Криптографические стандарты: планы на 2017 год

С.В. Агиевич

НИИ прикладных проблем математики и информатики
Белгосуниверситета

ТИБО

[Минск, 20.04.2017]

1: Криптографическая инфраструктура

ГосСУОК

(единая система управления открытыми ключами)

МСИ, Id-карта

(универсальная идентификация и аутентификация)

СТБ 34.101.bias: топология, объекты, протоколы, интерфейсы, форматы

форматы криптографических данных	службы	общие требования	прикладные протоколы
сертификаты открытых ключей, CMS, OCSP, **идентификаторы**, **XML DSig/Enc**, атрибутные сертификаты, **расширенные ЭЦП**	**штампов времени, заверения данных**	СКЗИ (в т.ч. аппаратные)	протокол TLS 1.2 с дополнительными криптонаборами
СТБ 34.101.17,19,23,26,**50**,67, **ades**	**СТБ 34.101.ts** **СТБ 34.101.dvcs**	СТБ 34.101.27	СТБ 34.101.65

криптографические алгоритмы и протоколы											
шифрование (формат, дисковое)	имитозащита	хэширование	ЭЦП	транспорт	HMAC	PRNG	**OTP**	разделение секрета	формирование общего ключа, аутентификация	хэширование	древовидное хэш-ие шифрование имитозащита защита сеансов
СТБ 34.101.31			СТБ 34.101.45		СТБ 34.**101.47**			СТБ 34.101.60	СТБ 34.101.66	СТБ 34.101.77	

2: СТБ 34.101.31: алгоритмы belt

Ядро: блочная криптосистема belt (2002+)

Идеи: экспоненциальные S-блоки • смешение операций (ARX)
• режим MR-AE (belt-datawrap) • XS-схемы (belt-keywrap)
• преобразование ключа (belt-keyrep)

Планы:

- шифрование с сохранением формата
- дисковое шифрование

Шифрование с сохранением формата:

9112 0000 9123 4567 $\mapsto$ 1415 9265 3589 7932 (10^{12})

1Ez5NQQu...hFeBm $\mapsto$ 1F1tAaz5...n4xqX ($58^{26\div35}$)

3: СТБ 34.101.77: алгоритмы хэширования bash

Ядро: sponge-функция Bash-f: $\{0,1\}^{1536} \to \{0,1\}^{1536}$

Длины хэш-значений: $32, 64, \ldots, 512$

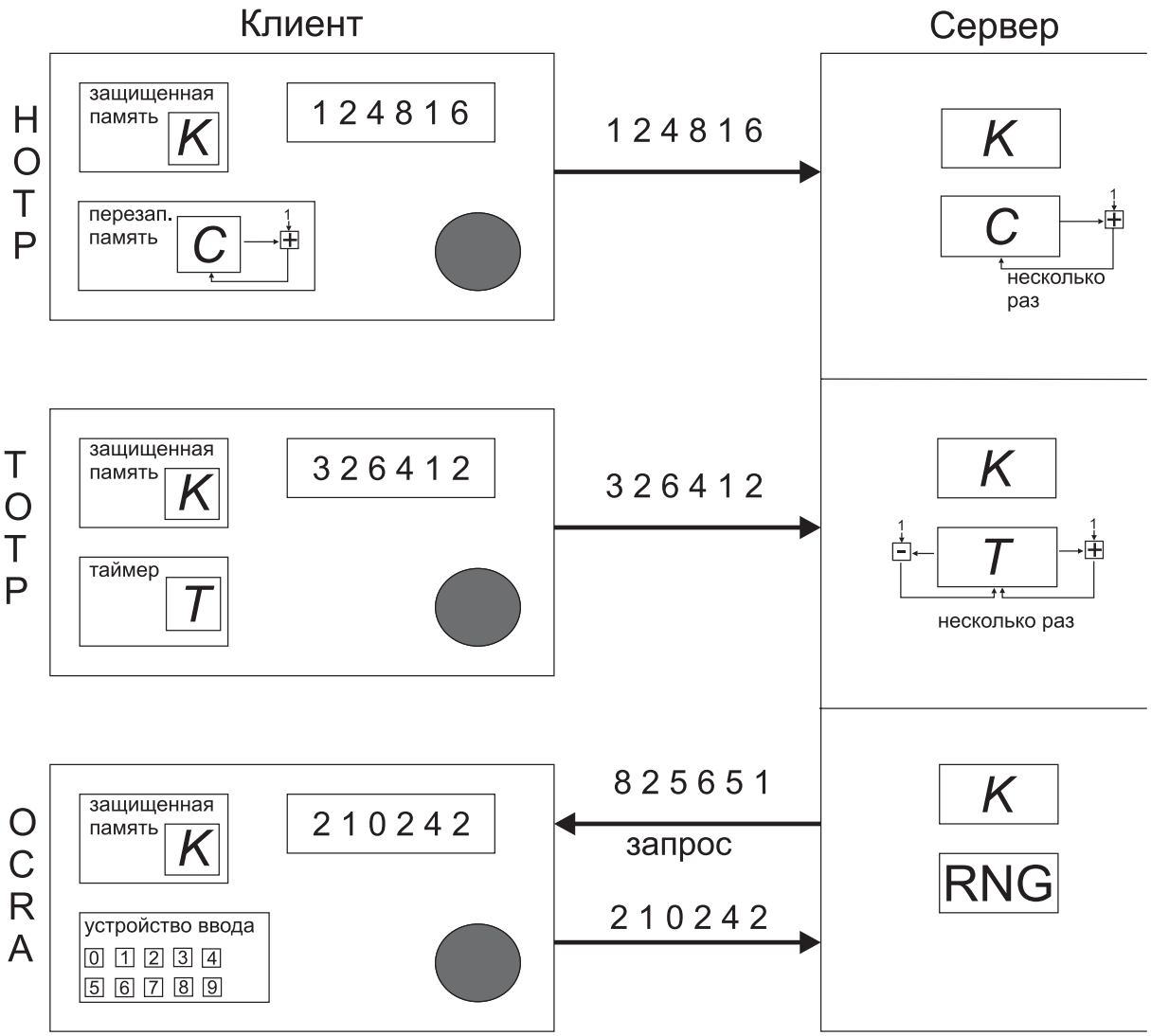
Алгоритмы ЭЦП: bign-with-bash256, bign-with-bash384, bign-with-bash512

Перспективы:

- древовидное хэширование (деревья Меркля, блокчейн)
- параллельное хэширование
- **поточное шифрование** (очень быстро на ПЛИС!)
- **имитозащита** (очень быстро на ПЛИС!)
- **защищенные сеансы** (очень быстро на ПЛИС!)

Новости: ~~SHA-1~~ (22 года), SHA-2 vs SHA-3

4: СТБ 34.101.47: одноразовые пароли



5: СТБ 34.101.47: одноразовые пароли-II

Система	Аппаратные требования	Синхронизация	Надежность
На основе событий	интерфейс вывода (дисплей)	динамически по правильным паролям, возможна потеря	средняя
На основе времени	интерфейс вывода, таймер	согласование времени	высокая
На основе запросов	интерфейс вывода и ввода (клавиатура)	не нужна	высокая

Стандартная реализация: `hmac[belt-hash]`

is welcome!

6: СТБ 34.101.17, 19, 23, 26, 50, 67: форматы

Проблемы:

- многообразие (СОК, СОС, АС, SignedData, XML-DSIG,...)
- разнородность (АСН.1, XML,...)
- вариабельность (optional, choice,...)
- сложность (главный враг безопасности)

Решения:

- профилирование (конкретизация) форматов
- адаптированный (не буквальный) перевод стандартов

7: ЭЦП 3.0

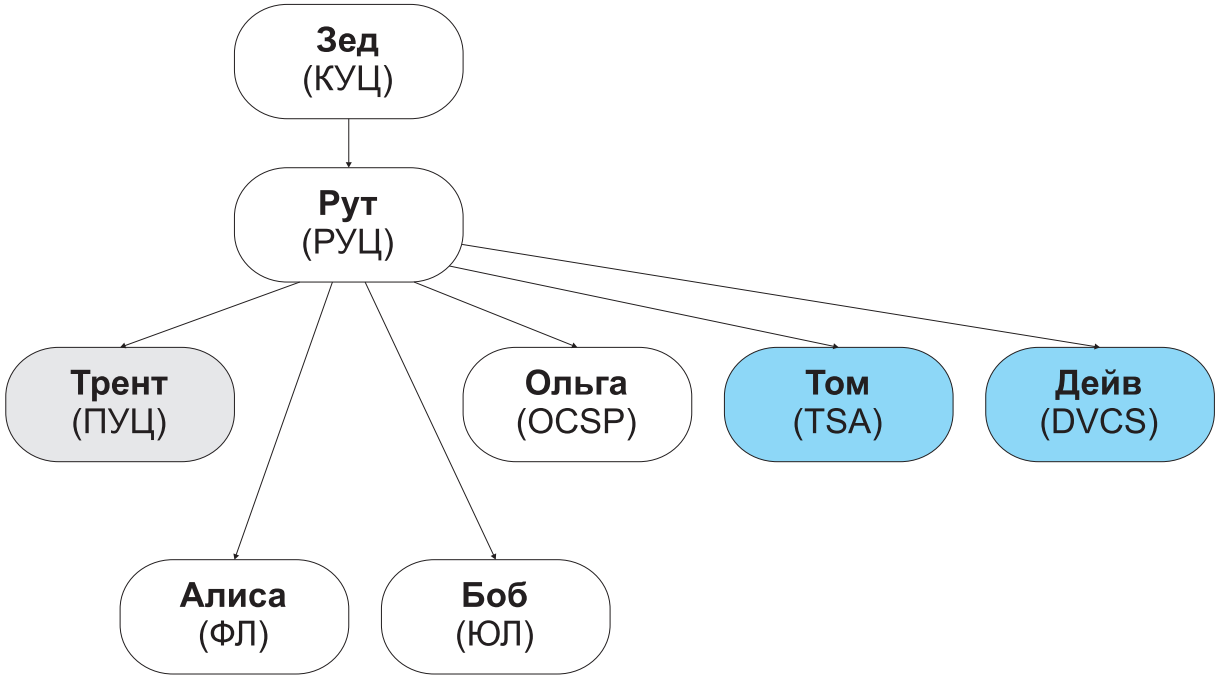
Закон об ЭЦП 1999: эцп, эд, лк, ок, карточка ок, средство

Закон об ЭЦП 2009: сертификат ок, ГосСУОК

Что дальше?

- новые поставщики услуг доверия (службы)
- расширенные подписи
- API взаимодействия со службами ГосСУОК
- новые сервисы ГоСУОК
- API взаимодействия с носителями лк

8: Поставщики услуг доверия



TSA = служба штампов времени

DVCS = служба заверения данных

9: СТБ 34.101.ts, dvcs

Служба штампов времени:

- запрос — $h(O)$
- ответ — $\texttt{Signed}(h(O), time)$ (штамп времени)
- интерпретация — объект O существовал к моменту $time$
- *тонкая интерпретация* — если O предъявлен после $time$ и h сохраняет стойкость

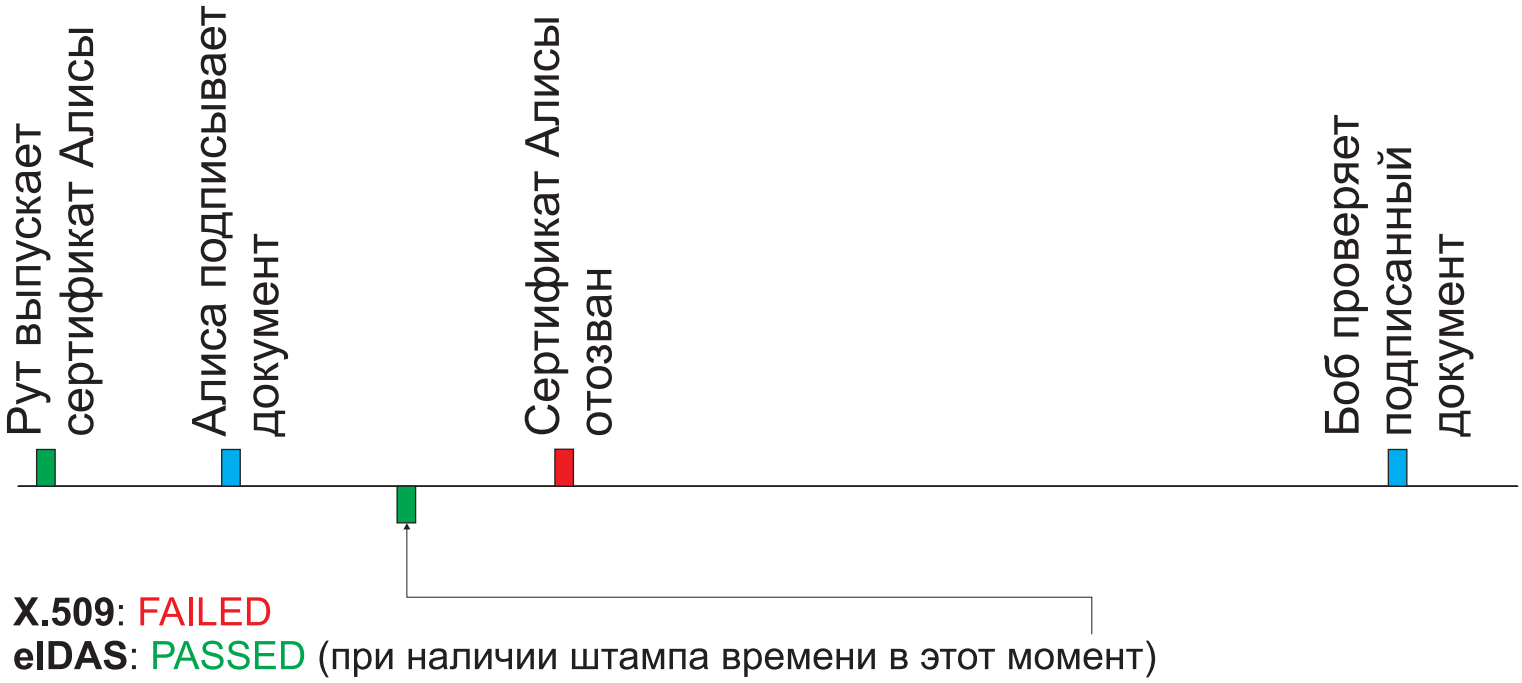
Служба заверения данных:

- заверение факта владения данными
- заверение факта существования данных (дублирование TSA)
- заверение сертификатов (дублирование OCSP)
- заверение ЭД (междоменное взаимодействие)

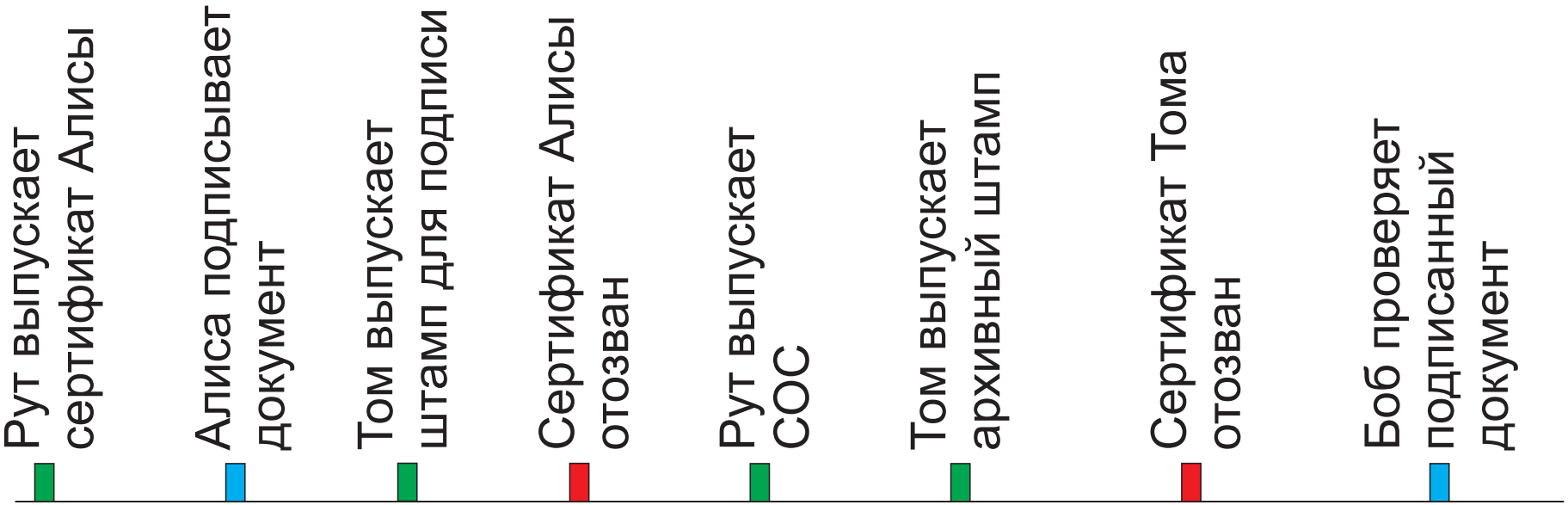
10: Модели проверки ЭЦП

X.509 (PKIX, СТБ 34.101.19): сертификат действителен в момент проверки

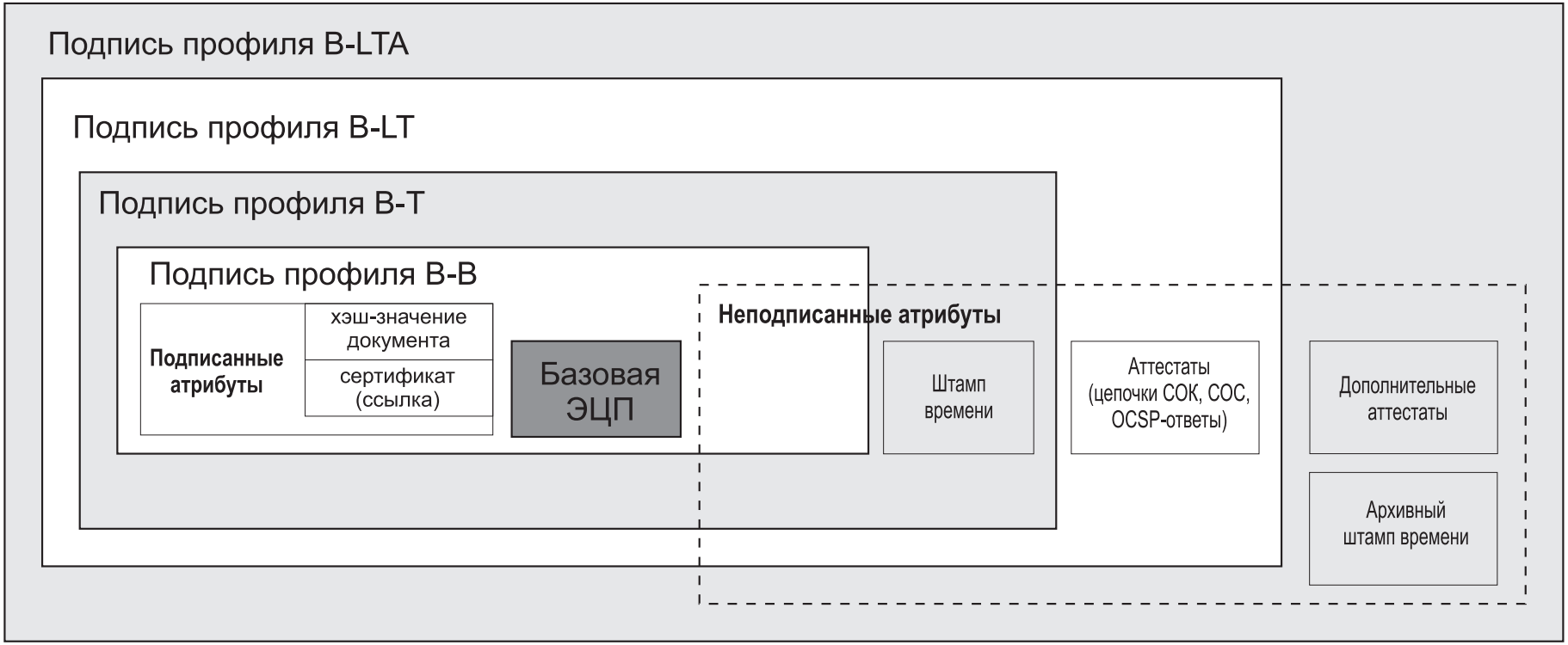
eIDAS (ETSI): сертификат действителен в момент выработки



11: Проверка ЭЦП (большой пример)



12: СТБ 34.101.ades: расширенные ЭЦП



13: Массовая аутентификация

Проекты: МСИ, БИСРС, Id-карта

14: СТБ 34.101.bias: аутентификация

Том 1: Архитектура аутентификации

- токены (пароль, карта секретов, криптографический,. . .)
- процедуры и протоколы
- билеты

Том 2: Реализация на основе OIDC (расширение OAuth 2.0)

Том 3: Криптографические токены (id-карты)

- объекты (сертификаты, личные ключи)
- пароли (PIN, PUK, CAN)
- криптографические протоколы
- APDU-команды

15: Реализация

Доверие к криптографическим продуктам:

- через доверие к ОАЦ[система ИЛ]/Microsoft/Samsung/...
- прямой доступ к программам, возможность сборки

Вторая модель:

- открытые операционные системы
- открытые криптобиблиотеки (OpenSSL, BouncyCastle)
- клиенты Bitcoin и Ethereum, TrueCrypt, Signal, Telegram,...
- библиотека bee2 

16: Библиотека bee2

 – криптоядро (нижний слой)

Расширения (средний слой):

bee2evp =  in OpenSSL

bee2j =  in Java

Возможности bee2evp:

```
openssl engine -c -t bee2evp

(bee2evp) Bee2evp Engine [belt + bign + bash]
[belt-ecb128, belt-ecb192, belt-ecb256, belt-cbc128, belt-cbc192,
belt-cbc256, belt-cfb128, belt-cfb192, belt-cfb256, belt-ctr128,
belt-ctr192, belt-ctr256, belt-dwp128, belt-dwp192, belt-dwp256,
belt-kwp128, belt-kwp192, belt-kwp256, bash256, bash384, bash512,
belt-hash, bign-with-hspec, bign-with-hbelt, bign-with-bash256,
bign-with-bash384, bign-with-bash512, bign-keytransport, bign-curve256v1,
bign-curve384v1, bign-curve512v1, bign-primefield, bign-pubkey,
belt-mac128, belt-mac192, belt-mac256, belt-hmac]
```

17: Первый белорусский криптограф

18: Ресурсы

groups.google.com:bcrypto

http://apmi.bsu.by/resources/std

http://apmi.bsu.by/resources/tools

https://github.com/bcrypto

https://github.com/agievich/bee2