У грудні 2014 року Мінекономрозвитку України наказом № 1493 прийняло як національні європейські та міжнародні нормативні документи, які будуть сприяти гармонізації вимог у сфері розвитку та забезпечення інтероперабельності системи електронного цифрового підпису. Йдеться про найбільш поширені у світі криптографічні алгоритми та протоколи, такі як RSA, DSA, KCDSA, ECDSA, EC KCDSA,EC-GDSA тощо.

Крім того, було прийнято два національних стандарти:

ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» (вводиться в дію 01 липня 2015 року);

ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування»на алгоритм симетричного блокового перетворення та на фукції хешування" (вводиться в дію 01 квітня 2015 року).

Стандарт **ДСТУ 7624:2014** розроблено задля поступової заміни міждержавного стандарту **ДСТУ ГОСТ 28147:2009** (на базі **ГОСТ 28147-89**, який визначає симетричний блочний алгоритм криптографічного перетворення), а **ДСТУ 7564:2014**
– для поступової заміни міждержавного стандарту
ДСТУ ГОСТ 34.311:2009
(визначає функцію хешування та має посилання на
ГОСТ 28147-89
), які не відповідають сучасним вимогам до швидкодії і потенційним викликам щодо криптографічної стійкості.

Стандарт **ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист**

інформації. Алгоритм симетричного блокового перетворення" визначає сучасний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності інформації під час її обробки і встановлює режими його роботи (застосування).

Криптографічні перетворення, що застосовуються в алгоритмі, відповідають сучасним вимогам щодорівня криптографічної стійкості та швидкодії. Алгоритм розроблено з урахуванням існуючих і потенційних загроз, подальшого інтенсивного розвитку інформаційних технологій та необхідності активного використання протягом декількох наступних десятиліть.

Стандарт **ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування"** разом з чинним національним стандартом **ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"**
забезпечать надання в державі безпечних електронних довірчих послуг з використанням засобів криптографічного захисту інформації, у тому числі надійних засобів електронного цифрового підпису, з підтвердженою відповідністю, що відповідає сучасним і перспективним вимогам Європейського Союзу.

Криптографічні алгоритми, що визначаються **ДСТУ 7624:2014** та **ДСТУ 7564:2014**, є гнучкими,підтримують розмір блока та довжину ключа від 128 до 512 бітів, що є унікальним у світі.
ДСТУ 7624:2014
визначає десять різних режимів роботи (застосування), які широко поширені відповідно до міжнародного стандарту
ISO/IEC 10116:2006
. Це спрямовано на забезпечення широкої застосовності
ДСТУ 7624:2014
, у тому числі для захисту інформації, що передається комп'ютерними мережами (Інтернет), прозорого шифрування жорстких дисків та знімних носіїв, електронних документів, ключових даних тощо. Наявність такої кількості режимів роботи надає можливість ефективної реалізації систем, засобів і протоколів криптографічного захисту інформації в інформаційно-телекомунікаційних системах різноманітного призначення.

Алгоритм **ДСТУ 7624:2014** є результатом багаторічної плідної співпраці Державної служби спеціального зв'язку та захисту інформації України та провідних українських

науковців і враховує досвід та результати проведення міжнародних і відкритого національного конкурсів криптографічних алгоритмів. Порівняно з відомим міжнародним стандартом AES **(ISO/IEC 18033-3:2010)**, алгоритм **ДСТУ 7624:2014** забезпечує вищий рівень криптографічної стійкості (із можливістю застосування блока та ключа шифрування включно до 512 бітів) і аналогічну або вищу швидкодію на сучасних і перспективних програмних і програмно-апаратних платформах.

Введення в дію нових національних стандартів **ДСТУ 7624:2014** та **ДСТУ 7564:2014** дозволить суттєво вдосконалити показники ефективності захисту систем, засобів і протоколів криптографічного захисту інформації, що розробляються в Україні, і у деяких випадках зробити їх суттєво кращими ніж наявні та перспективні світові рішення.

В данний час продовжуються роботи з стандартизації вітчизняних криптографічних алгоритмів і протоколів, при чому не обмежується застосування гармонізованих стандартів у сфері захисту конфіденційної інформації, а також зосереджуються зусилля на використанні кращих практик застосування стандартів для захисту інформації.