ТК 26:
от алгоритмов к протоколам

Александр Бондаренко
Григорий Маршалко
Василий Шишкин

ТК 26
ГОСТ Р

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

- организация **разработки** и **экспертизы** проектов **национальных** стандартов, **межгосударственных** и **международных** стандартов

- участие в работе **международных** (межгосударственных) **организаций** по стандартизации

ТК 26
ГОСТ Р

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

- **68** членов :
  - **20** государственных
  - **48** частных

- **4** подкомитета

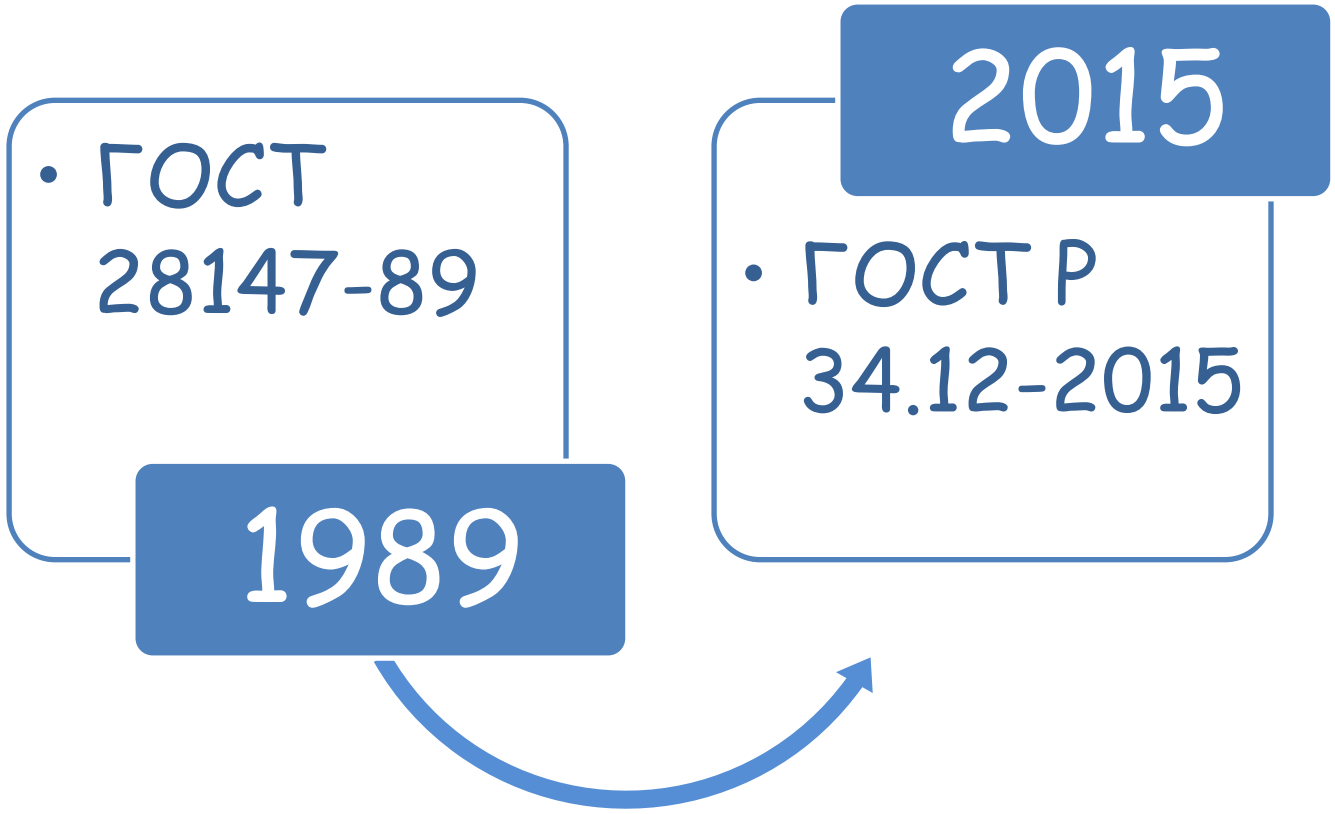
- **5** рабочих групп

ТК 26
ГОСТ Р

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

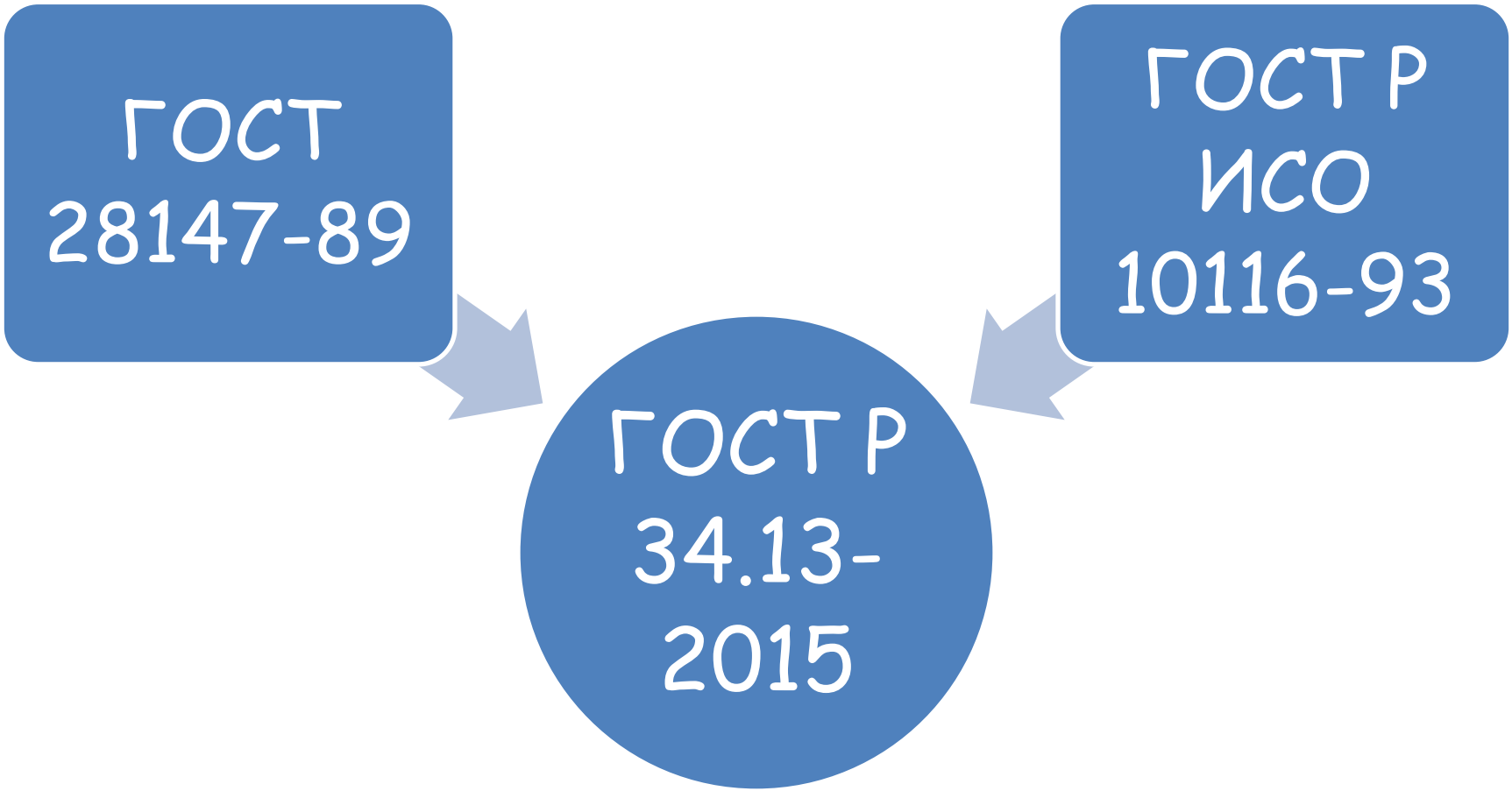
ТК 26 ГОСТР

Российские криптографические стандарты: блочные шифры



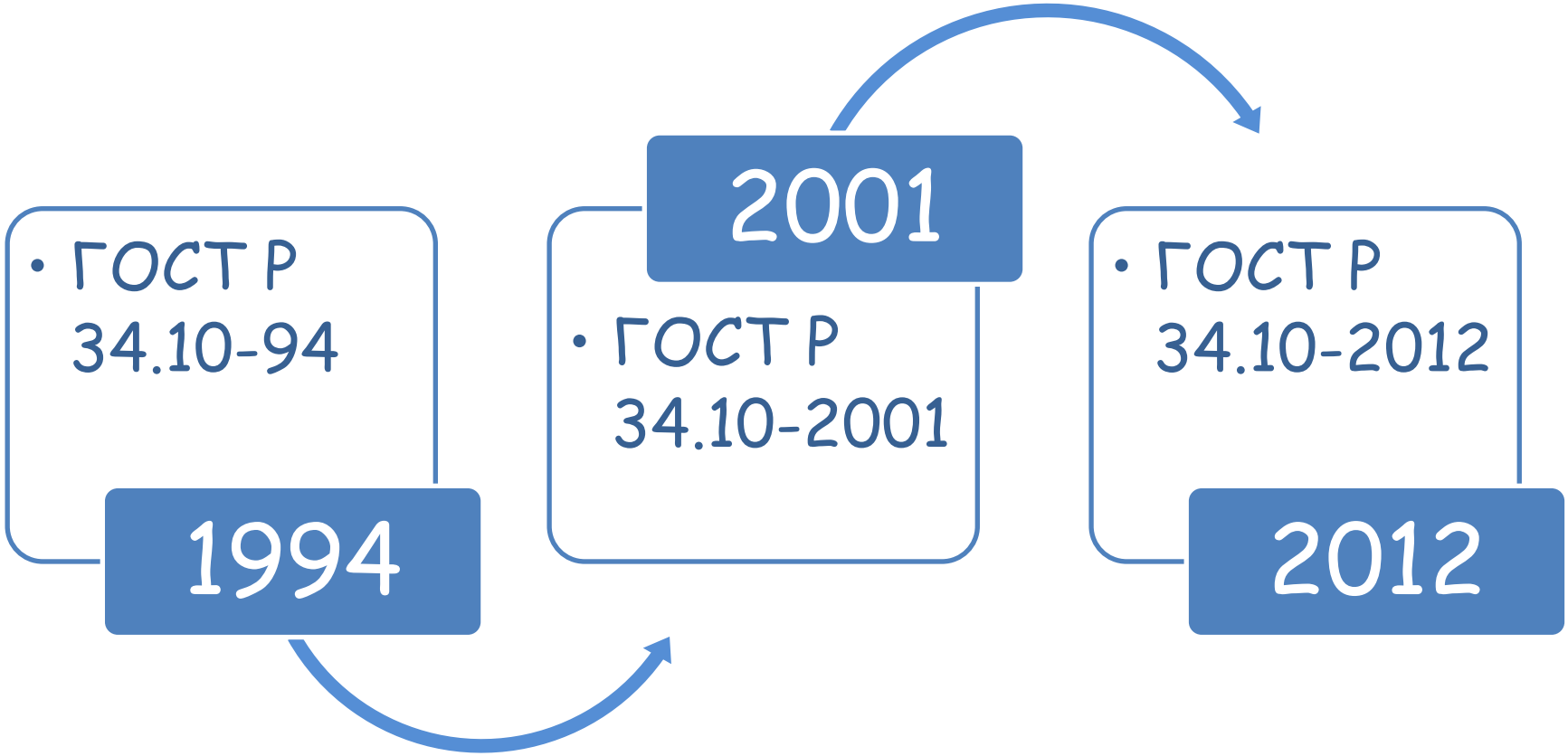
ТК 26 ГОСТ Р

Российские криптографические стандарты: режимы блочных шифров



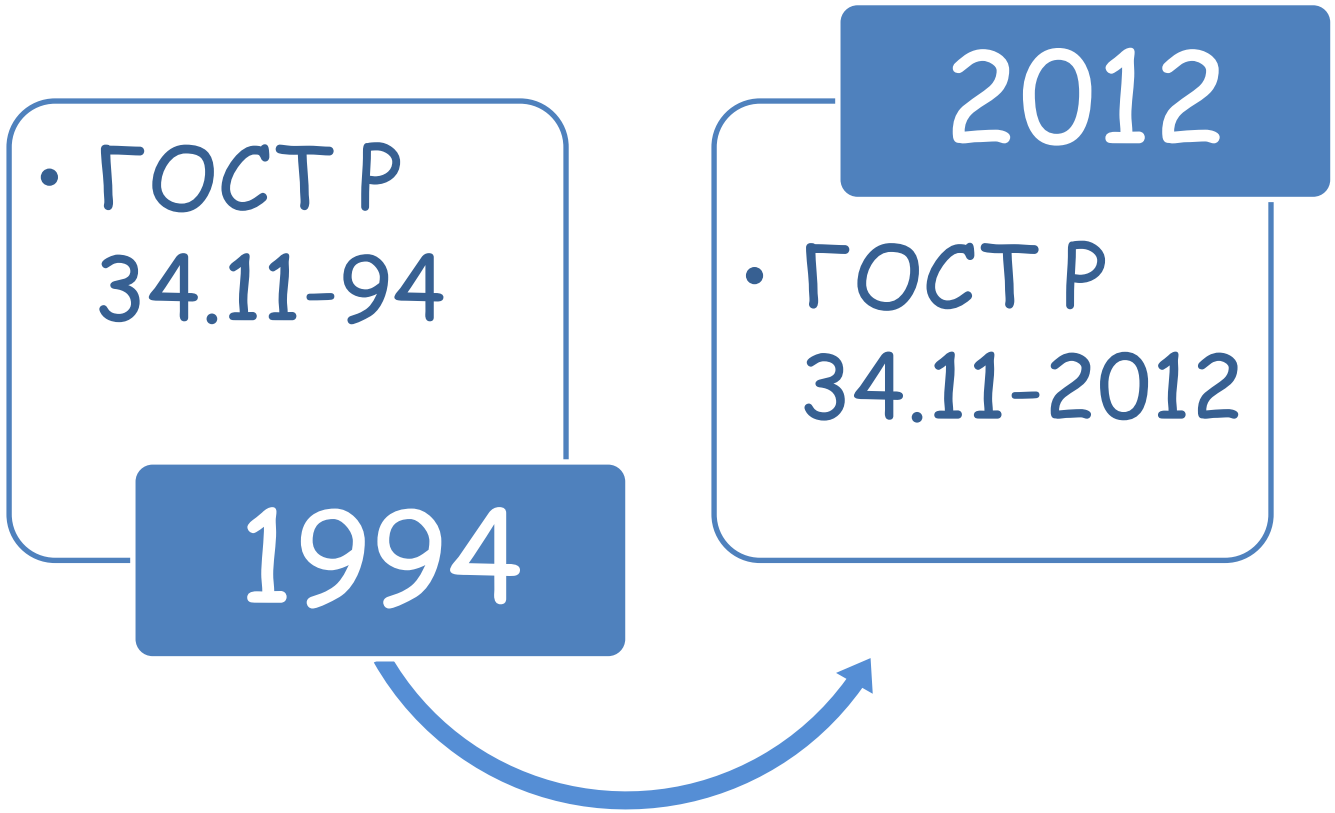
ТК 26 ГОСТ Р

Российские криптографические стандарты: электронная подпись



ТК 26 ГОСТ Р

Российские криптографические стандарты: хэш-функция



ТК 26 ГОСТ Р

Отечественные стандарты «второго» поколения

- ГОСТ Р 34.10-2012 (**подпись**):
  ISO/IEC 14888-3
- ГОСТ Р 34.11-2012 (**хэш**): RFC 6989
- ГОСТ Р 34.12-2015 (**шифры**):
  Магма aka ГОСТ 28147-89
  Кузнечик: RFC 7801
- ГОСТ Р 34.13-2015 (**режимы**):
  ~ ISO/IEC 10116

ТК 26
ГОСТ Р

Применение стандартов: методические рекомендации и технические спецификации

- Идентификаторы объектов (OID) технического комитета по стандартизации ТК 26
- Парольная защита с использованием алгоритмов ГОСТ (дополнения к PKCS#5)
- Транспортный ключевой контейнер (дополнения к PKCS#8 и PKCS#12)
- Ключевой контейнер (дополнение к PKCS#15)

ТК 26
ГОСТ Р

Применение стандартов: методические рекомендации и технические спецификации

- Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89
- Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012
- Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012
- Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012

ТК 26 ГОСТ Р

Применение стандартов: методические рекомендации и технические спецификации

- Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS
- Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)
- Протокол выработки общего ключа с аутентификацией на основе пароля

ТК 26
ГОСТ Р

Утверждение рекомендаций в Росстандарте

- Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования
- Параметры эллиптических кривых для криптографических алгоритмов и протоколов
- Протокол выработки общего ключа с аутентификацией на основе пароля
- Парольная защита ключевой информации
- Транспортный ключевой контейнер
- Контейнер хранения ключей

ТК 26
ГОСТ Р

Рабочие проекты

- Механизмы выработки псевдослучайных последовательностей
- Механизмы выработки производных ключей
- Схемы выработки ключа двумя абонентами по открытому каналу связи
- Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов в сетях мобильной связи (S3G-128 и S3G-256)

ТК 26
ГОСТ Р

Рабочие проекты

- Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования
- Использование ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 в сообщениях CMS
- Использование ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 в протоколе TLS версии 1.2
- Сертификаты X.509 ключей проверки подписи ГОСТ Р 34.10-2012

ТК 26
ГОСТ Р

Рабочие проекты (НСПК)

Ведется разработка 10 рекомендаций по стандартизации, определяющих использование отечественных алгоритмов в стандарте EMV: оффлайновая проверка PIN, имитозащита прикладных криптограмм, режимы шифрования в протоколе SCP-2, формирование производных ключей и др.

ТК 26 ГОСТ Р

Рабочие проекты (перспектива)

- Режимы блочных шифров, обеспечивающие одновременно шифрование и аутентификацию
- Древовидное хэширование
- Режимы блочных шифров, обеспечивающие шифрование статических данных
- Использование отечественных алгоритмов в протоколе TLS 1.3

ТК 26
ГОСТ Р

Спасибо за внимание!

Следите за новостями ТК 26:

www.tc26.ru

@CryptographyRU

www.ctcrypt.ru

ТК 26
ГОСТ Р