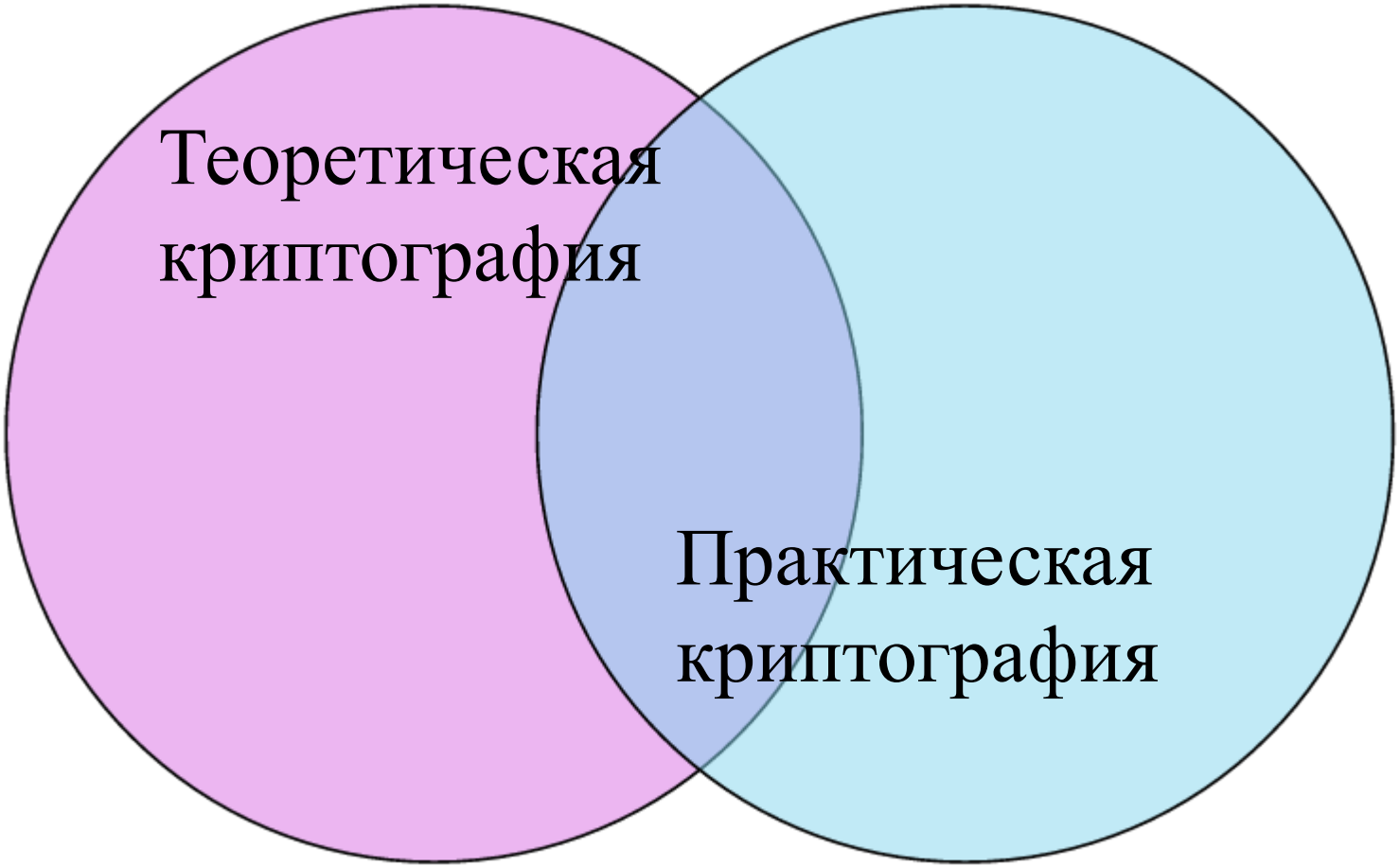
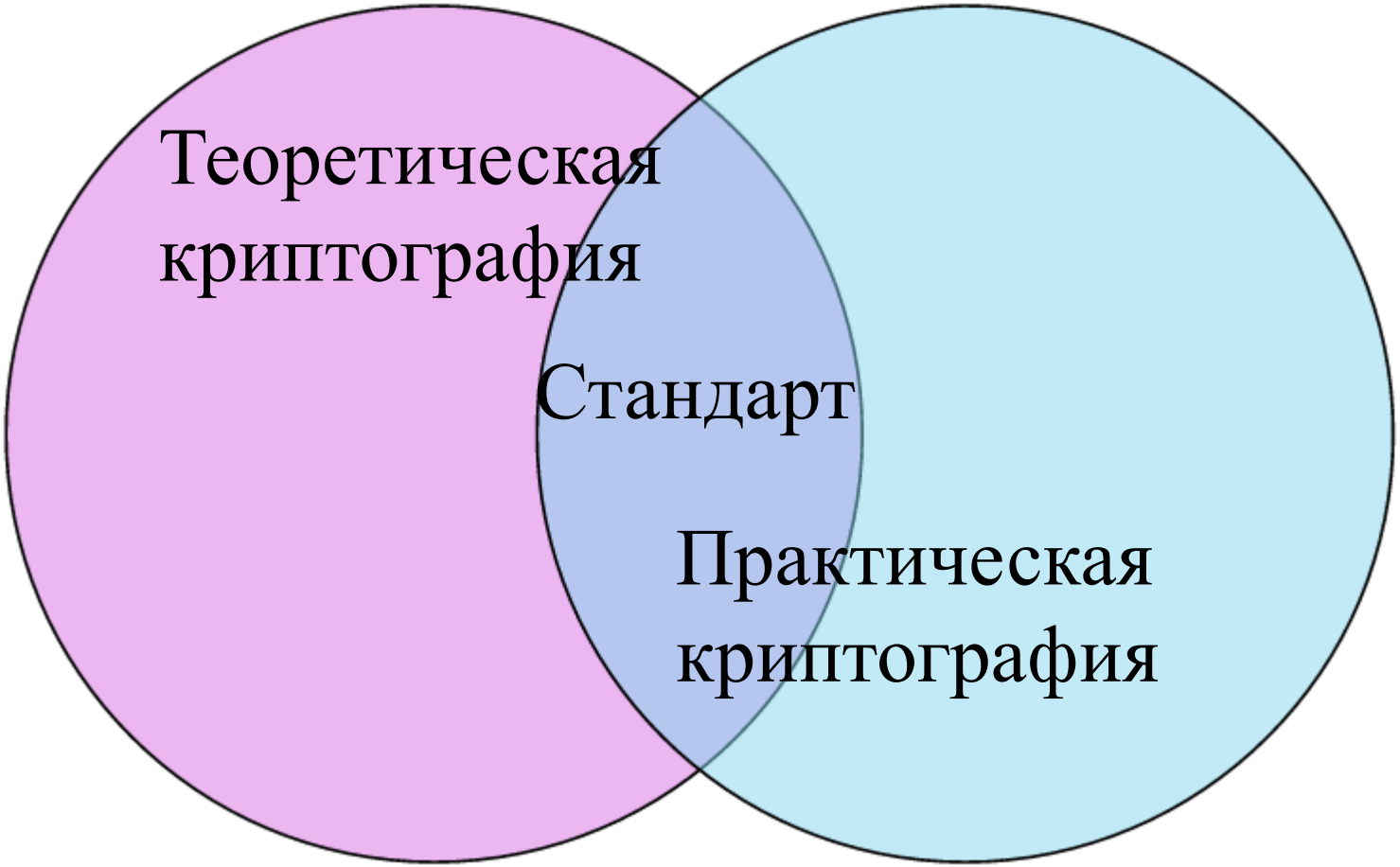
О некоторых особенностях применения межгосударственных стандартов, национальных стандартов, рекомендаций по стандартизации и технических спецификаций в СКЗИ

Докладчик: Н.С. Тыщенко


Теоретическая
криптография
Практическая
криптография


Теоретическая криптография
Стандарт
Практическая криптография

International Organization for Standardization

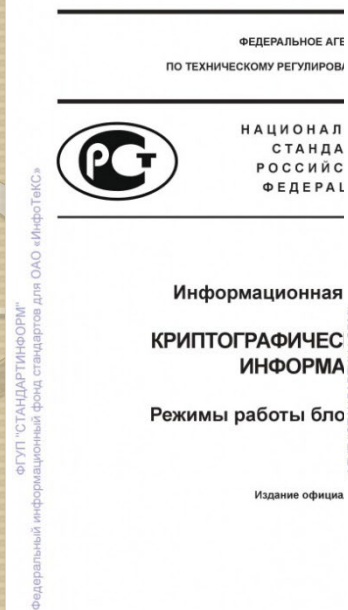
РОССТАНДАРТ

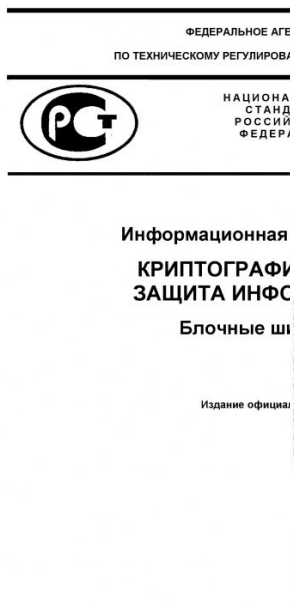
Федеральное агенство по техническому регулированию и метрологии


TK
26

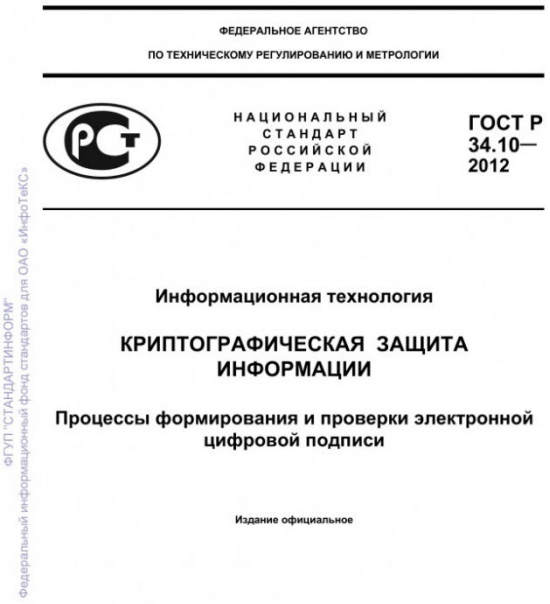
В ТК 26 разрабатывается:

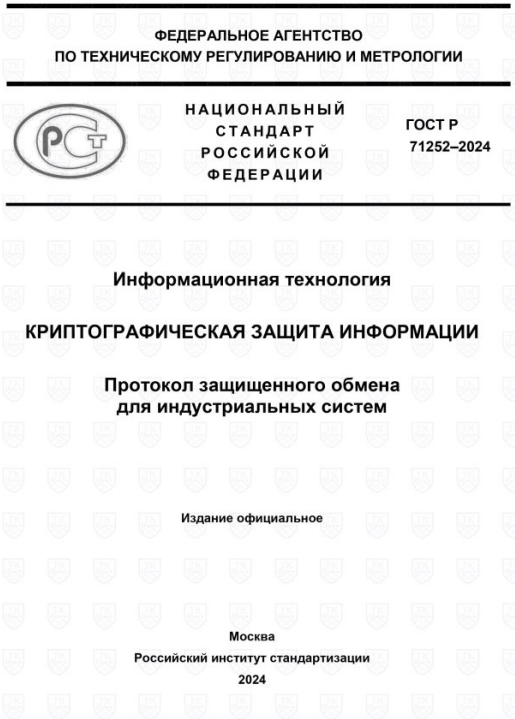
- Технические спецификации
- Методические рекомендации
- Рекомендации по стандартизации национальной системы стандартизации Российской Федерации
- Национальные стандарты Российской Федерации
- Межгосударственные стандарты.

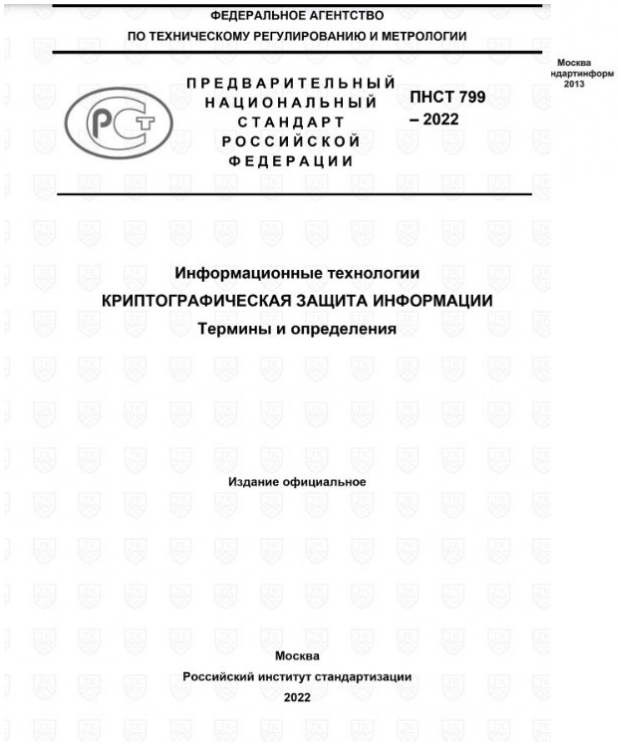

ФЕДЕРАЛЬНОЕ АГЕ
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВА
НАЦИОНАЛ
СТАНДА
РОССИЙС
ФЕДЕРАЦ
Информационная
КРИПТОГРАФИЧЕС
ИНФОРМА
Режимы работы бло
Издание официа
ФГУП "СТАНДАРТИНФОРМ"
Федеральный информационный фонд стандартов для ОАО «ИнфоТеКС»


ФЕДЕРАЛЬНОЕ АГЕ
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВА
НАЦИОНА
СТАНД
РОССИЙ
ФЕДЕРА
Информационная
КРИПТОГРАФИ
ЗАЩИТА ИНФО
Блочные ши
Издание официа
ФГУП "СТАНДАРТИНФОРМ"
Федеральный информационный фонд стандартов для ОАО «ИнфоТеКС»


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛО
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ
Информационная технологи
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИН
Функция хэширования
Издание официальное
ФГУП "СТАНДАРТИНФОРМ"
Федеральный информационный фонд стандартов для ОАО «ИнфоТеКС»


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ
ГОСТ Р
34.10—
2012
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА
ИНФОРМАЦИИ
Процессы формирования и проверки электронной
цифровой подписи
Издание официальное
ФГУП "СТАНДАРТИНФОРМ"
Федеральный информационный фонд стандартов для ОАО «ИнфоТеКС»


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ
ГОСТ Р
71252–2024
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Протокол защищенного обмена
для индустриальных систем
Издание официальное
Москва
Российский институт стандартизации
2024


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
Москва
ндартинформ
2013
ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ
ПНСТ 799
– 2022
Информационные технологии
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Термины и определения
Издание официальное
Москва
Российский институт стандартизации
2022

Independent Submission
Request for Comments: 6986
Updates: 5831
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.

August 2013

GOST R 34.11-2012: Hash Function

Abstract

This document is intended to be a source of information about the Russian Federal standard hash function (GOST R 34.11-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). This document updates RFC 5831.

Independent Submission
Request for Comments: 7091
Updates: 5832
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.

December 2013

GOST R 34.10-2012: Digital Signature Algorithm

Abstract

This document provides information about the Russian Federal standard for digital signatures (GOST R 34.10-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document provides information for developers and users of GOST R 34.10-2012 regarding digital signature generation and verification. This document updates RFC 5832.

Independent Submission
Request for Comments: 7801
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Research Computer Center MSU

March 2016

GOST R 34.12-2015: Block Cipher "Kuznyechik"

Abstract

This document is intended to be a source of information about the Russian Federal standard GOST R 34.12-2015 describing the block cipher with a block length of n=128 bits and a key length of k=256 bits, which is also referred to as "Kuznyechik". This algorithm is one of the set of Russian cryptographic standard algorithms (called GOST algorithms).

Independent Submission
Request for Comments: 8891
Updates: 5830
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
JSC "NPK Kryptonite"
D. Baryshkov
Auriga, Inc.

September 2020

GOST R 34.12-2015: Block Cipher "Magma"

Abstract

In addition to a new cipher with a block length of n=128 bits (referred to as "Kuznyechik" and described in RFC 7801), Russian Federal standard GOST R 34.12-2015 includes an updated version of the block cipher with a block length of n=64 bits and key length of k=256 bits, which is also referred to as "Magma". The algorithm is an updated version of an older block cipher with a block length of n=64 bits described in GOST 28147-89 (RFC 5830). This document is intended to be a source of information about the updated version of the 64-bit cipher. It may facilitate the use of the block cipher in Internet applications by providing information for developers and users of the GOST 64-bit cipher with the revised version of the cipher for encryption and decryption.

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО МЕТРОЛОГИИ, СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND SERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.10–2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО МЕТРОЛОГИИ, СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND SERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.11–2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО МЕТРОЛОГИИ, СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND SERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.12–2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО МЕТРОЛОГИИ, СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND SERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.13–2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное

Москва
Стандартинформ
2018

09.08.2023

МКС 35.040

Изменение № 1 ГОСТ 34.13–2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Принято Межгосударственным советом по стандартизации, метрологии и сертификации (протокол № от)

За принятие изменения проголосовали национальные органы по стандартизации следующих государств: AM, KG, RU, TJ, UZ [коды альфа-2 по МК (ИСО 3166) 004]

Дату введения в действие настоящего изменения устанавливают указанные национальные органы по стандартизации

Предисловие. Пункт 1 дополнить словами: «и Общества с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)».

Пункт 5 изложить в новой редакции:

«5 Настоящий стандарт подготовлен на основе применения ГОСТ Р 34.13–2015, Р 1323565.1.017–2018, Р 1323565.1.026–2019».

Содержание дополнить словами:

«4.4 Процедура преобразования ключа»;

«5.7 Режим гаммирования с преобразованием ключа

5.8 Режим аутентифицированного шифрования с ассоциированными данными».

Подраздел 2.1 дополнить пунктами 2.1.20, 2.1.21, 2.1.22:

«2.1.20 **ассоциированные данные** (associated data): Данные, для которых обеспечивается целостность, но не обеспечивается конфиденциальность.

2.1.21 **зашифрование с выработкой имитовставки** (authenticated encryption): Операция, состоящая из зашифрования открытого текста и вычисления имитовставки от открытого текста и ассоциированных данных, с использованием одного ключа в обоих преобразованиях.

2.1.22 **расшифрование с проверкой имитовставки** (authenticated decryption): Операция, обратная к зашифрованию с выработкой имитовставки, состоящая из проверки имитовставки и последующего расшифрования шифртекста в случае успешного завершения проверки».

Подраздел 2.2 дополнить обозначениями:

« $\sum_{i=1}^{m} a_i$ – битовая строка, являющаяся результатом покомпонентного сложения по модулю 2 битовых строк

ФГБУ «РСТ» В НАБОР №7

Н.Н.Кузьмина
05.09.2023 г.

В ТК 26 разработано около 50 рекомендаций по стандартизации:

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	Р 1323565.1.023-202
Р 1323565.1.041-2022	Р 1323565.1.040-2022	Р 1323565.1.043-2022	Р 1323565.1.044-2022
Р 1323565.1.042-2022	Р 1323565.1.048-2023	Р 1323565.1.046-2023	Р 1323565.1.059-2024
	Р 1323565.1.003-2024	Р 1323565.1.060-2024	Р 1323565.1.061-2024

- Указ Президента Российской Федерации от 03.04.1995 г. **№ 334** «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»
- Федеральный закон от 27.07.2006 г. **№ 152-ФЗ** «О персональных данных»
- Федеральный закон от 06.04.2011 г. **№ 63-ФЗ** «Об электронной подписи»
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации **(Положение ПКЗ-2005)»** – приложение к Приказу ФСБ России от 09.02.2025 № 66
- Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации (**Р 1323565.1.012-2017**)

Стандартами стоит пользоваться

Стандартами не стоит пользоваться необдуманно

ГОСТ Р 34.13-2015

В некоторых режимах должна использоваться **уникальная** синхропосылка, а в некоторых **случайная**

Не рекомендуется использовать ключ режима выработки имитовставки в других криптографических алгоритмах и режимах

ProtoQa (Р 1323565.1.046–2023)

Ограничения и условия (объем материала)

- Для обеспечения защиты от навязывания ложных сообщений разработчику необходимо ограничить максимальное количество обрабатываемых сообщений с неправильной имитовставкой в рамках использования одного ключа. Максимальное количество определяется разработчиком с учетом класса защиты конкретных СКЗИ, реализующих протокол Протока, и с учетом эксплуатационных характеристик конечной системы, в которой предполагается использовать указанные СКЗИ;
- Максимальный объем материала, который может быть обработан на одном ключе, должен определяться с учетом теоретических ограничений, возникающих при использовании конкретных криптографических алгоритмов, и практических ограничений, возникающих при реализации настоящего протокола. Теоретические ограничения на объем материала, который может быть обработан на одном ключе при использовании некоторых вариантов режимов работы блочных шифров согласно ГОСТ 34.13-2018, приведены в Р 1323565.1.005-2017. Практические ограничения на объем материала, который может быть обработан на одном ключе, должны быть получены в рамках тематических исследований конкретных СКЗИ, реализующих описанный протокол, при оценке соответствия данных СКЗИ требованиям по безопасности информации, предъявляемых к СКЗИ, в соответствии с Р 1323565.1.012-2017

ProtoQa (Р 1323565.1.046–2023)

Ограничения и условия (объем материала)

- …разработчику необходимо **ограничить максимальное количество обрабатываемых сообщений с неправильной имитовставкой** в рамках использования одного ключа….;
- …. **теоретические ограничения** на объем материала, который может быть обработан на одном ключе при использовании некоторых вариантов режимов работы блочных шифров согласно ГОСТ 34.13-2018, приведены в Р 1323565.1.005-2017…
- …практические ограничения на объем материала, который может быть обработан на одном ключе, должны быть получены в рамках **тематических исследований конкретных СКЗИ…**

TLS 1.2 (P 1323565.1.020-2020)
TLS 1.3 (P 1323565.1.030-2020)
Вопросы реализации и безопасности

Механизм защиты от побочных каналов

$$TLSTREE(K_{root}, i) = Divers_3\,(Divers_2\,(Divers_1(Kroot, STR8\,(i\&C1)), STR8\,(i\&C2)), STR8\,(i\&C3))$$

В случае, когда $seqnum\ \&\ C_j \neq (seqnum - 1)\ \&\ C_j$. **не вызывать** подфункции $Divers_j$, $j \in \{1,2,3\}$ при использовании TLSTREE

TLS 1.2 (Р 1323565.1.020-2020)
TLS 1.3 (Р 1323565.1.030-2020)
Вопросы реализации и безопасности

Механизм защиты от downgrade-атаки

Рекомендуется в поле random помимо случайного числа последними 8 байт устанавливать специальные значения:

при выборе протокола TLS 1.2: 44 4F 57 4E 47 52 44 01;

при выборе протокола TLS 1.1 или ниже: 44 4F 57 4E 47 52 44 00

TLS 1.3 (Р 1323565.1.030-2020)

ПРИЛОЖЕНИЕ А

Приоритет использования криптонаборов:

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

ИТОГ

Стандарт это **хорошо**,
Стандарт это **надежно**,
Но его нужно реализовать правильно

Спасибо за внимание!