

# С 1 апреля действуют новые алгоритмы шифрования

Дата публикации: 31.03.2026 10:00

С 1 апреля ФНС России переходит на использование новых Межгосударственных стандартов криптографической защиты информации – ГОСТ 34.12-2018 и ГОСТ 34.13-2018. Поддержка алгоритмов шифрования по действовавшему ранее ГОСТ 28147-89 будет прекращена.

Новые стандарты безопасности, внедряемые в рамках законодательства об **электронной подписи**, поддерживаются только сертифицированными ФСБ современными программными средствами криптографической защиты информации и аппаратными ключевыми носителями.

Реализация шифрования по ГОСТ 34.12-2018 и ГОСТ 34.13-2018 возможна:

- с использованием аппаратных криптографических механизмов активного ключевого носителя (в случае формирования закрытых ключей в неизвлекаемом виде в формате PKCS#11),

- при помощи только программного средства криптографической защиты информации, в частности КриптоПро CSP 5.0 R2 и выше (в случае использования ключевого носителя в качестве пассивного хранилища ключей, что является менее защищенным сценарием работы с электронной подписью).

Техническая поддержка устаревших версий линейки КриптоПро CSP 4.0 официально прекращена в январе 2026 года.



Реализация шифрования по ГОСТ 34.12-2018 и ГОСТ 34.13-2018 с использованием аппаратных криптографических механизмов активного ключевого носителя и, соответственно, применение неизвлекаемых ключей электронной подписи возможны только при использовании носителей Рутокен ЭЦП версии 3.0 и выше, поддерживающих актуальные стандарты. Если ваш закрытый ключ записан на носитель предыдущего поколения — Рутокен ЭЦП 2.0, он не сможет отвечать новым требованиям безопасности.

Для обеспечения возможности бесперебойной сдачи отчетности в налоговые органы, а также обмена документами с контрагентами необходимо заблаговременно проверить версию КриптоПро CSP, установленную на рабочем компьютере, а также модель вашего USB-токена. Если версия КриптоПро CSP ниже 5.0 – обновите программу. Если вы используете Рутокен ЭЦП 2.0 в режиме неизвлекаемых ключей, необходимо заменить активный ключевой носитель на новый.

---

Поделиться:

