Гостификация ПО: подход из мира Open Source

Дмитрий Белявский, «Криптоком»
OS DAY 2019, Москва, Россия

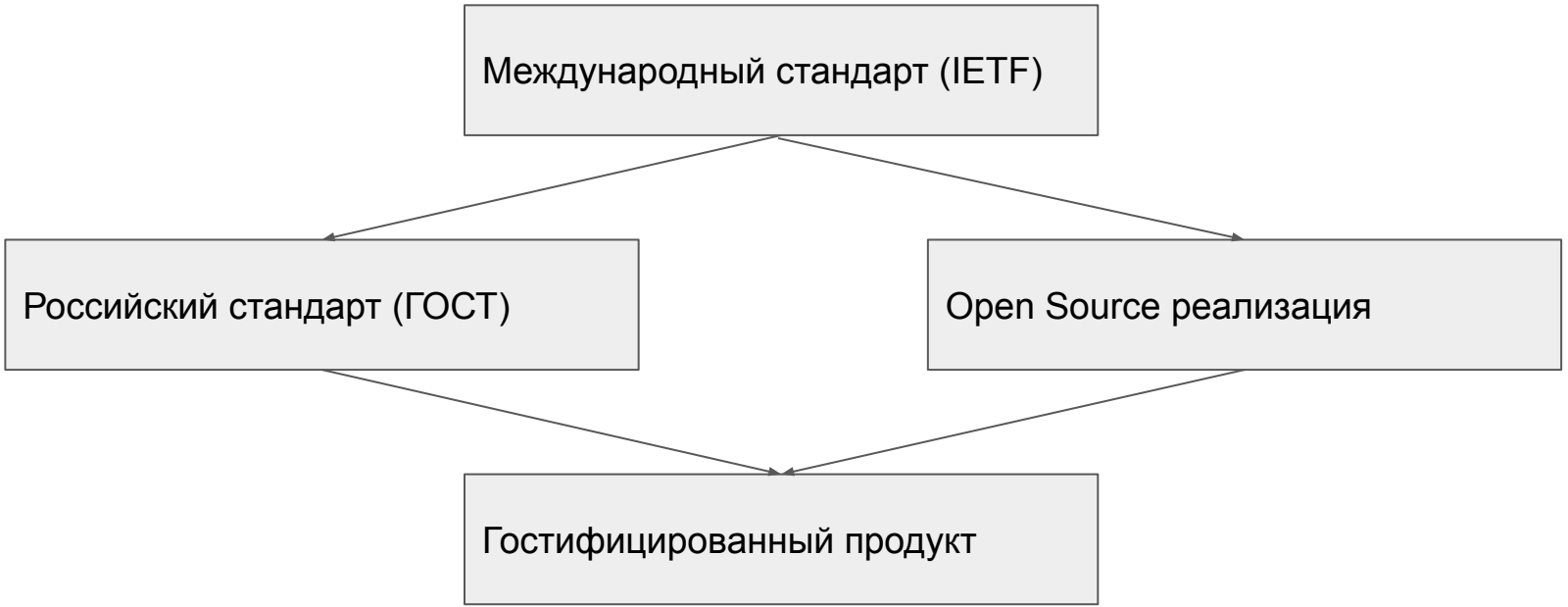
Кто я такой?

- Дмитрий Белявский, программист
- Читаю и развиваю код OpenSSL с 2005 года
  - Коммиттер с 2019 года
- Где я работаю:
  - ООО «Криптоком», https://www.cryptocom.ru/
  - Ведущий разработчик
- Мой вклад в проекты OpenSource:
  - Российские варианты TLS, CMS, PKCS12 в OpenSSL
  - GOST engine — реализация алгоритмов ГОСТ для OpenSSL
  - XMLSec — подпись по ГОСТ для XML
  - Модули Perl (криптография, домены)

Как внедряется отечественная криптография

- Проприетарные протоколы, проприетарные решения
- Стандартные протоколы, Windows
  - Хуки
  - Бинарные патчи
  - Трудности при реализации протоколов в полном виде
  - Трудности при обновлениях
- Стандартные протоколы, системы с открытым кодом
  - Расширяем при необходимости протокол
  - Реализация протокола уходит в сообщество
  - Сертифицированные решения: Open Source продукт + немного закрытого кода
  - Если сертификат не нужен: открытая реализация

Жизненный цикл стандартов и их воплощения



Где можно поучаствовать?

- Процесс стандартизации в IETF — легко
  - Открытый процесс, индивидуальное участие
- Процесс российской стандартизации — тяжело
  - Надо быть представителем организации
- Реализация протокола — требует специфических знаний
- Гостификация — требует специфических знаний

Где поддержана российская криптография

- OpenSSL
  - Отдельный engine (https://github.com/gost-engine/engine)
  - Протоколы — в основном коде
  - LibreSSL
- Прочие библиотеки
  - GnuTLS
  - Libgcrypt
  - Патчи для NSS, Nettle, etc
- Ядро Linux
  - Хеш — начиная с версии 5.0
  - Подпись — подсистема EVM/IMA, начиная с версии 5.2

Каждая библиотека теоретически позволяет добавить поддержку сразу в большое количество приложений

Международная стандартизация

- RFC:
  - RFC 4357, 4490, 4491, 5830-32 — «старые» алгоритмы, 1994-2001 годы
  - RFC 6986, 7091, 7801, 7836 — «новые» алгоритмы
  - https://tools.ietf.org/html/draft-smyshlyaev-tls12-gost-suites-04 — WIP TLS 1.2
- Регистрация в IANA
  - Алгоритмы
  - Криптонаборы для TLS
- Без регистрации идентификаторов работа обесценивается
  - Для регистрации нужны стандарты на английском

Чего нам не хватает

- Людей
  - Энтузиасты
  - Часть кода из коммерческих компаний
    - Это выгодно — экономия на поддержке
- Инфраструктуры
  - Нет нормальной иерархии УЦ
  - Нет признанных УЦ
- Реализации на популярных языках
  - Java

Полезные ссылки

- Листы рассылки
  - https://lists.altlinux.org/mailman/listinfo/oss-gost-crypto
  - http://www.wagner.pp.ru/list-archives/openssl-gost/
- Реализации
  - ГОСТ engine https://github.com/gost-engine/engine
- Стандарты
  - ТК 26 https://tc26.ru/

Спасибо тем, кто

OpenSSL: Dr. Stephen Henson, Rich Salz, Richard Levitte, Matt Caswell

Российские криптографические компании: Василий Долматов, Вартан Хачатуров, Игорь Устинов, Станислав Смышляев, Валерий Смыслов

AltLinux: Алексей Новодворский, Дмитрий Левин, Виталий Чикунов, Глеб Фотенгауэр-Малиновский, Павел Волнейкин

Криптоэнтузиасты: Александр Боковой, Дмитрий Ерёмин-Солейников, Виктор Вагнер, Артём Чуприна, Алексей Дегтярёв, Максим Тишков, Илья Шипицын

Вопросы?

beldmit@cryptocom.ru

beldmit@gmail.com