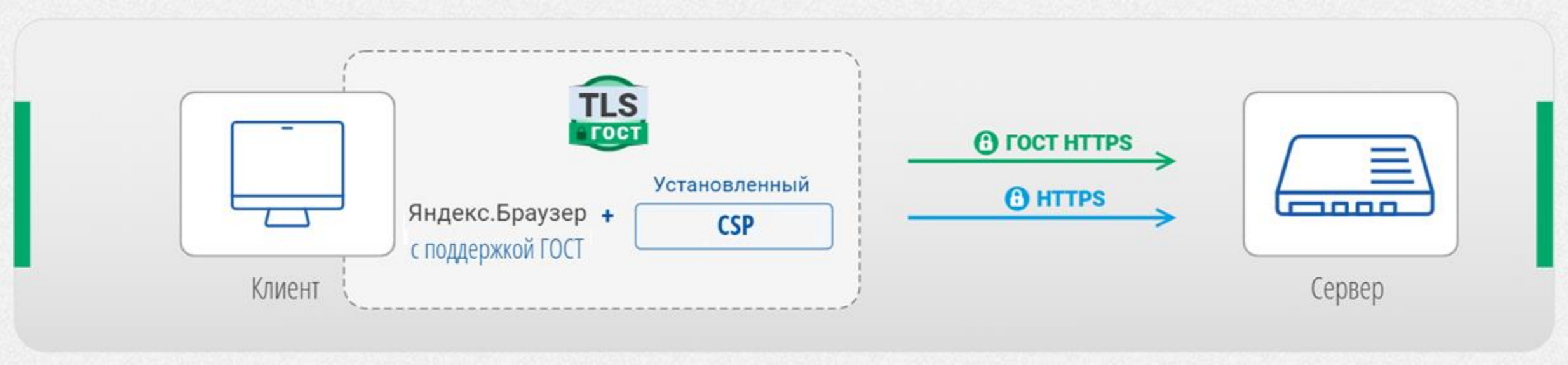
Защищено

- https://gosuslugi.ru – ЕПГУ
- https://www.mos.ru/uslugi/ – госуслуги Москвы
- https://lkul.nalog.ru – личный кабинет налогоплательщика (юрлица)
- https://eruz.zakupki.gov.ru/auth/ – единая ИС в сфере закупок
- https://agregatoreat.ru – единый агрегатор торговли (по 44-ФЗ)
- https://cryptoacademy.gov.ru/ – сайт Академии криптографии РФ
- https://cryptopro.ru – сайт КриптоПро



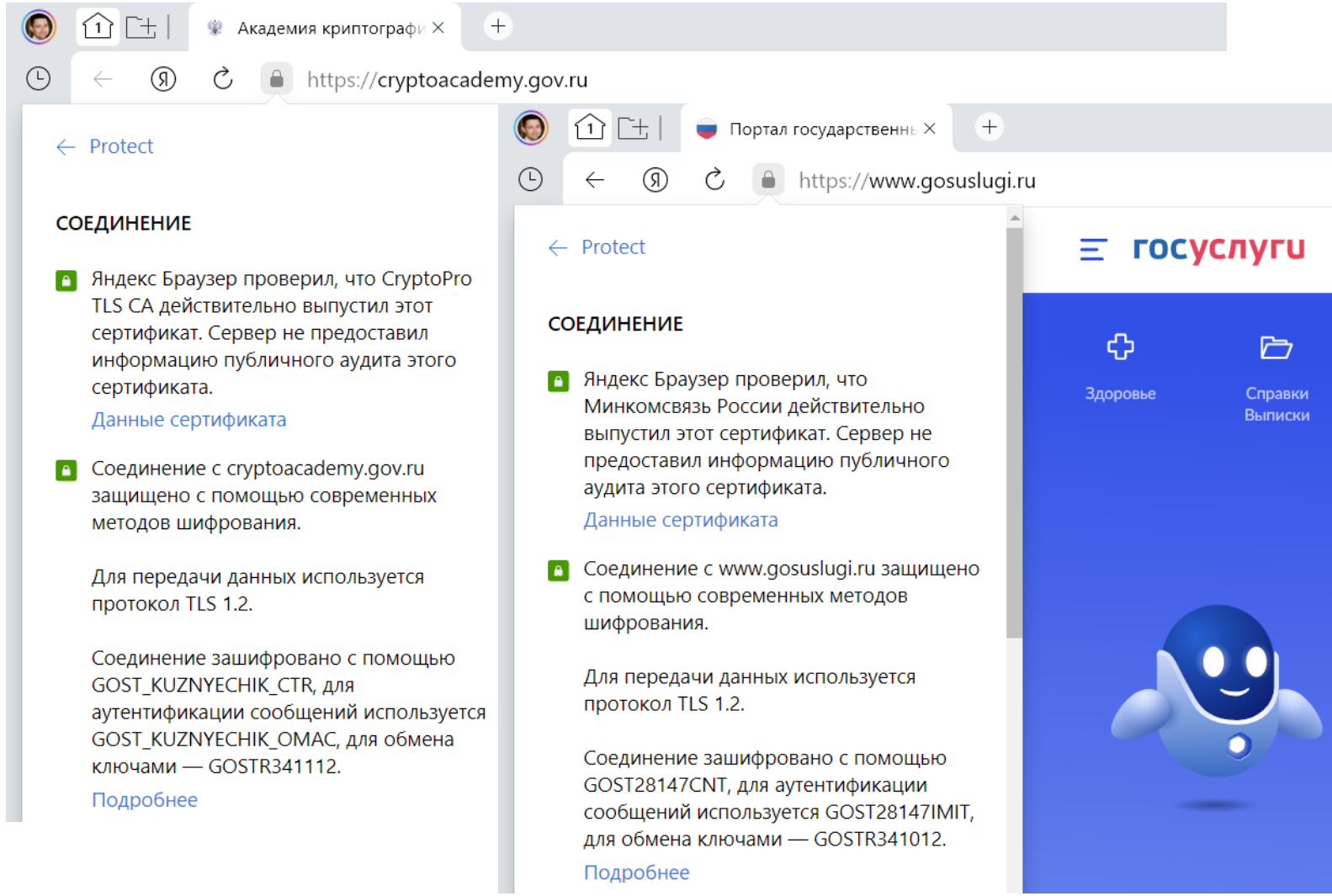
КРИПТОПРО

Клиентские решения для ПК



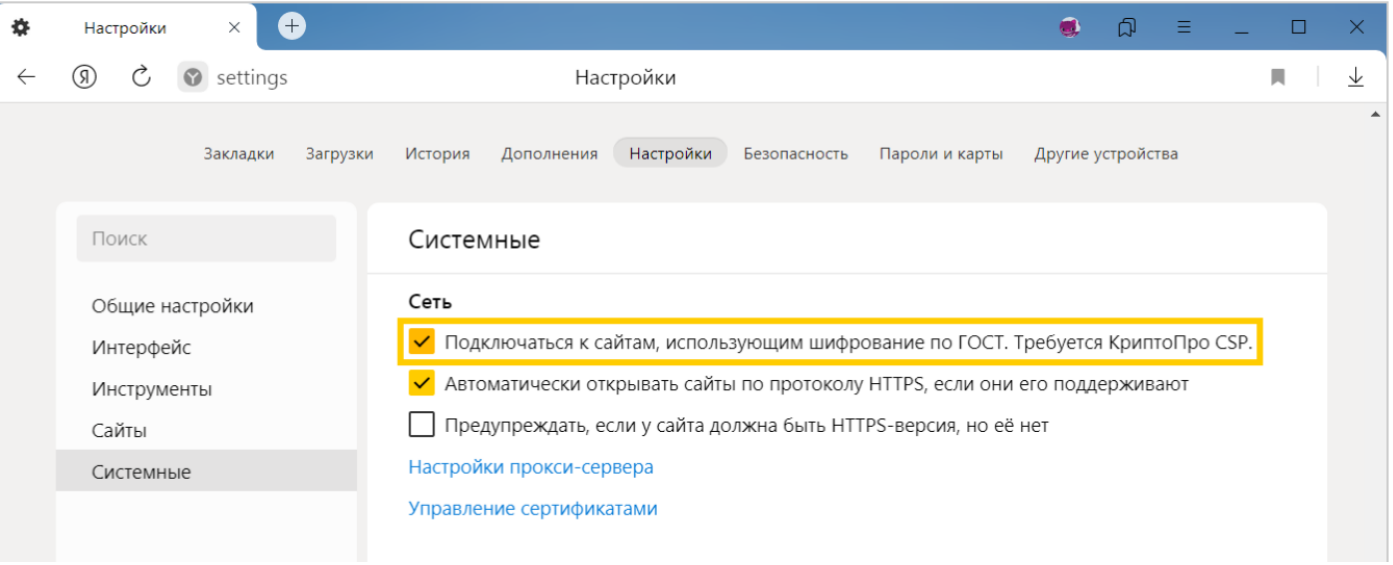
Поддержка ГОСТ в Яндекс Браузере

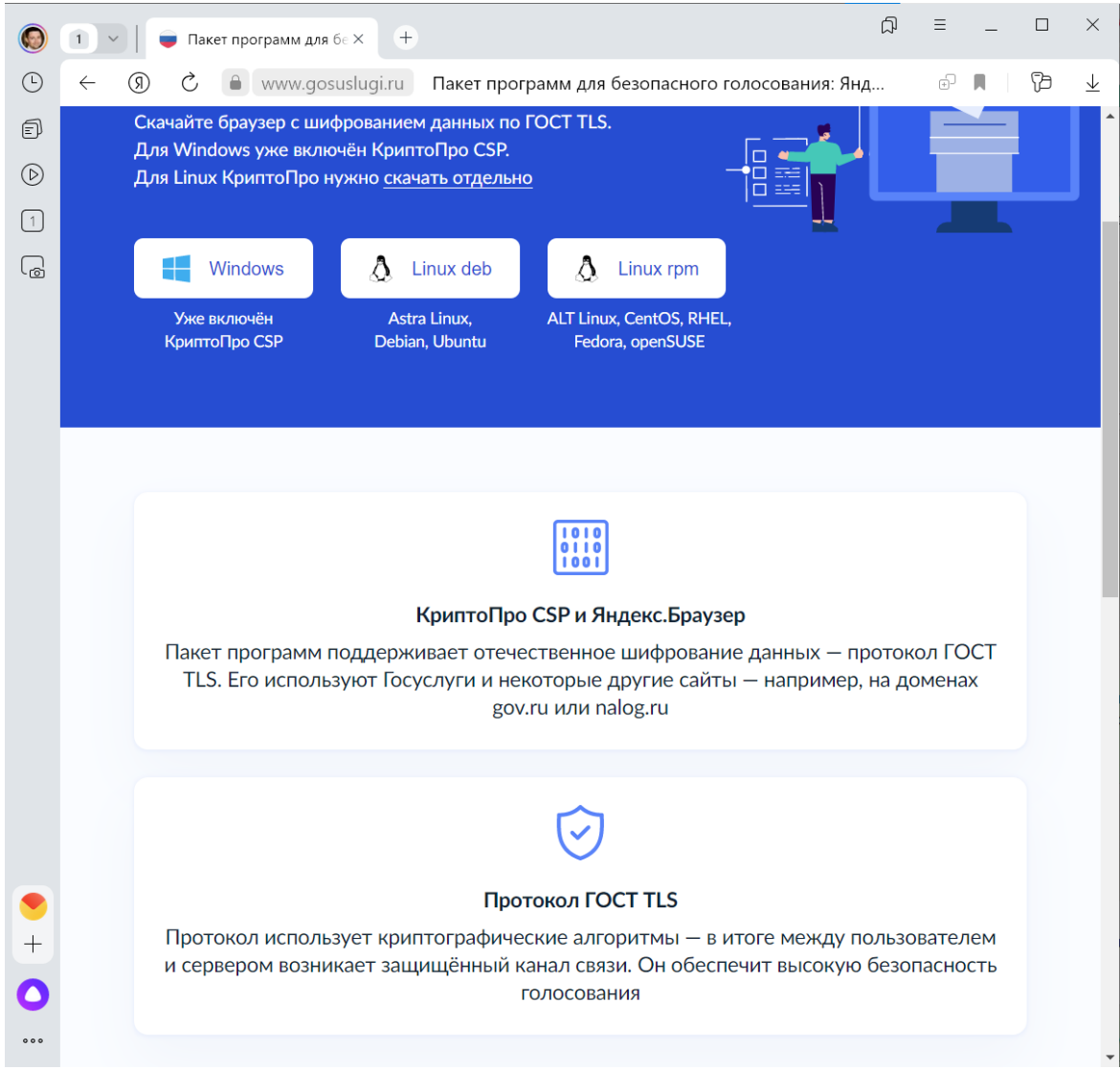
- Интегрирован с криптопровайдером
- Криптонаборы TLS 1.2 с ГОСТ 28147-89 и ГОСТ 34.12-2018
- Доверие к корневым сертификатам ГУЦ, НУЦ и др.



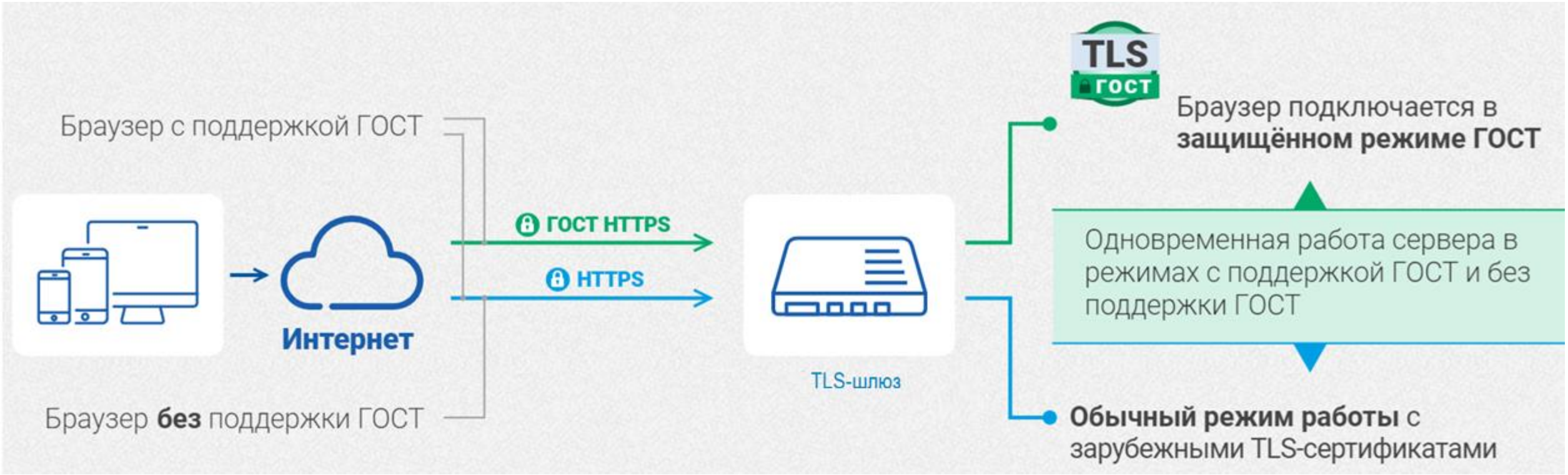
Поддержка ГОСТ в Яндекс Браузере

- Бандл для Windows
- Поддержка Linux (deb/rpm)
- Заключение ФСБ России, КС1, КС2, КС3: №149/3/2/2-2541 от 06.09.2021 г.



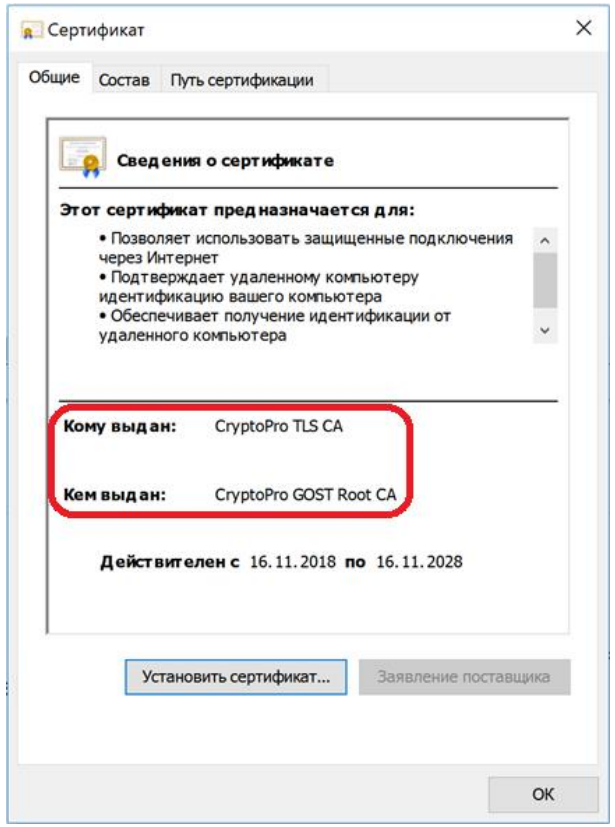


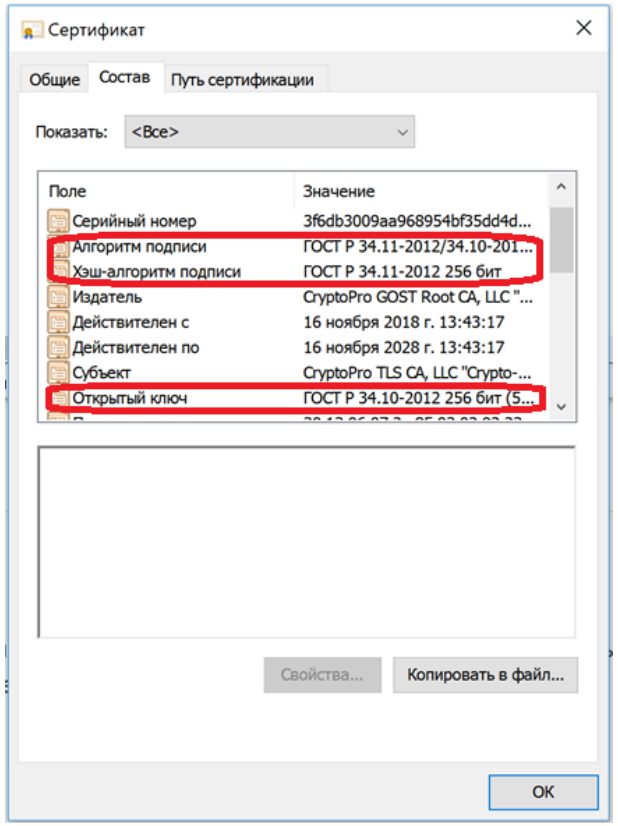
Постепенный переход на ГОСТ TLS



Два TLS-сертификата (RSA и ГОСТ) у сайтов

- Получить RSA-сертификат (в зарубежном УЦ и/или в НУЦ)
- Получить ГОСТ-сертификат
- Использовать на веб-сайте одновременно два сертификата – RSA и ГОСТ





НУЦ RSA: выявленные задачи

- Развитие НУЦ RSA и порядка применения его сертификатов в ИС в 2022 г. Внедрение НУЦ-RSA в марте 2022 – для массового применения сертификатов ГОСТ намечен путь, выявлены потенциальные трудности:
  - Важность обеспечения доверия граждан: не только развивать Certificate Transparency, но и объяснять роль этой технологии для тех, кто хочет разбираться
  - Существенная доля систем, априори полагающихся на сертификаты CAB forum
  - Важность разнонаправленности мер, направленных на массовую установку на устройства:
    - Реклама, баннеры, ссылки, инструкции
    - Поддержка госсайтами, требование доверия российским сертификатам для части услуг в личных кабинетах
    - Предустановка на легально ввозимые устройства (теперь – меньшая доля, чем раньше) и в российские ОС/ПО.
    - ACME, массовая выдача сертификатов с упрощенным подтверждением владения доменом
  - Существенный негативный эффект для перехода в случае отмены ограничений зарубежными УЦ
  - Сертификаты CAB forum необходимы для веб-сайтов, обеспечивающих взаимодействие с иностранцами

ГОСТ: дополнительные задачи

- Дополнительные трудности для ГОСТ:
  - Протоколы Certificate Transparency для ГОСТ необходимо специфицировать, стандартизировать; разработать и сертифицировать решения
  - Аспекты совместимости с СЗИ: необходимы реализации TLS с ГОСТ для СЗИ, расшифровывающих трафик
    - Не только российская проблема: TLS 1.3 и US Bank
  - Установка и встраивание нужны не только для сертификатов, но сразу и для СКЗИ
  - Протоколы ACME с ГОСТ необходимо специфицировать, стандартизировать; разработать и сертифицировать решения
  - Применение сертификатов с ГОСТ должно давать коммерческим организациям явные преимущества (либо, напротив, устранение нарушений)
  - Покрытие 100% вряд ли возможно даже в отдаленном будущем
- Важно работать в направлении продвижения применения совмещенных решений: двух TLS-сертификатов (RSA и ГОСТ)

Задачи для АНО «НТЦ ЦК»

- Над решением части задач представляется целесообразным работать вместе в рамках АНО «НТЦ ЦК»:
  - Государство (Минцифры, ФСБ России, …)
  - Разработчики СКЗИ (КриптоПро, ИнфоТеКС, Код Безопасности, …)
  - Заказчики (банки, разработчики ИС, доменные регистраторы, …)
- Архитектура, определение недостающих компонент
- Разработка протокольных решений, в том числе CT, ACME, DTLS 1.2/1.3 с ГОСТ
- Решения по автоматизированной выдаче TLS-сертификатов с ГОСТ коммерческим организациям и частным лицам
- Обеспечение доверенного распространения ПО (в частности, для массовых СКЗИ)

Спасибо за внимание!

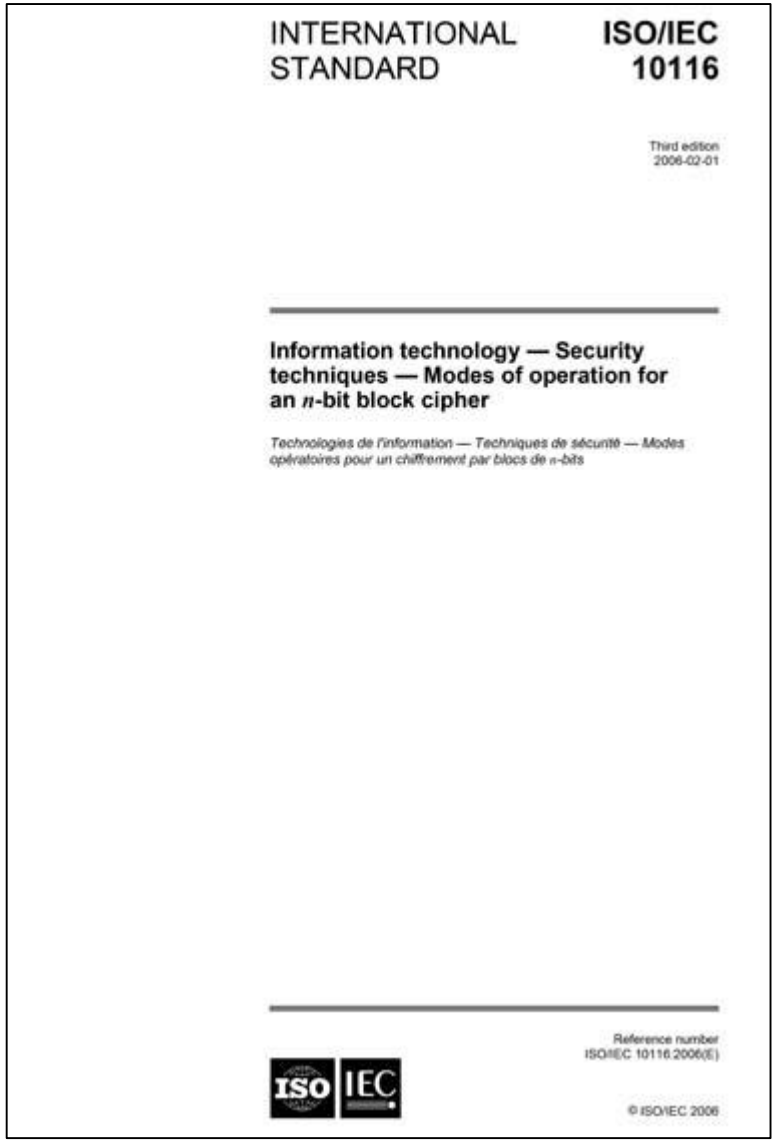
ISO/IEC 10116:2017/AMD 1:2021

- CTR-ACPKM вошел в международный стандарт ISO наряду с разработанными более 30 лет назад классическими режимами:
  - ECB (простой замены)
  - CTR (гаммирования)
  - CFB (гаммирования с обратной связью по шифртексту)
  - CBC (простой замены с зацеплением)
  - OFB (гаммирования с обратной связью по выходу)

И стал шестым режимом работы блочных симметричных алгоритмов:

- **CTR-ACPKM** (гаммирования с преобразованием ключей)

- Применяется в:
  - CMS: Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»
  - TLS 1.2: Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»


INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits

Reference number
ISO/IEC 10116:2006(E)

© ISO/IEC 2006