УДК 003.26

А. А. Єфіменко, Є. М. Байлюк, О. А. Покотило

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМУ СИМЕТРИЧНОГО БЛОКОВОГО ПЕРЕТВОРЕННЯ «КАЛИНА» (ДСТУ 7624:2014) З ІНШИМИ МІЖНАРОДНИМИ СТАНДАРТАМИ ШИФРУВАННЯ ДАНИХ

Статтю присвячено проблемі застосування національних стандартів криптографічного захисту інформації. Розглянуто алгоритм симетричного блокового перетворення «Калина» та проаналізовано його відмінності від інших міжнародних стандартів шифрування даних, що використовуються в Україні. З'ясовано, які функціональні особливості є в кожного зі стандартів шифрування даних. У результаті аналізу встановлено факт зменшення практичного використання вказаних алгоритмів у зв'язку з розробкою нових стандартів із підвищеною криптостійкістю. Описано переваги й недоліки кожного алгоритму із зазначенням їх рівня безпеки та практичного застосування. Спланово подальші кроки удосконалення показників ефективності систем криптографічного захисту, що розробляються в нашій державі.

Ключові слова: *алгоритм шифрування, симетричне блокове перетворення, стандарт шифрування даних, криптографічний захист інформації.*

Постановка проблеми в загальному вигляді. Роль інформаційних технологій та використання обчислювальної техніки є дуже важливими на сьогоднішній день. У зв'язку з глобальним поширенням комп'ютерних мереж актуалізувалася проблема надійного обміну інформацією, адже під час обміну, зберігання та обробки вона повинна зберігати усі свої властивості. Саме тому одним з найважливіших питань є захист інформації в інформаційно-комунікаційних системах. Користувачі глобальних та локальних мереж потребують простих і водночас потужних засобів захисту інформації, що здатні зберегти її конфіденційність, цілісність та доступність. Криптографічний захист цілком відповідає цим вимогам. Сучасні стандарти шифрування розроблені з урахуванням особливостей середовища, у якому вони мають затосовуватися. Звідси постає актуальне питання аналізу використовуваних алгоритмів для визначення найбільш криптостійких або тих, що мають найвищу швидкодію та забезпечують високий рівень безпеки інформаційних систем.

Аналіз останніх досліджень і публікацій показав, що головним завданням криптографічних методів захисту інформації є забезпечення конфіденційності, цілісності та доступності даних, що циркулюють в інформаційно-телекомунікаційних системах. Вивченням загальних питань захисту, у тому числі за допомогою криптографічних методів, займалися І. І. Маракова, А. А. Петров, А. І. Рибак, Ю. С. Ямпольський та інші. Вагомий внесок у висвітлення основних теоретичних понять, завдань і проблем класичної та сучасної криптології зробили М. В. Адаменко, А. П. Алферов, В. М. Богуш, О. В. Вербицький, А. Ю. Зубов, А. В. Бабаш, С. Г. Баричев, С. А. Дориченко, М. А. Молдовян, О. А. Молдовян, А. С. Кузьмин, Р. Є. Сєров, А. В. Черемушкін, Г. П. Шанкін, В. В. Ященко та багато інших [1]. Дослідниками розроблено методологічні та науково-теоретичні основи побудови алгоритмів шифрування, оцінювання їх

ефективності. Постійне розширення кола дослідників та предмета досліджень зумовлює появу нових стандартів шифрування.

Таким чином**, метою статті** є порівняльний аналіз міжнародних алгоритмів шифрування даних та національного стандарту «Калина» із врахуванням переваг і недоліків кожного з них.

Виклад основного матеріалу. На сьогоднішній день в Україні використовуються такі алгоритми симетричного блокового шифрування: ДСТУ ГОСТ 28147:2009, AES (у складі операційних систем загального призначення), RC4 (іноземні реалізації засобів захисту веб-з'єднань відповідно до протоколів SSL/TLS), Triple DES (Національний банк України, іноземні реалізації засобів захисту мережевого трафіка IPsec), ДСТУ 7624:2014 («Калина»).

Для вибору оптимального алгоритму шифрування даних з переліку використовуваних на даний час необхідно здійснити їх порівняльний аналіз з урахуванням усіх переваг та недоліків.

Для здійснення швидкісного симетричного шифрування в Україні використовується стандарт ДСТУ ГОСТ 28147:2009. За показниками криптостійкості він відповідає лише задовільному рівню. Крім того, даний стандарт шифрування поступається перспективним шифрам за швидкодією вдвічі або більше. ДСТУ ГОСТ 28147:2009 використовується лише на регіональному рівні. Більшість держав практично відмовилися від його застосування.

Перевагами стандарту ДСТУ ГОСТ 28147:2009 є: загальна відомість шифру, оскільки він був добре досліджений міжнародною спільнотою протягом більше ніж 20 років; прийнятний рівень швидкодії (32-бітові платформи), достатньо зручний для апаратної реалізації, зокрема для малоресурсної (lightweight) криптографії; вузли заміни (S-блоки) з хорошими властивостями забезпечують практичну стійкість шифру.

Недоліками ДСТУ ГОСТ 28147:2009 є: наявність теоретичних атак зі складністю, значно меншою повного перебору ключів; великі класи слабких ключів; використання вузлів заміни спеціального виду дозволяє зменшити рівень стійкості до реалізації практичних атак (виключно на основі шифр-текстів) із використанням одного персонального комп'ютера; швидкодія на сучасних системах суттєво нижча порівняно з іншими блоковими шифрами [2, 3].

AES (Advanced Encryption Standard, також відомий під назвою Rijndael) – це симетричний алгоритм блочного шифрування, який був прийнятий урядом США як національний стандарт шифрування, оскільки став фіналістом конкурсу. Розмір блоку даних шифрування становить 128 біт, а розмір ключа – 128/192/256 біт. Підтримка AES введена фірмою Intel у сімейство процесорів x86, починаючи з Intel Core i7-980X Extreme Edition, а потім на процесорах Sandy Bridge [4].

Переваги AES: найбільш досліджений у світі криптографічний алгоритм, висвітлений у відкритих публікаціях; забезпечує високу практичну стійкість, включений до набору Suite-B Агентства національної безпеки США, дозволений для захисту інформації з обмеженим доступом уряду США; ефективний для реалізації на 32-бітових платформах; наявність низки апаратних акселераторів (включаючи старші моделі процесорів загального призначення).

Недоліки алгоритму шифрування AES: відомі теоретичні атаки зі складністю, меншою, ніж повний перебір; не може в повній мірі використати можливості 64-бітових платформ; відносна застарілість (розроблений у 1997 році, у конкурсі NIST SHA-3 перевага віддана рішенням із архітектурою, що значно відрізняється від AES); відсутність довіри до іноземних апаратних реалізацій AES (у тому числі набору інструкцій AES-NI процесорів x86 і x86_64) на основі даних Е. Сноудена [5]. Світові лідери IT-індустрії почали поступово відмовляться від AES, наприклад, компанія Google у 2014 році впровадила на заміну алгоритм ChaCha20 для захисту каналів зв'язку мобільних пристроїв на базі операційної системи Android [6].

RC4 (Rivest Cipher 4 або Ron's Code) – потоковий шифр, який широко застосовується в комп'ютерних мережах (наприклад, у протоколах SSL і TLS, алгоритмах забезпечення безпеки бездротових мереж WEP і WPA). Також RC4 використовується в різних системах захисту інформації. Цей алгоритм шифрування даних був розроблений компанією RSA Security. Для його використання необхідно мати ліцензію.

Основними перевагами алгоритму шифрування RC4 є: висока швидкість роботи, змінний розмір ключа.

RC4 досить уразливий, якщо: використовуються не випадкові або пов'язані ключі, один ключовий потік застосовується двічі. Ці фактори, а також спосіб використання можуть зробити криптосистему небезпечною (наприклад, WEP).

Алгоритм шифрування даних RC4 використовується в таких криптосистемах та протоколах: WEP, BitTorrent protocol encryption, Microsoft point-to-point encryption, браузер Opera Mini, протокол SSL (варіативно), протокол SSH (варіативно), протокол RDP, Kerberos (варіативно), SASL mechanism digest-MD5 (варіативно), формат PDF, Skype (in modified form).

Зараз не рекомендується використовувати даний алгоритм шифрування, оскільки було знайдено методи успішної атаки на нього. Тому підтримка RC4 поступово видаляється з різних криптосистем [7, 8].

Triple DES (3DES) – симетричний блоковий шифр, створений у 1978 році Уітфілдом Діффі, Мартіном Хеллманом і Уолтом Тачманом на основі алгоритму шифрування даних DES. Головною метою розробки було усунення основного недоліку алгоритму шифрування DES, а саме малої довжини ключа в 56 біт, що може бути зламаний методом повного перебору. 3DES поступається за швидкістю DES утричі, але за криптостійкістю він набагато кращий. Час, потрібний для криптоаналізу 3DES, може бути в мільярд разів більшим, ніж необхідний для аналізу DES. Саме тому він використовується частіше, ніж алгоритм шифрування DES. Останній можна легко зламати за допомогою сучасних комп'ютерних технологій. У 1998 році організація Electronic Frontier Foundation, використовуючи спеціальний комп'ютер DES Cracker, розкрила DES за 3 дні.

Симетричний алгоритм шифрування даних 3DES реалізований у багатьох програмних додатках, орієнтованих на роботу з Інтернетом, у тому числі в PGP і S/mime. Triple DES є досить достойною і популярною альтернативою шифру DES. Потрійний DES використовується в стандартах ISO 8732, ANSI X9.17, а також у Privacy Enhanced Mail для управління ключами. Індустрія електронних платежів використовує 3DES і продовжує активно розробляти та публікувати стандарти, що ґрунтуються на ньому (наприклад, EMV). Компанія Microsoft для захисту даних системи і користувачів за допомогою

парольного захисту використовує 3DES є, а саме в додатках Microsoft OneNote, Microsoft Outlook 2007 і Microsoft System Center Configuration Manager 2012.

На сьогоднішній день не існує відомих криптографічних атак на 3DES, які можна застосувати на практиці. Але Triple DES потроху виходить з ужитку.

На зміну даному алгоритму прийшов новий – AES Rijndael, який було розглянуто вище. Програмно реалізований алгоритм шифрування даних AES працює в шість разів швидше за 3DES. Саме з цієї причини шифр 3DES більше підходить для апаратних реалізацій. Багато систем безпеки продовжують підтримувати як 3DES, так і AES. Але за замовчуванням у них використовується алгоритм AES. Triple DES може підтримуватися для забезпечення сумісності, проте його більше не рекомендують до використання.

Переваги Triple DES (3DES, TDEA): відомий шифр, який добре досліджений міжнародною спільнотою протягом більше ніж 30 років; забезпечує припустиму практичну стійкість (2112); поширений у банківських системах, імпортованих або орієнтованих на застарілі стандарти.

Недоліки Triple DES: практична стійкість значно нижча теоретичної; наявність класів слабких ключів; швидкодія на сучасних системах суттєво нижча навіть порівняно із ДСТУ ГОСТ 2814:2009 та іншими блоковими шифрами [9].

Одним із основних алгоритмів симетричного блокового шифрування, що використовуються в Україні, є ДСТУ 7624:2014 («Калина»), який визначає сучасний алгоритм симетричного блокового перетворення для забезпечення конфіденційності й цілісності інформації при її обробці та встановлює режими його роботи.

В алгоритмі шифрування даних «Калина» використовуються криптографічні перетворення, які відповідають сучасним вимогам до рівня криптостійкості та швидкодії. Даний стандарт розроблено з урахуванням існуючих та потенційних загроз, подальшого інтенсивного розвитку інформаційних технологій та необхідності активного використання протягом кількох наступних десятиліть.

Стандарт блокового симетричного шифрування ДСТУ 7624:2014 визначає десять різних режимів роботи, що широко поширені відповідно до міжнародних стандартів ISO/IEC 10116:2006. Це спрямовано на забезпечення широкого застосування ДСТУ 7624:2014, у тому числі для захисту інформації, що передається комп'ютерними мережами, прозорого шифрування жорстких дисків і змінних носіїв, електронних документів, ключових даних.

Ефективність реалізації систем, засобів та протоколів криптографічного захисту інформації в інформаційно-телекомунікаційних системах різного призначення може бути забезпечена саме наявністю такої кількості режимів роботи алгоритму.

До блокового шифру «Калина» ставляться такі вимоги: високий рівень криптографічної стійкості з достатнім запасом у разі появи нових атак протягом тривалого часу; висока швидкодія програмної реалізації на сучасних та перспективних платформах; компактність програмної та програмно-апаратної реалізації; можливість ефективної інтеграції декількох алгоритмів в одному засобі криптографічного захисту; прозорість проектування, консервативний підхід до забезпечення стійкості; вища (або однакова) ефективність порівняно з найкращими світовими рішеннями.

Криптографічні алгоритми, які визначаються стандартами ДСТУ 7624:2014 і ДСТУ 7564:2014, є гнучкими, підтримують розмір блоку і довжину ключа від 128 до

512 біт. Стандарт симетричного блокового шифрування «Калина» є результатом багаторічної плідної співпраці Державної служби спеціального зв'язку та захисту інформації України та провідних українських вчених. Даний алгоритм шифрування враховує досвід і результати проведення міжнародних та відкритих національних конкурсів криптографічних алгоритмів.

Алгоритм ДСТУ 7624:2014 забезпечує досить високий рівень криптостікості порівняно з міжнародним стандартом AES (ISO/IEC 18033-3:2010), оскільки дає можливість застосовувати блок даних і ключ шифрування розміром аж до 512 біт. Крім того, він має аналогічну або навіть більш високу швидкодію на сучасних і перспективних програмних та програмно-апаратних платформах.

На даний момент продовжуються роботи зі стандартизації вітчизняних криптографічних алгоритмів та протоколів. При цьому не обмежується застосування гармонізованих стандартів у сфері захисту конфіденційної інформації. Також зусилля зосереджено на використанні кращих практик застосування стандартів шифрування даних для захисту інформації в інформаційно-комунікаційних системах [10, 11].

Оскільки в стандартах симетричного блокового шифрування «Калина» та AES використовуються аналогічні криптографічні перетворення, на наш погляд, буде доцільним порівняти ці два алгоритми.

Основними відмінностями «Калина» від «Rijndael» (AES) є: збільшена кількість циклів шифрування (запас стійкості); використання додавання за модулем 264 і за модулем 2 для введення ключової інформації (захист від алгебричних атак, лінійного та диференціального криптоаналізів, інтерполяційної атаки тощо); використання чотирьох блоків нелінійного перетворення (S-блоків) замість одного (додатковий захист від алгебричних атак, поліпшення властивостей розсіювання алгоритму – покращені статистичні властивості, відповідно, більш високий рівень стійкості до диференціального та лінійного криптоаналізів тощо); використання випадково сформованих чотирьох блоків, відібраних критеріями стійкості до диференціального, лінійного криптоаналізів, ступені нелінійності булевих функцій (на відміну від S-блоку Rijndael/Camellia та інших шифрів, що використовують звернення в полі та, відповідно, квадратичні залежності між входом і виходом, – захист від алгебричних атак); принципово нова схема створення підключів (захист від усіх відомих атак на схеми створення підключів); досить висока продуктивність; можливість відновлення сеансового ключа за окремим підключем (додатковий захист від атак, що виконують відновлення підключів).

Усі поліпшення спрямовані на збільшення стійкості та запобігання потенційним вразливостям відносно Rijndael, виявленим в останні роки [12].

Висновки. Таким чином, у статті розглянуто алгоритм симетричного блокового перетворення «Калина» та проаналізовано його відмінності від інших міжнародних стандартів шифрування даних, що використовуються в Україні. Основними перевагами шифру порівняно з іншими міжнародними аналогами є можливість застосовувати блок даних і ключ шифрування розміром аж до 512 біт, збільшена кількість циклів шифрування та принципово нова схема створення підключів, що забезпечують захист від усіх відомих атак на схеми їх створення. Тому введення в дію нових національних стандартів ДСТУ 7624:2014 і ДСТУ 7564:2014 дозволить суттєво удосконалити показники

ефективності систем захисту, засобів і протоколів криптографічного захисту інформації, які розробляються в Україні, а в деяких випадках поліпшити їх порівняно з існуючими та перспективними світовими практиками.

СПИСОК ЛІТЕРАТУРИ

1. Основи понятійно-термінологічного апарату криптології. URL: https://bit.ly/2N7BZIO (дата звернення: 14.04.2018).
2. ДСТУ ГОСТ 28147:2009 Система обробки інформації. Криптографічний захист. Алгоритм криптографічного перетворення. Київ, 2009. С. 10–15.
3. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. URL: https://www.slideshare.net/oliynykov/kalyna (дата звернення: 19.05.2018).
4. Advanced Encryption Standard. URL: https://uk.wikipedia.org/wikiAdvanced_Encryption_Standard (дата звернення: 20.05.2018).
5. Сноуден пролил свет на ситуацию со взломом криптографии. URL: https://habr.com/post/192722/ (дата звернення: 21.05.2018).
6. Остапов С. Є. , Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : Вид-во ХНЕУ, 2013. 476 с.
7. Самойлов С. А., Зуєв М. С. Шифрование данных. Алгоритм RC4. URL: https://cyberleninka.ru/article/v/shifrovanie-dannyh-algoritm-rc4 (дата звернення: 05.05.2018).
8. RC4. URL: https://uk.wikipedia.org/wiki/RC4 (дата звернення: 04.06.2018).
9. Triple DES. URL: https://ru.wikipedia.org/wiki/Triple_DES (дата звернення: 04.06.2018).
10. ДСТУ 7624-2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення «Калина (з внесеними змінами в 2015 р.)». Київ, 2014. С. 20–23.
11. О новом украинском стандарте шифрования. URL: http://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863 (дата звернення: 20.05.2018).
12. Быстродействие шифров «Калина» и AES. URL: http://cyberleninka.ru/article/bystrodeystvie-shifrov-kalina-i-aes (дата звернення: 05.05.2018).

Подано 23.07.2018

А. А. Ефименко, Е. М. Байлюк, А. А. Покотило

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМА СИММЕТРИЧНОГО БЛОЧНОГО ПРЕОБРАЗОВАНИЯ «КАЛИНА» (ДСТУ 7624:2014) С ДРУГИМИ МЕЖДУНАРОДНЫМ СТАНДАРТАМ ШИФРОВАНИЯ ДАННЫХ

Статья посвящена проблеме применения национальных стандартов криптографической защиты информации. Рассмотрен алгоритм симметричного блочного преобразования «Калина» и проанализированы его отличия от других международных стандартов шифрования данных, используемых в Украине. Выяснено, какие функциональные особенности есть у каждого из стандартов шифрования данных. В результате анализа установлен факт уменьшения практического использования указанных алгоритмов в связи с разработкой новых стандартов повышенной криптостойкости. Описаны преимущества и недостатки каждого метода с указанием

их уровня безопасности и практического применения. Запланированы дальнейшие шаги совершенствования показателей эффективности систем криптографической защиты, которые разрабатываются в нашем государстве.

Ключевые слова: *алгоритм шифрования, симметричное блочное преобразование, стандарт шифрования данных, криптографическая защита информации.*

A. A. Yefimenko, Y. M. Bailiuk, O. A. Pokotylo

COMPARATIVE ANALYSIS OF THE "KALINA" SYMMETRIC BLOCK CONVERGENCE ALGORITHM (DSTU 7624:2014) WITH OTHER INTERNATIONAL DATA SHEET STANDARDS

The article is devoted to the problem of the application of national cryptographic information security standards. The algorithm of the symmetric block conversion "Kalina" is considered and its differences from other international data encryption standards used in Ukraine are analyzed. It is determined which functional features are in each of the data encryption standards. As a result of the analysis, the fact of reducing the practical use of these algorithms in connection with the development of new standards with increased cryptantability is established. The advantages and disadvantages of each algorithm with their level of safety and practical application are described. Further steps are planned to improve the performance of cryptographic protection systems developed in Ukraine.

Keywords: *encryption algorithm, symmetric block transformation, data encryption standard, cryptographic information protection.*