

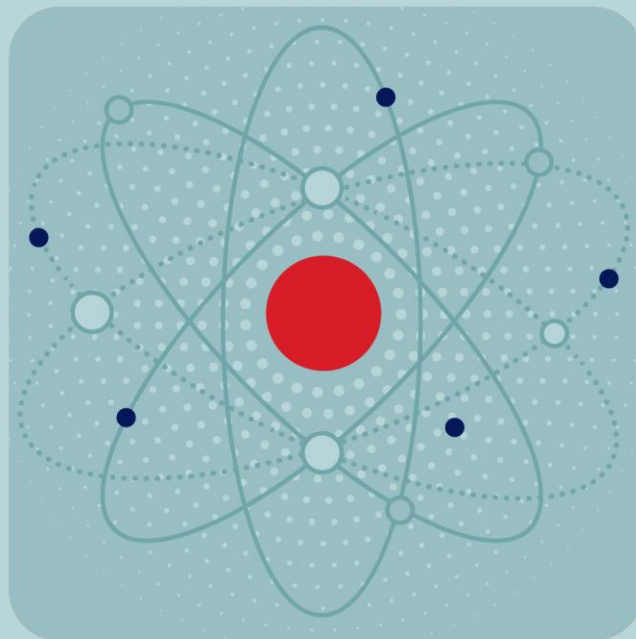
ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН

ОАЧ

ТЕХНОЛОГИИ

ДОВЕРИЯ



КОМПАНИЯ
ПРАКТИВ

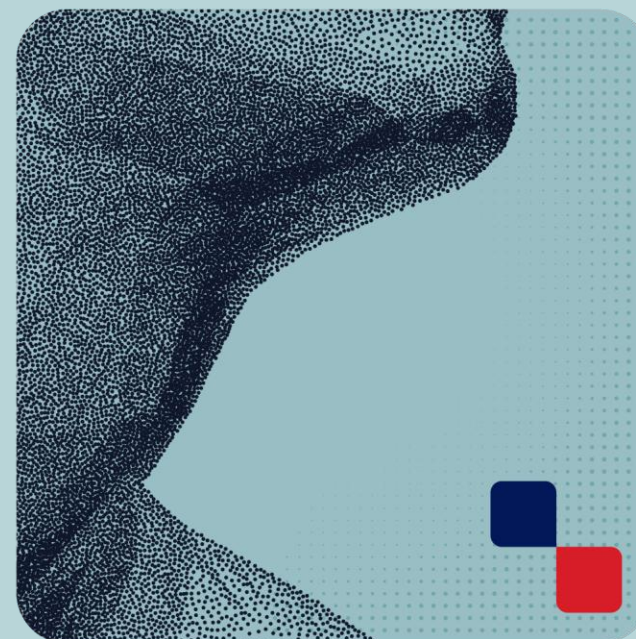


Open source-инициативы

Как и почему мы контрибьютим
в open source

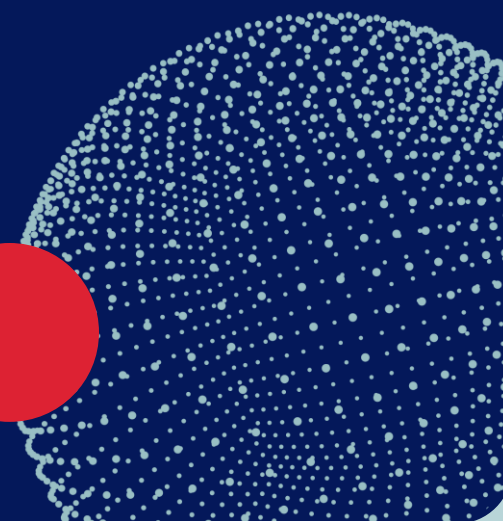
**Евгений
Мироненко**

Руководитель отдела исследований,
Компания «Актив»





Кто использует open source?



Выбор: как добавить функции



	Open source	Своя разработка	Чужая закрытая разработка
Стоимость старта	+	-	+/-
Время старта	+	-	+
Гибкость / контроль / отладка	+/-	+	-
Зависимость (lock-in)	+/-	+	-
Операционная сложность	+/-	-	+

**Быстро, дешево, надежно,
но есть нюанс...**



**Бесплатный
ускоритель**



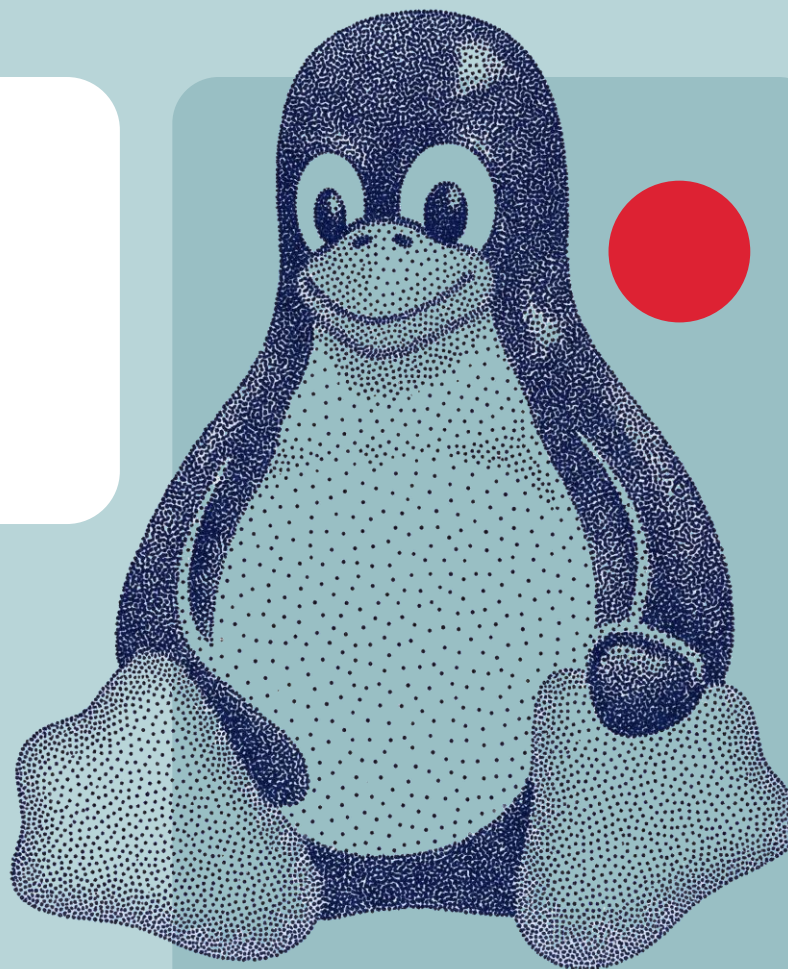
**Источник
риска**



Рутокен + Linux

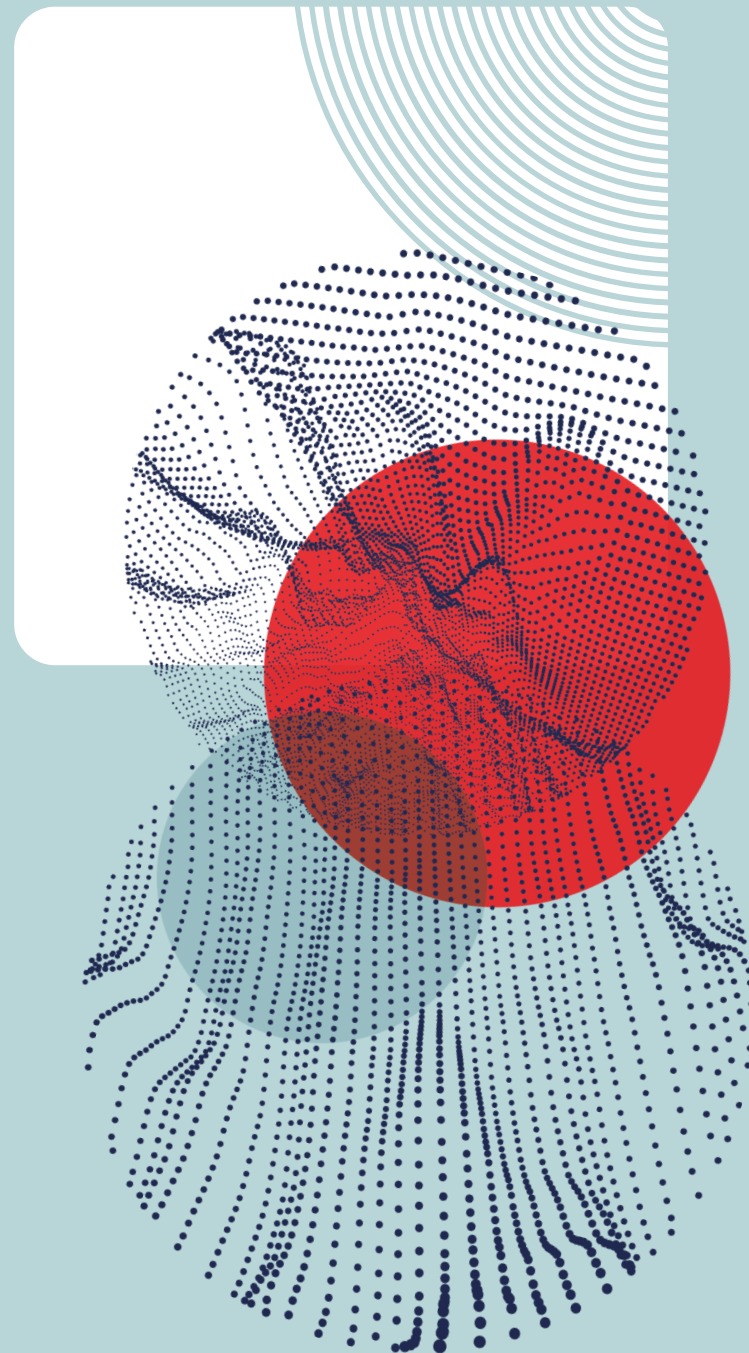


- ✓ Открытый код
- ✓ Нет привычного CryptoAPI
- ✓ Нужен криптографический интерфейс

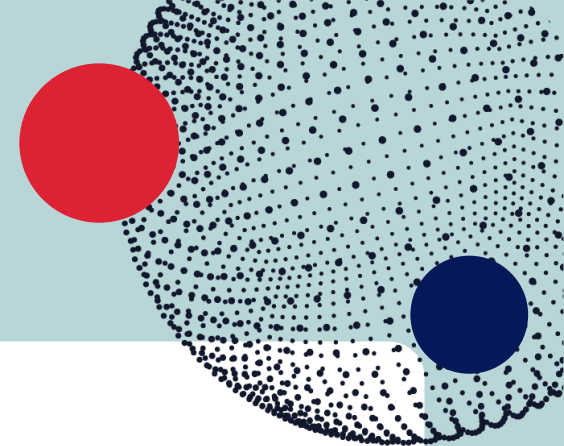


Рутокен + OpenSSL

- ✓ Наша криптография
- ✓ Международные криптопротоколы
- ✓ Привычный интерфейс
- ✓ Удобство для партнеров



Рутокен + OpenSSL



OpenSSL

криптопротоколы и программная криптография

ENGINE interface

engine_pkcs11
RSA
на смарт-картах

engine_rand
аппаратный
ГСЧ

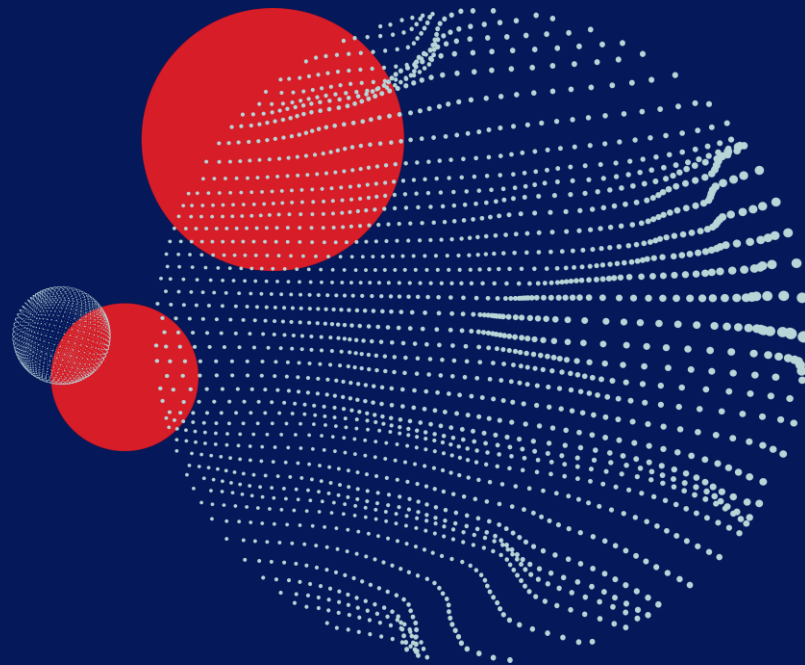
engine_vigenere
новый
криптоалгоритм

gost_engine
программные
алгоритмы
ГОСТ

rtengine
алгоритмы
ГОСТ
на Рутокен



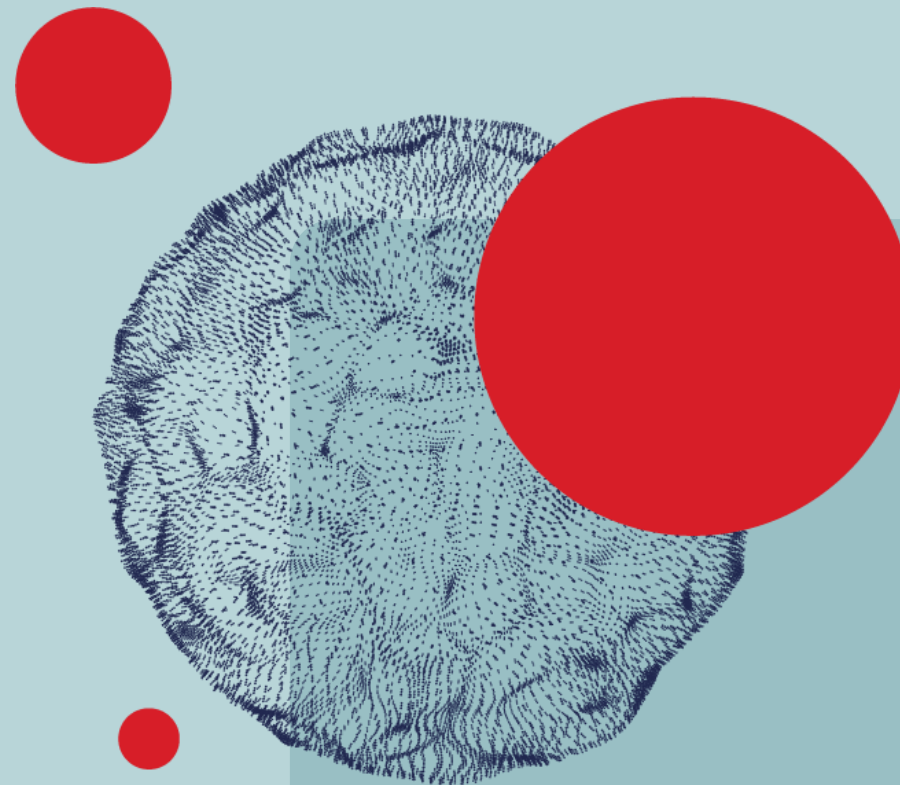
OpenSSL не совсем подходит.
Отечественные криптопротоколы
отличаются от международных



Gost-engine



- ✓ Референсная реализация
- ✓ Тестирование с OpenSSL
- ✓ Продвижение особенностей российских протоколов



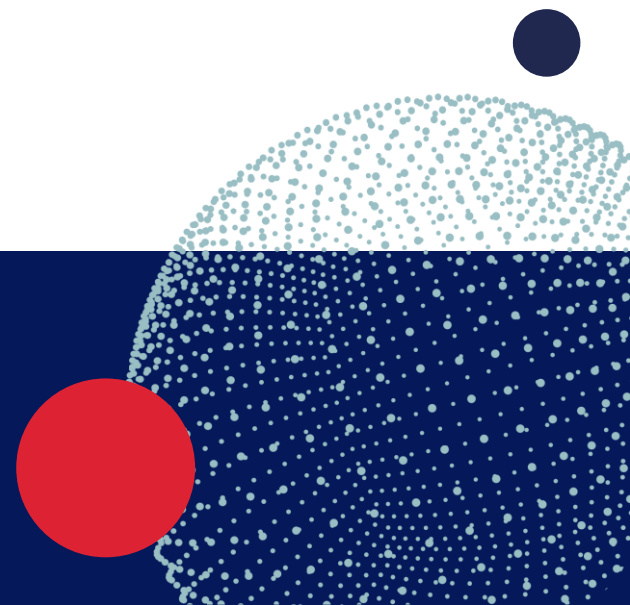
«Здоровые» отношения



Кризис



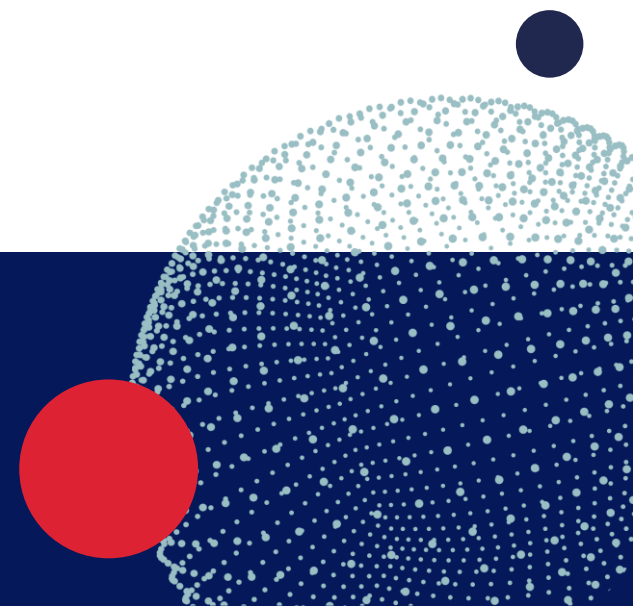
✓ **OpenSSL: ENGINE -> PROVIDER**



Кризис



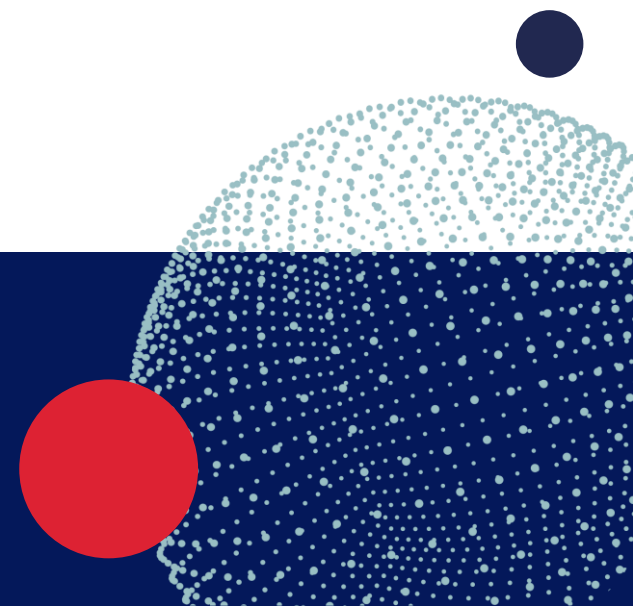
- ✓ **OpenSSL: ENGINE -> PROVIDER**
- ✓ **Gost-engine: мейнтейнер «остыл»**



Кризис



- ✓ **OpenSSL: ENGINE -> PROVIDER**
- ✓ **Gost-engine: мейнтейнер «остыл»**
- ✓ **Нам нужен TLS 1.3**

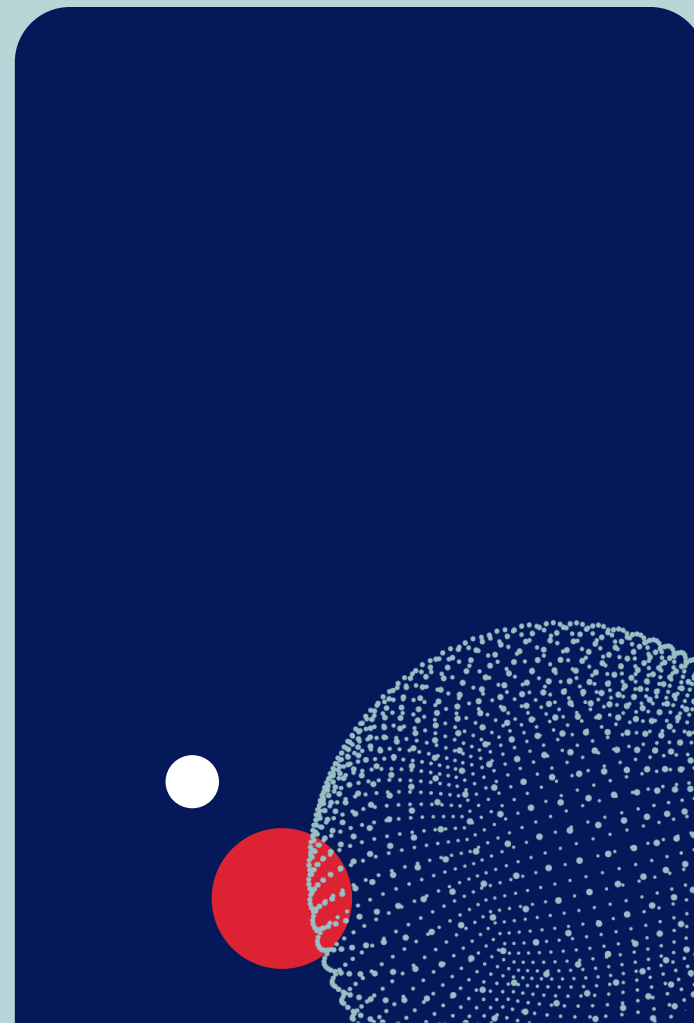


Что делать?



FORK

- ✓ быстро
- ✓ полный контроль
- ✓ ты владелец



Что делать?



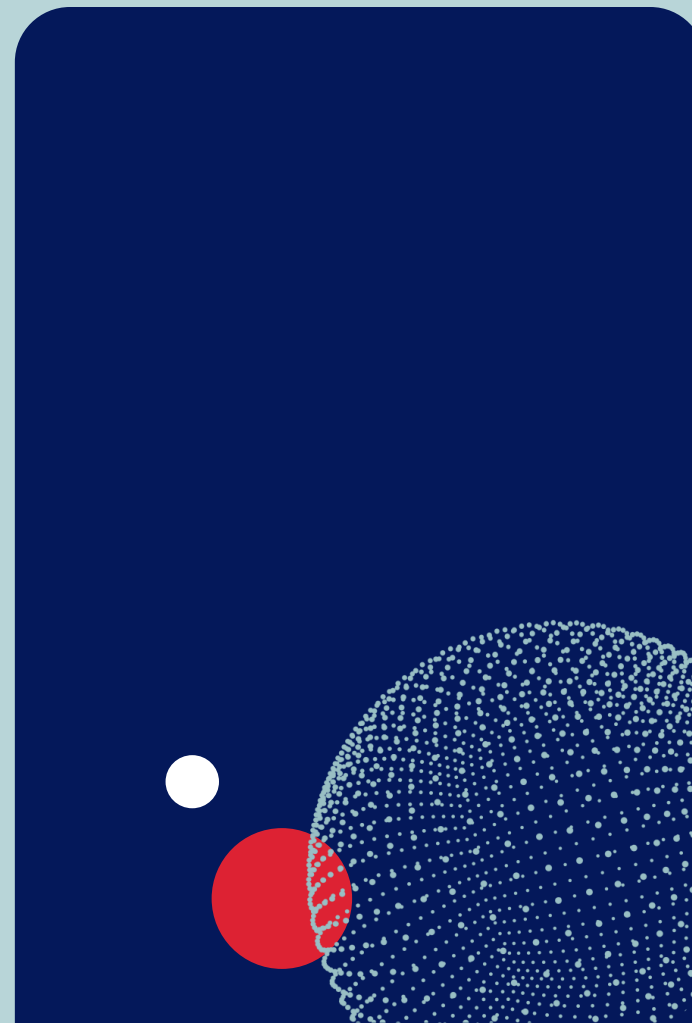
FORK

- ✓ быстро
- ✓ полный контроль
- ✓ ты владелец



Свой стек

- ✓ дорого
- ✓ полный контроль
- ✓ ты владелец



Что делать?



FORK

- ✓ быстро
- ✓ полный контроль
- ✓ ты владелец



Свой стек

- ✓ дорого
- ✓ полный контроль
- ✓ ты владелец

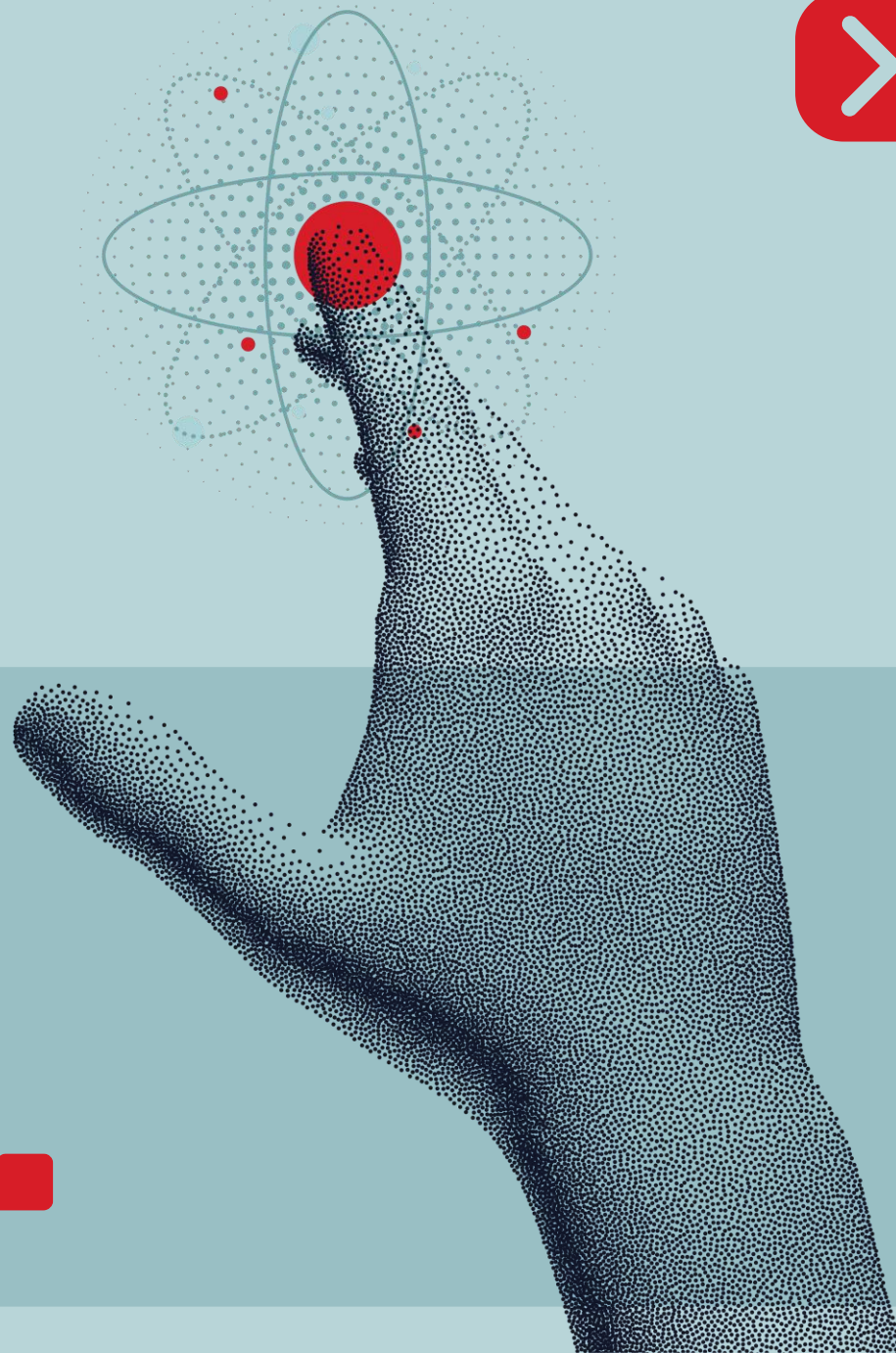
Upstream

- ✓ долго
- ✓ зависимость
- ✓ ты участник,
поддержка
сообществом



Мы выбрали upstream

- ✓ Gost-engine -> gost-provider
- ✓ Минимальная функциональность для TLS 1.3
- ✓ Патч в OpenSSL



Что сделали

- ✓ Используем provider-cipher, -digest, -mac поверх ENGINE
- ✓ Добавляем provider для ассимметричных алгоритмов
- ✓ Патч в OpenSSL с TLS 1.3
- ✓ Тестирование с серверами ИнфоТеКС и КриптоПро

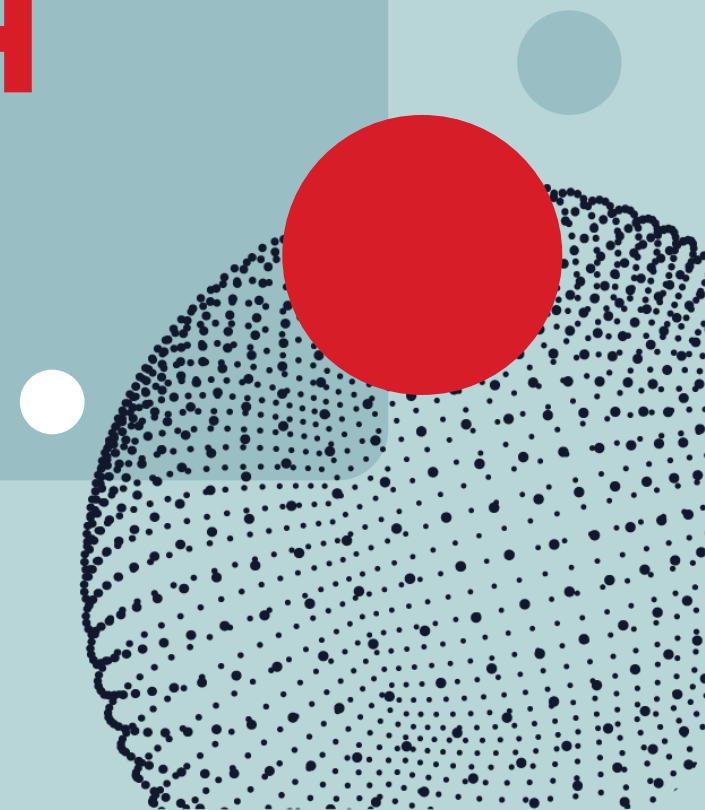


Все готово, **НО...**



ENGINE удален

> provider-cipher, -digest, -mac
поверх ENGINE



Цена

#1

Еще тысячи строк
изменений

#2

Условная компиляция
ENGINE/PROVIDER под
разные версии OpenSSL

#3

Новая синхронизация
с upstream еще в будущем



Open source – это здорово, но не бесплатно



Участие в развитии

Погоня за upstream





Евгений
Мироненко

Руководитель отдела
исследований,
Компания «Актив»



mironenko@rutoken.ru
info@rutoken.ru



www.rutoken.ru
www.aktiv-company.ru



+7 495 925-77-90
+7 905 509-28-00