ГОСТ Р 34.10-94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

Information technology.
Cryptographic Data Security.
Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm.

Дата введения 1995-01-01

Предисловие

1. **Разработан** Главным управлением безопасности связи Федерального агентства правительственной связи и информации и Всероссийским научно-исследовательским институтом стандартизации.

Внесен Техническим комитетом по стандартизации ТК 22 “Информационная технология” и Федеральным агентством правительственной связи и информации.

2. **Принят и введен в действие** Постановлением Госстандарта России от 23.05.94 № 154

3.**Введен впервые**

Введение

Расширяющееся применение информационных технологий при создании, обработке, передаче и хранении документов требует в определенных случаях сохранения конфиденциальности их содержания, обеспечения полноты и достоверности.

Одним из эффективных направлений защиты информации является криптография (криптографическая информация), широко применяемая в различных сферах деятельности в государственных и коммерческих структурах.

Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

Настоящий стандарт определяет процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма с применением функции хэширования.

Электронная цифровая подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ).

Область применения

Настоящий стандарт устанавливает процедуры выработки и проверки электронной цифровой подписи (ЭЦП) сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, на базе асимметричного криптографического алгоритма с применением функции хэширования.

едрение системы ЭЦП на базе настоящего стандарта обеспечивает защиту передаваемых бщений от подделки, искажения и однозначно позволяет доказательно подтвердить подпись а, подписавшего сообщение....