Байлюк Є.М., асистент,
Покотило О.А., асистент,
Житомирський державний технологічний університет

АНАЛІЗ ТА ПОРІВНЯННЯ АЛГОРИТМУ СИМЕТРИЧНОГО БЛОКОВОГО ПЕРЕТВОРЕННЯ «КАЛИНА» (ДСТУ 7624:2014) З МІЖНАРОДНИМ СТАНДАРТОМ ШИФРУВАННЯ ДАНИХ AES

В наш час роль інформаційних технологій та використання обчислювальної техніки є надзвичайно важливою. У зв'язку з глобальним поширенням комп'ютерних мереж з'явилась проблема надійного обміну інформацією, адже під час обміну, зберігання та обробки вона повинна зберігати усі свої властивості. Користувачі Інтернету та локальних мереж потребують простих і водночас потужних засобів захисту інформації, що здатні зберегти її конфіденційність, цілісність та доступність. Криптографічний захист інформації цілком задовольняє цим вимогам.

Одним з основних алгоритмів симетричного блокового шифрування, що використовуються в Україні, є ДСТУ 7624:2014 ("Калина"). Цей стандарт визначає сучасний алгоритм симетричного блокового перетворення для забезпечення конфіденційності і цілісності інформації при її обробці та встановлює режими його роботи.

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

ДСТУ 7624:2014 визначає десять різних режимів роботи, які широко поширені у відповідності з міжнародним стандартом ISO/IEC 10116:2006. Це спрямовано на забезпечення широкого застосування ДСТУ 7624:2014, в тому числі для захисту інформації, що передається комп'ютерними мережами, прозорого шифрування жорстких дисків і змінних носіїв, електронних документів, ключових даних.

Наявність такої кількості режимів роботи дозволяє ефективно реалізувати системи, засоби та протоколи криптографічного захисту інформації в інформаційно-телекомунікаційних системах різного призначення.

У порівнянні з відомим міжнародним стандартом AES (ISO/IEC 18033-3:2010), алгоритм ДСТУ 7624:2014 забезпечує високий рівень криптографічної стійкості (з можливістю застосування блоку даних і ключа шифрування аж до 512 біт) і аналогічну або більш високу швидкодію на сучасних і перспективних програмних та програмно-апаратних платформах.

Основні відмінності "Калина" від "Rijndael"(AES):

– збільшена кількість циклів шифрування;

– використання додавання за модулем 2^{64} і за модулем 2 для введення ключової інформації (захист від алгебраїчних атак, лінійного та диференціального криптоаналізів, інтерполяційної атаки тощо);

– використання 4 блоків нелінійного перетворення (S-блоків) замість одного (додатковий захист від алгебраїчних атак, поліпшення властивостей розсіювання алгоритму);

– використання випадково сформованих 4-блоків, відібраних критеріями стійкості до диференціального, лінійного криптоаналізів та степені нелінійності булевих функцій;

– принципово нова схема створення підключів (захист від всіх відомих атак на схеми створення підключів);

– досить висока продуктивність;

– високе відновлення сеансового ключа за окремим підключем.

Введення в дію нового національного стандарту ДСТУ 7624:2014 дозволить суттєво удосконалити показники ефективності систем захисту, засобів і протоколів криптографічного захисту інформації, які розробляються в Україні, і в деяких випадках поліпшити їх у порівнянні з існуючими та перспективними світовими практиками.

Використані джерела

1. ДСТУ 7624-2014 (з внесеними змінами в 2015 р.) Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення «Калина».

2. «Быстродействие шифров «Калина» и AES» // [Електронний ресурс]. – Режим доступу до статті: http://cyberleninka.ru/article/n/bystrodeystvie-shifrov-kalina-i-aes

3. «О новом украинском стандарте шифрования» // [Електронний ресурс]. – Режим доступу до статті: http://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863