

Приложение
к приказу Федерального
агентства по техническому
регулированию и метрологии
от «1» июля 2022 г. № 1611

**Перечень
документов национальной системы стандартизации,
закрепленных за техническим комитетом по стандартизации
«Криптографическая защита информации» (ТК 026)**

№ п/п	Обозначение стандарта	Наименование стандарта
1	ГОСТ 34.10-2018	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
2	ГОСТ 34.11-2018	Информационная технология. Криптографическая защита информации. Функция хэширования
3	ГОСТ 34.12-2018	Информационная технология. Криптографическая защита информации. Блочные шифры
4	ГОСТ 34.13-2018	Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров
5	ГОСТ Р 34.10-2012	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
6	ГОСТ Р 34.11-2012	Информационная технология. Криптографическая защита информации. Функция хэширования
7	ГОСТ Р 34.12-2015	Информационная технология. Криптографическая защита информации. Блочные шифры
8	ГОСТ Р 34.13-2015	Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров
9	Р 50.1.110-2016	Информационная технология. Криптографическая защита информации. Контейнер хранения ключей
10	Р 50.1.113-2016	Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

11	Р 50.1.111-2016	Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации
12	Р 50.1.115-2016	Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля
13	Р 50.1.112-2016	Информационная технология. Криптографическая защита информации. Транспортный ключевой контейнер
14	Р 1323565.1.003-2017	Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи
15	Р 1323565.1.004-2017	Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа
16	Р 1323565.1.006-2017	Информационная технология. Криптографическая защита информации. Механизмы выработки псевдослучайных последовательностей
17	Р 1323565.1.012-2017	Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
18	Р 1323565.1.009-2017	Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах
19	Р 1323565.1.007-2017	Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN
20	Р 1323565.1.010-2017	Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения

21	Р 1323565.1.008-2017	Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением
22	Р 1323565.1.011-2017	Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайн-проверке PIN
23	Р 1323565.1.013-2017	Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт
24	Р 1323565.1.015-2018	Информационная технология. Криптографическая защита информации. Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем
25	Р 1323565.1.016-2018	Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре офлайн-аутентификации платежного приложения
26	Р 1323565.1.017-2018	Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования
27	Р 1323565.1.018-2018	Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта
28	Р 1323565.1.019-2018	Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных
29	Р 1323565.1.025-2019	Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами

30	P 1323565.1.026-2019	Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование
31	P 1323565.1.028-2019	Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств
32	P 1323565.1.029-2019	Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для промышленных систем
33	P 1323565.1.030-2020	Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)
34	P 1323565.1.032-2020	Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS
35	P 1323565.1.033-2020	Информационная технология. Криптографическая защита информации. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML
36	P 1323565.1.034-2020	Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня
37	P 1323565.1.020-2020	Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)
38	P 1323565.1.035-2021	Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP