мальне число фрагментів, а за кращим шляхом – їх максимальна кількість.

Ключові слова: безпечна маршрутизація, MANET, ймовірність компрометації, балансування числа фрагментів, маршрут.

MODEL IMPROVEMENT OF MESSAGE SECURE ROUTING WITH OPTIMAL BALANCING ITS FRAGMENTS NUMBER TRANSMITTED OVER NON OVERLAPPING PATHS

The given work is devoted to improvement and investigation of secure routing model with optimal balancing of message fragments number in mobile self-organizing networks. Within the work it was explored the concept of threshold secret sharing scheme in relation to secure routing using non overlapping paths for the message frag-ments transmission. Based on analysis of disadvantages of existing mechanism SPREAD it was proposed the im-provement of fragments allocation model which had been reduced to the optimal balancing of message fragments number transmitted over the non overlapping paths. It was proposed several optimality criterions related to the so-lution of balancing problem. In a comparative analysis it is justified to use on practice optimality criterion, providing on the one hand minimizing dynamically managed upper bound number of fragments transmitted over separate non overlapping paths in the network, and from the other hand – to adapt to security parameters (probability of compromise) of individual network elements: nodes, links and paths. Numerical examples of models with different optimality criterion of the solutions obtained, and their comparative analysis represented. The comparison results confirmed the effectiveness of the proposed model, when by the worst path in terms of the probability of com-promise transmitted the minimum number of fragments, and by the best path – their maximum number.

Index terms: secure routing, MANET, probability of compromise, number of fragments balancing, path.

Лемешко Олександр Віталійович, доктор технічних наук, професор, професор кафедри телекомунікаційних систем Харківського національного університету радіоелектроніки.
E-mail: avlem@ukr.net.

Лемешко Александр Витальевич, доктор технических наук, профессор, профессор кафедры телекоммуникационных систем Харьковского национального универ-ситета радиоэлектроники.

Lemeshko Olexandr, Doctor of Science, Professor, Professor of Telecommunication Systems Department, Kharkiv National Uni-versity of Radio Electronics.

Єременко Олександра Сергіївна, кандидат технычних наук, старший науковий співробатний, доцент кафедри телекомунікаційних систем Харківського національного університету радіое-лектроніки.
E-mail: alexere@ukr.net.

Еременко Александра Сергеевна, кандидат технических наук, старший научный сотрудник, доцент кафедры телекоммуникационных систем Харьковского национального университета радиоэлектроники.

Yeremenko Oleksandra, PhD, Senior Researcher, Associate Professor of Telecommunication Systems Department, Kharkiv National University of Radio Electronics.

УДК 681.3.06:006.354

ПРИНЦИПИ ПОБУДОВИ І ОСНОВНІ ВЛАСТИВОСТІ НОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ БЛОКОВОГО ШИФРУВАННЯ УКРАЇНИ

Роман Олійников, Іван Горбенко, Олександр Казимиров, Віктор Руженцев, Юрій Горбенко

З 1-го липня 2015 р. в Україні вводиться в дію криптографічний стандарт блокового симетричного перетворення ДСТУ 7624:2014 [3], що визначає шифр "Калина" та режими його роботи для забезпечення конфіденційності і цілісності. Національний стандарт розроблений у співпраці Державної служби спеціального зв'язку та захисту інформації України і провідних українських науковців на основі проведення відкритого конкурсу криптографічних алгоритмів. Порівняно із відомим міжнародним стандартом AES, алгоритм ДСТУ 7624:2014 забезпечує вищий рівень криптографічної стійкості (із можливістю застосування блока та ключа шифрування включно до 512 бітів) і порівняну або вищу швидкодію на сучасних і перспективних програмних і програмно-апаратних платформах, суттєво

перевершуючи показники ДСТУ ГОСТ 28147:2009 (ГОСТ 28147-89), який застосовується вже більше 25 років. У статті розглянуті сучасні проблеми розробки блокових шифрів та їхні вирішення, впроваджені розробниками у новому національному стандарті України.

Ключові слова: *ДСТУ 7624:2014, блоковий шифр, криптоаналіз, швидкодія шифрування, національний стандарт.*

ВСТУП. Блокові шифри є одним із найбільш розповсюджених криптографічних примітивів. Крім забезпечення конфіденційності, вони використовуються як конструктивний елемент в ході побудови функцій гешування, кодів автентифікації повідомлення тощо. Значення цього примітива додатково підкреслює проведення низки міжнародних криптографічних конкурсів [13, 28, 22], які були орієнтовані на розробку блокового шифру (як основної мети або у складі набору перспективних перетворень).

З практичної точки зору, у сучасних інформаційно-комунікаційних системах основний потік інформації, що передається відкритими каналами зв'язку, захищається за допомогою саме симетричних перетворень із залученням блокового шифру. Засоби криптографічного захисту інформації (КЗІ), які існують зараз, у ряді випадків не можуть забезпечити рівень пропускної здатності, який повністю відповідає актуальним вимогам. Ця проблема може бути вирішена за допомогою декількох підходів. Крім екстенсивного, який передбачає масштабування систем КЗІ з їх ускладненням за рахунок додаткових модулів балансування навантаження, збільшення вартості та зниження надійності, існує підхід, який передбачає вдосконалення алгоритмів криптографічного перетворення, зниження їхньої обчислювальної складності при збереженні або збільшенні стійкості.

Блоковий шифр, визначений ДСТУ ГОСТ 28147:2009 (ГОСТ 28147-89 [1]) був введений в дію 25 років тому. Хоча він все ще забезпечує практичну стійкість, тим не менш, для цього алгоритму відомі ефективні методи криптоаналізу, які мають складність значно меншу, ніж переборні атаки. Цей стандарт вже виведений із дії в Білорусії [10] та планується до модифікації у РФ у 2015 р. (у якості основного застосовується новий 128-бітовий шифр [9]). З точки зору швидкодії, на сучасних обчислювальних архітектурах загального призначення ДСТУ ГОСТ 28147:2009 суттєво поступається іноземними аналогам (наприклад, AES [12]), що призводить до ускладнення та подорожчання засобів КЗІ при однакових інших характеристиках.

Водночас, заміна ДСТУ ГОСТ 28147:2009 на міжнародний стандарт AES не є вирішенням цієї проблеми для України, бо світові тенденції вже свідчать про поступову відмову від AES: у конкурсі SHA3 [18] перевага віддана рішенням із архітектурою, що значно відрізняється від AES. Деякі компанії, лідери IT-індустрії, застосовують власні рішення щодо заміни цього алгоритму для шифрування в протоколі TLS: наприклад, компанія Google у 2014 році впровадила алгоритм ChaCha20 [17] для захисту каналів зв'язку мобільних пристроїв з операційною системою Android. Відповідно, введення в Україні в дію AES у якості національного стандарту свідчило б про використання рішення, від якого вже почали поступово відмовлятися світові лідери IT-індустрії.

Таким чином, в Україні існувала суттєва проблема розробки та введення в дію нового сучасного стандарту шифрування, який дозволить створення ефективних засобів КЗІ наступних поколінь.

Враховуючи позитивний світовий досвід криптографічних конкурсів AES, NESSIE, CRYPTREC [13, 28, 22], який був додатково підтверджений в ході пізніше проведеного SHA3 [18], Державна служба спеціального зв'язку та захисту інформації України успішно провела національний відкритий конкурс симетричних блокових криптографічних алгоритмів [2] у 2007-2010 рр., у результаті якого [30] був відзначений алгоритм «Калина», на базі якого і був розроблений національний стандарт.

Перед розробниками постала складна та суперечна задача.

З одного боку, новий стандарт криптографічного перетворення повинний забезпечувати високий рівень стійкості із необхідним запасом для застосування протягом декількох десятків років.

З іншого боку, однією з найважливіших характеристик криптографічного перетворення є швидкодія, і порівняння нового стандарту буде здійснюватися не тільки із застарілим ДСТУ ГОСТ 28147:2009, але й з широко поширеним AES (стандарт США FIPS-197 [12], введений в дію в 2002 р., також включений у міжнародний стандарт ISO/IEC 18033-3:2010 [23]), в якому вже досягнута низка екстремальних показників щодо швидкодії, а деякі компромісні рішення призвели до появи деяких теоретичних атак. Таким чином, новий стандарт повинен забезпечувати швидкодію, суттєво вищу за ДСТУ ГОСТ 28147:2009 і порівняну з AES, водночас, мати вдосконалений рівень стійкості відносно AES і ГОСТ.

Додатково завдання ускладнюється відсутністю в Україні ресурсів, які є в наявності у країнах із великими криптологічними службами, – наприклад, Агенція національної безпеки США налічує десятки тисяч висококваліфікованих математиків-криптографів та застосовує найпотужніші в світі спеціалізовані центри обробки даних [27].

Таким чином, розробка нового національного стандарту України вимагала вирішення складної задачі побудови швидкого криптографічного перетворення, яке водночас забезпечує високий і надвисокий рівень стійкості, в умовах обмеження часових, дослідницьких і обчислювальних ресурсів.

СУЧАСНІ ТЕНДЕНЦІЇ ТА ВІДКРИТІ ПИТАННЯ ЩОДО РОЗРОБКИ АЛГОРИТМІВ ШИФРУВАННЯ. При розробці нового перетворення постають питання вибору і обґрунтування низки рішень щодо нового криптографічного алгоритму.

Розмір блоку і довжина ключа визначають зовнішні параметри алгоритму та його галузь використання (за умови забезпечення внутрішніх компонентів стійкості до відповідних видів атак).

Довжина ключа повинна забезпечувати практичне унеможливлення здійснення перебірних атак та методів аналізу, що засновані на таблицях передобчислень, із суттєвим запасом стійкості.

Розмір блоку впливає на колізійні властивості перетворення, що, в свою чергу, визначає рівень стійкості більшості режимів роботи блокового шифру, спрямованих як на забезпечення конфіденційності, так і цілісності й інші застосування (генерація псевдовипадкових послідовностей, побудова функції ґешування та ін.).

Саме ці параметри криптографічного перетворення визначають граничні показники стійкості і формують загальні критерії, яким повинні відповідати внутрішні компоненти (нижня границя складності аналітичних атак).

Криптографічний примітив повинний реалізовувати властивості випадкового відображення, а за умови фіксації ключа шифрування моделлю ідеального ендоморфного шифру є випадкова перестановка відповідного ступеня.

Вимоги випадковості (псевдовипадковості) необхідні для приховування надмірності вхідних даних, коли нерівноймовірність вхідних символів або їхніх груп перетворюється в нерівноймовірність послідовностей значно більшої довжини, що експоненційно збільшує кількість ресурсів, потрібних для криптоаналізу. Ці вимоги формалізовані через модель на основі простору з мірою ще в [11]. Однак пряма реалізація підстановки вимагає недосяжних на практиці обсягів пам'яті (наприклад, 64-бітовий шифр для одного ключа потребує 2^{27} ТБ [8]), що призводить до необхідності застосування ітеративних перетворень.

В свою чергу, для такого типу шифрів потрібно задати високорівневу конструкцію. На поточний момент, розповсюджені перетворення використовують ланцюг Фейстеля, SPN-структуру, схему Лей-Мессі або їхні модифікації. Водночас, вибір високорівневої конструкції шифру здійснюється на основі переваг розробника і у більшості випадків не має теоретичного обґрунтування із чисельними оцінками ефективності.

Для ефективної реалізації властивостей розсіювання та перемішування [11] у циклової функції, що застосовується високорівневою конструкцією, на сучасних програмно-апаратних платформах потрібно застосування шарів лінійного та нелінійного відображень. Слід відзначити, що при реалізації вони можуть бути виконані у вигляді єдиної таблиці підстановки, але при криптографічному аналізі властивостей виділяють два послідовних перетворення.

Нелінійне перетворення може бути реалізоване на основі двох підходів:

- набір логічних або арифметичних функцій (на основі команд процесорів деякої архітектурі або відповідного набору логічних функцій при апаратної релізації);
- табличного перетворення із розміром, припустимим для програмної і апаратної реалізації.

Перший підхід реалізований в алгоритмах SIMON і SPECK [16], блокових шифрах, на основі яких побудовано сімейство ґеш-функцій SHA-0,1,2 і інших перетвореннях. Такі методи побудови дозволяють отримати високошвидку і компактну реалізацію. Але навіть із найпотужнішими можливостями для аналізу стійкості в світі, США були повинні декілька разів змінювати свої стандарти ґешування із-за знайдених вразливостей: з 1993 до 1995 діяла SHA-0, з 1995 по 2001 діяла SHA-1, з того часу використовується SHA-2. Крім того, з 2008 до 2012 р. був проведений відкритий конкурс на розробку нової функції ґешування SHA-3 [18], і розробники засобів криптографічного захисту США можуть обирати між стандартами ґешування SHA-2 і SHA-3.

Другий підхід передбачає формування таблиць підстановок (S-блоків) із заданими властивостями. Він використаний у більшості поширених блокових шифрів, в т.ч. AES, DES (TripleDES [21]), ГОСТ 28147-89, нових стандартах шифрування РФ [9] і Білорусії [10]. Перевагою

підходу є можливість суворого обґрунтування криптографічних властивостей і стійкості до відомих атак, але реалізація вимагає більш значних ресурсів і, як правило, поступається швидкодією порівняно із застосуванням виключно логічних або арифметичних функцій.

Лінійне перетворення, як правило, реалізується на основі транспозиції (перестановки) або лінійної комбінації елементів. Транспозиція застосовується в ГОСТ 28147-89 і СТБ 34.101.31-2011 (циклічний зсув), DES і PRESENT (бітова перестановка) та інших шифрах. Сучасні шифри, які не мають обмежень відповідно до малоресурсної (lightweitght) криптографії використовують лінійну комбінацію вхідних значень, як правило, МДВ-перетворення (частковий випадок мультиперестановки [34]), що гарантує властивості поширення впливу вхідних значень на вихідні.

Крім основного перетворення, що шифрує, блоковий шифр вимагає наявності схеми формування циклових ключів, які генеруються на основі ключа шифрування і використовуються на кожній ітерації. Цей компонент криптографічного перетворення визначає складність реалізації атак «зустріч посередині» (meet-in-the-middle) і деяких інших методів аналізу, і є приклади, коли слабка схема дозволяла реалізовувати навіть практичні атаки на поширені шифри, що забезпечують високий рівень стійкості до всіх інших відомих методів криптоаналізу [32]. Крім того, вразливі схеми у низці випадків дозволяють реалізацію атак на основі зв'язаних ключів (related keys), що ставить під загрози інші криптографічні примітиви, що побудовані на їх основі (наприклад, геш-функцію на основі конструкції Девіса-Мейера [26]).

Зараз існує декілька різних підходів до побудови схем формування циклових ключів. Найпростіші передбачають мінімальні додаткові обчислення і реалізують транспозицію або лінійну комбінацію бітів ключа шифрування для отримання значень циклових ключів. Такий підхід реалізований, наприклад, в ГОСТ 28147-89 і DES. Перевагою є простота і низка обчислювальна складність реалізації, недоліком, як вже зазначено, потенційна можливість реалізації криптоаналітичних атак, які вимагають дуже специфічних умов, але в цих рамках є дуже ефективними. Інший підхід передбачає використання окремого нелінійного перетворення, що забезпечує високу стійкість і до зазначених атак, але при цьому обчислювальна складність формування циклових ключів (key agility) може перевищувати зашифрування навіть десяти блоків відкритого тексту. Додатково слід відзначити нелінійні складнозворотні схеми (Twofish [33], FOX [24]), що не забезпечують властивість ін'єктивності і теоретично допускають існування еквівалентних ключів. Тим не менш, така конструкція частково забезпечує і захист від атак на реалізацію, що неможливо із ін'єктивною схемою.

Таким чином, при розробці схеми формування циклових ключів також потрібне вирішення задачі пошуку оптимального рішення при обмеженнях щодо криптографічної стійкості, гнучності, швидкості і компактності цього додаткового перетворення.

Крім зазначених питань, у окремий напрямок виділяють т.з. малоресурсну (lightweight) криптографію, яка передбачає компактну апаратну реалізацію і мінімальне енергоспоживання, забезпечуючи припустимий рівень криптографічної стійкості. Водночас, в умовах відсутності в Україні власного мікроелектронного виробництва і неможливості надійного контролю іноземного, цей напрямок зараз є другорядним для України і не розглядався в рамках розробки нового стандарту.

КОНСТРУКТИВНІ РІШЕННЯ, ОБРАНІ ПРИ РОЗРОБЦІ ПЕРСПЕКТИВНОГО БЛОКОВОГО ШИФРУ. Як вже було відзначено вище, новий алгоритм повинен забезпечувати швидкодію, порівняну з AES, водночас, мати вдосконалений рівень стійкості відносно AES. Завдання додатково було ускладнено обмеженням кількості дослідницьких та обчислювальних ресурсів, що можна задіяти для розробки нового національного стандарту України і обґрунтуванню його криптографічної стійкості. Відповідно, при розробці було вирішено забезпечити прозорість проектування і використовувати консервативний підхід із залученням відомих і добре досліджених конструкцій, а також наявність достатнього запасу стійкості для безпечного використання алгоритму в умовах значного прогресу криптоаналітичних технік та засобів обробки даних.

Нове криптографічне перетворення повинно відповідати наступним загальним вимогам [8]:

1. Високий рівень криптографічної стійкості (складність відомих криптоаналітичних атак має бути вище складності атак переборного типу, які, в свою чергу, є нездійсненними на практиці з врахуванням перспектив розвитку масових напівпровідникових технологій).

2. Швидкодія нового криптографічного перетворення має бути вищою, ніж у чинного алгоритму та порівняна із найкращими міжнародни-

ми стандартами, на сучасних і перспективних програмних платформах.

3. Проста програмна і програмно-апаратна реалізація.

Вибір базових зовнішніх параметрів шифру був здійснений на основі аналізу можливостей сучасних переборних атак із застосуванням таблиць передобчислень [8, 6, 29, 15, 25], а також колізійних властивостей із критерієм, що такі методи не можуть бути практично здійснені із використанням сучасних та перспективних напівпроводникових технологій, з наявністю запасу стійкості.

Крім того, була забезпечена гнучкість вибору таких параметрів для розробників систем КЗІ, що дозволяє досягнення як найвищого рівня швидкодії, так і найбільшого запасу стійкості перетворення.

Новий національний стандарт шифрування підтримує наступні комбінації довжини ключа і розміру блоку (табл. 1), забезпечуючи високий та надвисокий рівень криптографічної стійкості.

Таблиця 1

Комбінації довжини ключа і розміру блоку шифру «Калина»

Розмір блоку	Довжина ключа
128	128, 256
256	256, 512
512	512

Розмір блока і довжина ключа використовуються і у позначенні шифру як параметр. Наприклад, Калина-128/256 визначає використання алгоритму з розміром блоку 128 бітів, довжиною ключа 256 бітів. Крім того, в позначенні може бути зазначений і режим роботи з додатковими параметрами.

Для вибору високорівневої конструкції був розроблений аналітичний метод порівняння їхньої ефективності [8,5] на основі складності розрізнення випадкової перестановки і блокового шифру, що базується на відповідному перетворенні. У результаті як високорівнева конструкція перспективного шифру обрана SPN-структура. Крім того, додатковим аргументом на користь саме цієї конструкції є неможливість використання недокументованих властивостей з несюр'єктивними S-блоками [7], що є припустимим для ланцюга Фейстеля і схеми Лей-Мессі.

Для підвищення складності атак лінійного, диференційного і алгебраїчного криптоаналізу додатково застосовується попереднє и прикінцеве забілювання (pre- and postwhitening) із використанням модульного додавання (2^{64}).

В рамках консервативного і прозорого підходу до проектування блокового шифру, шар нелінійного перетворення циклової функції реалізований на базі S-блоків. Крім вже зазначених у попередньому розділі переваг перед використанням специфічного набору арифметичних або логічних функцій, це рішення додатково забезпечує можливість:

− застосування підходу щодо доказової стійкості до диференційного і лінійного криптоаналізу на базі стратегії «широкого сліду» (wide trail strategy [19]);

− реалізації на широкому спектрі програмних і апаратних платформ.

Недоліком є нижча швидкість перетворення (компроміс заради стійкості без необхідності зміни стандарту через 2-5 років) і потенційна залежність часу виконання шифрування блоку при програмній реалізації на процесорах загального призначення із-за особливостей реалізації кеша L1. Ця особливість присутня у більшості блокових алгоритмів, що зараз використовуються, включаючи AES і ДСТУ ГОСТ 28147:2009, а в новому національному стандарті України необхідність впровадження контрзаходів відзначено у спеціальному додатку («Вимоги до реалізації»).

Розмір S-блоку був обраний виходячи з можливості ефективної реалізації на процесорах загального призначення, а при формуванні враховувались показники, що впливають на стійкість шифру до диференційного, лінійного, алгебраїчного криптоаналізу та відсутність нерухомих точок (fixed points) [4].

Стандарт передбачає використання чотирьох S-блоків, не є CCZ-еквівалентними [4]. Характеристики S-блоків наведені у таблиці 2.

Таблиця 2

Характеристики S-блоків шифру «Калина»

Характеристика	Номер S-блоку			
	1	2	3	4
Мінімальне значення нелінійності булевої функції	104			
Мінімальна алгебраїчна степінь булевої функції	7			
Макс. значення табл. розпод. різниць (ДК)	8			
Макс. значення табл. лін. апроксим. (ЛК)	24			
Степінь перевизначеної системи	3 (441 рівняння)			
Кількість циклів	4	4	6	4
Мінімальна довжина циклу	6	8	4	4

При порівнянні характеристик підстановок алгоритму «Калина» та інших блокових і потокових шифрів, геш-функцій, в т.ч. нових білоруських і російських перетворень можна відзначити, що саме національний стандарт України забезпе-

чує найбільшу нелінійність булевих функцій S-блоку, що дає додатковий запас стійкості до лінійного криптоаналізу. Більш високе значення нелінійності для бієктивного S-блока можна отримати використовуючи, наприклад, афінно-еквівалентні степенні функції у скінченому полі [4], але такі перетворення, використані у алгоритмах AES/Rijndael [19], Square [20], Camellia [14] та ін. можуть бути описані перевизначеною системою 2-го степеня, що ставить шифр під загрозу реалізації алгебраїчної атаки.

Крім того, у стандарті допускається використання іншого набору S-блоків (від одного до восьми), що постачаються в установленому порядку і можуть бути використані як додатковий довготерміновий ключовий елемент.

Для реалізації блоку лінійного розсіювання було обране множення на МДВ-матрицю як найбільш ефективний метод реалізації впливу кожного вхідного символу на кожний вихідний завдяки отриманню найбільшого індексу галуження (branch number) відображення [34, 19].

Для блокового шифру МДВ-перетворення може бути реалізовано двома способами:

- розмір вектора, який умножається на МДВ-матрицю, співпадає з розміром блоку шифру і проміжних значень між циклами шифрування;
- значення, що обробляється, розділяється на декілька блоків одного розміру, кожен з яких інтерпретується як вектор-стовпець, що множиться на МДВ-матрицю розміру, меншого розміру блоку шифру.

Вочевидь, підвищення розміру МДВ-матриці призводить до покращення криптографічних властивостей циклового перетворення. Приклад залежності кількості активних S-блоків від кількості операцій, необхідних для реалізації шифру з блоком 256 бітів для МДВ-матриці розміром 32 біта і 64 біта (відповідно, 4x4 і 8x8 над полем $GF(2^8)$), наведені на рис.1 [8]. Таким чином, збільшення розміру МДВ-перетворення призводить до підвищення стійкості при однаковій кількості операцій (або, при однаковій стійкості, збільшенню швидкодії за рахунок зменшення обчислювальної складності шифрування).

Водночас, існує технологічна межа збільшення розміру МДВ-матриці заради підвищення швидкодії на сучасних програмних платформах загального призначення. Найбільш ефективною є реалізація цієї операції у вигляді табличного перетворення (look-up tables), і всі таблиці, що використовуються при шифруванні, повинні уміщуватися до кешу L1 сучасних процесорів [8]. У іншому випадку, навіть при суттєво меншій кількості операцій, час виконання може бути значно більшим за рахунок промахів кешу (cache misses). Прикладом цього випадку є новий російський шифр «Кузнечик» [9] («Коник»), який має AES-подібну структуру, такий же розмір блоку (128 бітів), зменшену кількость циклів (9 замість 10). При цьому новий російський стандарт забезпечує нижчу швидкодію (див. табл. 7 та рис. 2), порівняно з «Калиною» та AES, на програмних платформах загального призначення, за рахунок збільшення розміра МДВ-матриці з 32 біт до 128 біт (відповідно, з 4x4 до 16x16 над полем $GF(2^8)$), викликане розміром табличного перетворення – 64кБ для найшвидшої версії «Кузнечика», що перевищує можливості ефективної роботи кеша L1 сучасних процесорів. На наш погляд (без доступу до проектної документації розробника алгоритму), це обумовлено вимогами оптимізації Rijndael-подібного перетворення російського шифру для компактної апаратної реалізації і високої криптографічної стійкості без вимог щодо високої швидкодії порівняно із іншими сучасними рішеннями.

Таким чином, при виборі розміру МДВ-матриці необхідно враховувати не тільки кількість операцій, що забезпечують достатні криптографічні властивості, але й обсяг пам'яті, необхідний для швидкісної програмної реалізації. Крім того, потрібно приймати до уваги кратність розміру матриці і блоку шифру (для запобігання застосування декількох комплектів таблиць, що збільшує розмір потрібної пам'яті) та розмір машинного слову процесорних архітектур.

Для блокового шифра «Калина» була обрана МДВ-матриця розміром 64x64 біта (8x8 над полем $GF(2^8)$) як така, що забезпечує необхідні криптографічні властивості і вимоги щодо швидкодії на сучасних програмних 64-бітових архітектурах, – настольних і серверних системах та мобільних пристроях. Зокрема, розмір табличного перетворення для найшвидшої реалізації дорівнює 16 кБ, що дозволяє ефективно використовувати можливості сучасних процесорів з розміром кешу даних L1 у 32 кБ або 64 кБ.

Кількість циклів (ітерацій) криптографічного алгоритму було обрано на основі достатнього запасу стійкості до різних видів криптоаналізу (див. нижче) і наведено у табл. 3.

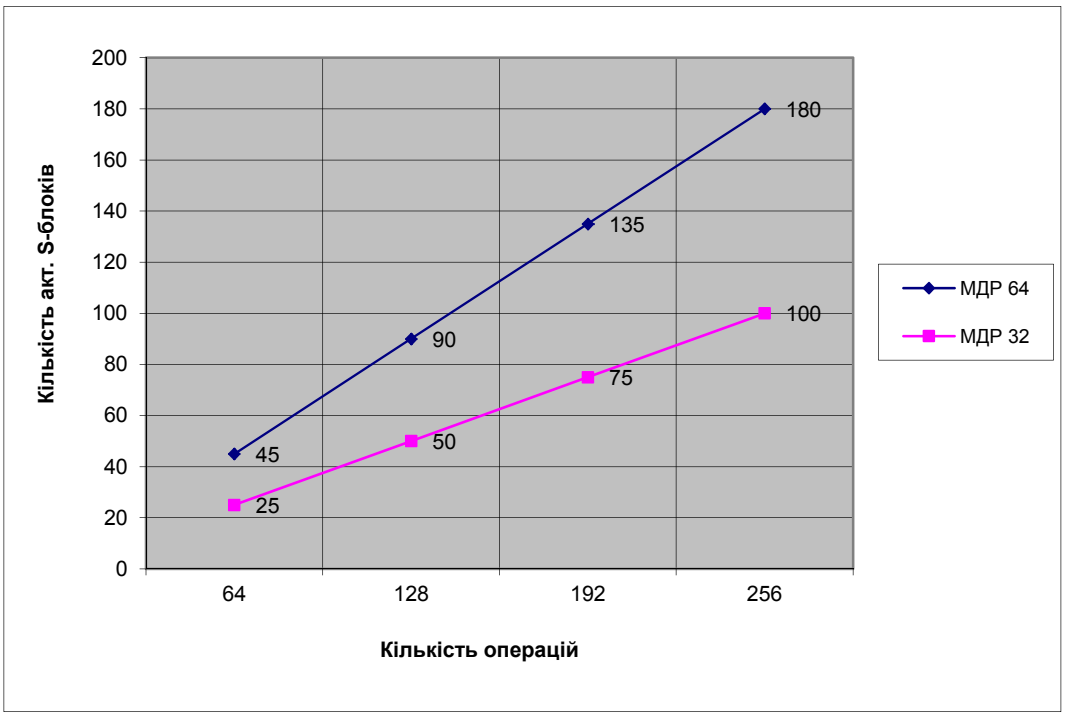

Рис. 1. Залежність кількості активних S-блоків від кількості операцій для шифру з розміром блоку 256 біт

Таблиця 3

Кількість циклів шифрування блокового шифру «Калина»

Довжина ключа, біт	Кількість циклів
128	10
256	14
512	18

Оптимальна реалізація алгоритму передбачає використання таблиць передобчислень, що одночасно реалізують нелінійні і лінійні перетворення (S-блок і множення на МДВ-матрицю). Вдосконалення, зроблені в шифрі Калина, дозволили залишити тільки один набір таблиць (AES потребує два набору), виконавши оптимізацію для прямого криптографічного перетворення (зашифрування). З врахуванням властивостей режимів роботи блокового шифру, така модифікація дозволяє досягти вищої швидкодії як при зашифруванні, так і розшифруванні для більшості режимів (CTR, CFB, CMAC, OFB, GCM, GMAC, CCM).

Для схеми розгортання ключів перспективного шифру були сформульовані наступні вимоги для забезпечення необхідних криптографічних і експлуатаційних властивостей [8].

1. Нелінійна залежність кожного біта кожного циклового ключа від кожного біта ключа шифрування.

2. Циклові ключі суттєво відрізняються і мають складну нелінійну залежність.

3. Захист від відомих криптоаналітичних атак, що орієнтовані на схему розгортання ключів.

4. Відсутність слабких ключів, при яких погіршуються криптографічні властивості або знижується стійкість перетворення.

5. Обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування трьох блоків.

6. Простота програмної, програмно-апаратної і апаратної реалізації.

Перша вимога необхідна для захисту від атак типу «зустріч посередині» (meet-in-the-middle), друга для попередження використання криптоаналітиком нерухомих точок (fixed points) циклового перетворення. Інші вимоги визначають загальну криптографічну стійкість і експлуатаційні властивості.

Як додаткові вимоги, доцільно розглянути наступні:

1. Неможливість отримання ключа шифрування по одному або декільком цикловим ключам, що є доступними для криптоаналитика.

2. Можливість формування циклових ключів у довільному порядку (однакова обчислювальна і просторова складність для зашифрування і розшифрування).

Перша додаткова вимога забезпечує лише лінійне зростання складності виконання криптоаналітичної атаки, тобто якщо криптоаналитик був спроможний отримати останній цикловий ключ, то він зможе отримати і попередні, із порі-

вняною складністю, і т.д. Тим не менш, для низки застосувань, для яких можуть бути застосовані атаки на реалізацію (наприклад, смарт-карти, usb-токени і т.ін.) наявність такої властивості є додатковою перевагою блокового шифру [8]. Тобто для випадків, коли криптоаналитик вже успішно відновив ключ шифрування для алгоритма із ін'єктивною схемою формування циклових ключів, шифр із неін'єктивним відображенням ще має запас стійкості.

Друга додаткова вимога є експлуатаційною і дозволяє більш ефективну реалізацію блокового шифру.

Таким чином, виключно на базі циклового перетворення блокового шифру «Калина» був реалізований генератор псевдовипадкових послідовностей, який задовольняє сформульованим вимогам як з точки зору криптографічних властивостей, так і обмеження на кількість операцій. Схема формування циклових ключів передбачає обчислення допоміжного ключа K_σ, а вже на його основі – циклових ключів.

K_σ генерується на основі ключа шифрування і початкового вектора, який, в свою чергу, залежить від розміру блоку і довжини ключа. Допоміжний ключ необхідний для забезпечення односпрямованості схеми формування (високої обчислювальної складності відновлення ключа шифрування із циклових ключів) і руйнування симетрії перетворення, що шифрує [8]. Призначення початкового вектора – забезпечення унікальних послідовностей циклових ключів для кожної комбінації розміру блока і ключа (наприклад, для режима 128/128 і 128/256 циклові ключі будуть формувати унікальні псевдовипадкові послідовності, навіть якщо 256-бітовий ключ складається із співпадаючих 128-бітових підблоків, які дорівнюють ключу режиму 128/128).

Циклові ключі з парними індексами формуються на основі ключа шифрування, допоміжного ключа і константи ϑ, яка залежить від номеру циклу (індексу). Така схема забезпечує односпрямованість, унікальність кожного сформованого значення та додатково покращує криптографічні властивості як схеми розгортання, так і всього шифру для забезпечення стійкості до атак, що використовують нерухомі точки циклового перетворення. Для отримання необхідних експлуатаційних характеристик, циклові ключі з непарними індексами формуються шляхом циклічного зсуву парних. Цей підхід забезпечує як необхідний рівень запасу криптографічної стійкості, так і достатню швидкодію перетворення.

Як вже було зазначено, для забезпечення додаткового захисту обрана схема є односпрямованою (неін'єктивною), що теоретично допускає існування еквівалентних ключів (різних ключів шифрування, що формують однакові послідовності циклових ключів).

В той же час, потужність множини значень послідовностей циклових ключів запропонованої схеми практично повністю співпадає зі потужністю множини значень ключа шифрування (від 0,9817 до 0,9999 залежно від розміру блоку і довжини ключа [8]). Таким чином, неін'єктивність схеми розгортання, необхідна для реалізації властивості односпрямованості, не дозволяє криптоаналитику зменшити складність атак переборного типу, в той же час забезпечуючи додаткову стійкість до низки методів криптографічного аналізу, спрямованого, в тому числі, і на апаратну або програмну реалізацію перетворення.

Таким чином, блоковий шифр «Калина» побудований на основі Rijndael-подібної структури із аналітичним обґрунтуванням саме цієї конструкції, але на відміну від AES в новому національному стандарті України застосовується:

- попереднє и прикінцеве забілювання (pre- and postwhitening) із використанням модульного додавання (2^{64}) для підвищення складності атак лінійного, диференційного і алгебраїчного криптоаналізу;
- чотири S-блока (замість одного), які не є CCZ-еквівалентними, не можуть бути описані перевизначеною системою 2-го степеня, і при порівнянні характеристик з іншими блоковими і потокових шифрами, геш-функціями забезпечують найбільшу нелінійність булевих функцій (104), що дає додатковий запас стійкості до алгебраїчного і лінійного криптоаналізу;
- збільшений розмір МДВ-перетворення, що покращує криптографічні властивості і є оптимальним для швидкодіючої реалізації на сучасних 64-бітових платформах;
- нова односпрямована схема розгортання циклових ключів, що забезпечує як захист від атак на схеми розгортання, яка забезпечує як достатню швидкодію перетворення, так і додаткову стійкість до низки методів криптографічного аналізу, спрямованого, в тому числі, і на апаратну або програмну реалізацію перетворення.

Крім більшого запасу криптографічної стійкості порівняно з AES, блоковий шифр «Калина» ефективно використовує особливості 64-бітових архітек-

тур, що дозволяє вдосконалити продуктивність. Додатково, нові національні стандарти шифрування (ДСТУ 7624:2014) і гешування (ДСТУ 7564:2014) мають спільний набір S-блоків та однакове МДВ-перетворення, за рахунок чого отримується компактна реалізація обох перетворень.

КРИПТОГРАФІЧНА СТІЙКІСТЬ БЛОКОВОГО ШИФРУ «КАЛИНА». При розробці національного стандарту була виконана оцінка стійкості перспективного криптографічного перетворення щодо різних видів криптоаналітичних атак [8].

Складність найбільш ефективних криптоаналітичних атак при зменшеної кількості циклів (послабленому алгоритмі) і необхідна кількість циклів для забезпечення стійкості наведені у табл.4-6 для шифру з розміром блока 128, 256 і 512 бітів.

Таблиця 4

Результати аналізу стійкості шифру «Калина» із розміром блоку 128 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість циклів	Обчисл. складність, екв. оп. шифрув.	Пам'ять, байтів
Диференційний	5	4	2^{55}	
Лінійний	5	3	$2^{52,8}$	
Усіч. диференц.	4	3		
Інтегральний	6	5	2^{97}	2^{33+4}
Нездійсн. дифер.	6	5	2^{62}	2^{66}
Бумеранг	5	4	2^{120}	

Таблиця 5

Результати аналізу стійкості шифру «Калина» із розміром блоку 256 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість циклів	Обчисл. складність, екв. оп. шифрув.	Пам'ять, байтів
Диференційний	7	6	2^{230}	
Лінійний	7	5	$2^{220,8}$	
Усіч. диференц.	4	3		
Інтегральний	7	6	2^{145}	2^{64+5}
Нездійсн. дифер.	6	5	2^{61}	2^{66}
Бумеранг	6	5	2^{220}	

Таблиця 6

Результати аналізу стійкості шифру «Калина» із розміром блоку 512 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість циклів	Обчисл. складність, екв. оп. шифрув.	Пам'ять, байтів
Диференційний	9	8	2^{490}	
Лінійний	9	7	$2^{470,4}$	
Усіч. диференц.	4	3		
Інтегральний	7	6	2^{137}	2^{64+5}
Нездійсн. дифер.	6	5	2^{60}	2^{66}
Бумеранг	7	6	2^{340}	

Відповідно, криптографічне перетворення є стійким при 6 циклах для 128-бітового блоку, 7 циклах для 256-бітового і 9 циклах для 512-бітового. Таким чином, шифр, який містить 10, 14 і 18 циклів для розміру блоку 128, 256 і 512 біт відповідно (див. табл. 3), забезпечує захист від розглянутих методів криптоаналізу і має достатній запас стійкості.

ШВИДКОДІЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ. Тестування було спрямоване на моделювання особливостей роботи засобів криптографічного захисту, що потребують високої швидкодії перетворень (захист IP-трафіку та ін.).

Для виключення впливу дискової підсистеми всі дані були розміщені в ОЗП (RAM). Для попередження використання даних, що розміщені тільки в кеш-пам'яті процесору був виділений

блок розміром 1 ГБ, який гарантовано у багато разів більший порівняно із наявним доступом кеш-пам'яті будь-якого сучасного процесора, що призведе до необхідності здійснення звернень до основного ОЗП. Для зниження впливу переключення контексту процесора, цей блок пам'яті був перешифрований декілька разів.

Вимірювання швидкодії через шифрування однакового обсягу відкритих текстів (режим простої заміни, ECB) виконувалось для блокового шифру „Калина" (всі комбінації розміру блоку і довжини ключа), AES-128, AES-256, ГОСТ 28147-89, СТБ 34.101.31-2011 («БелТ», національний стандарт Білорусії) і шифру «Кузнечик» (проект державного стандарту РФ) в однакових умовах в рамках роботи одного інтерактивного процесу користувача операційної системи.

Для отримання найбільшої швидкодії апаратно-незалежної реалізації була обрана мова програмування C++, використаний компілятор gcc version 4.9.2 (Ubuntu 4.9.2-0ubuntu1~12.04, 30-Oct-2014), тестування виконувалось на комп'ютері під управлінням 64-бітової ОС Linux (Ubuntu) з процесором Intel Core i5-4670@3.40GHz.

Результати тестування швидкодії програмної реалізації [31] для версій із найкращою оптимізацією компілятора (-O3 –m64) та порівняння результатів наведені у таблиці 7 та на рис. 2.

Таблиця 7

Швидкодія оптимізованих версій програмної реалізації блокових шифрів

№ з/п	Блоковий шифр	Швидкодія, Мбіт/с
1	Kalyna-128/128	2611.77
2	Kalyna-128/256	1779.52
3	Kalyna-256/256	2017.97
4	Kalyna-256/512	1560.89
5	Kalyna-512/512	1386.46
6	AES-128	2525.89
7	AES-256	1993.53
8	GOST 28147-89	639.18
9	STB 34.101.31-2011(BelT)	1055.92
10	Kuznyechik	1081.08

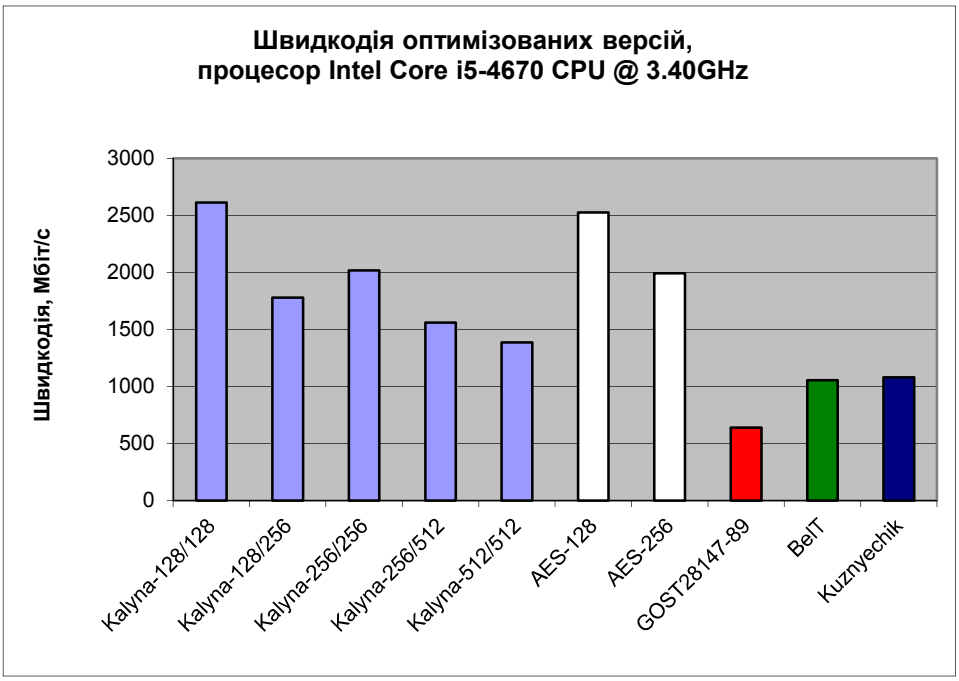

Рис. 2. Швидкодія оптимізованих версій програмної реалізації блокових шифрів

Таким чином, для оптимізованих версій на 64-бітовій платформі:

– для 128-бітової довжини ключа швидкодія «Калини» вища за AES на 3% (86 Мбіт/с);

– для 256-бітової довжини ключа швидкодія «Калини» повільніша за AES на 10% (для 128-бітового блоку) та швидше на 1% (для 256-бітового блоку);

– швидкодія «Калини» при відповідній довжині ключа вища за ГОСТ 28147-89 у 2,8 рази (для 128-бітового блоку) і 3,16 рази (для 256-бітового блоку), і приблизно у 2 рази вища, ніж у нових стандартів шифрування Білорусії і Росії.

Без фіксації розміру блоку Калина безумовно забезпечує більш швидке перетворення на тієї ж самої довжині ключа порівняно із AES.

Крім того, швидкісні показники та їх співвідношення для різних шифрів можуть достатньо суттєво змінюватися в залежності від версії компілятора (наприклад, використання нової версії компілятора gcc 4.9.2 замість 4.8.2 дозволило підвищити швидкість шифрування майже на 80 Мб/с.

Для порівняння програмних реалізації на інших платформах (мікроконтролерах, смарт-картах та ін.), де компілятори не реалізують надскладний модуль оптимізації, було виконано порівняння із відімкненими відповідними параметрами. Результати, що отримаються в цьому випадку, є, зазвичай, повільнішими ніж при включеній оптимізації. Водночас, такі результати корисні при оцінці співвідношення швидкодії при реалізації на асемблері та відповідній розробці апаратного-програмного модулю.

В цьому випадку перевага швидкодії «Калини» над AES складає від 12,5% до 27% в залежності від розміру блока та довжини ключа. У цих же умовах Калина виконує обробку швидше ніж ГОСТ 28147-89 від 3,17 до 3,72 разів.

Додатково слід зазначити, що «Калина» забезпечує суттєво більш високий запас стійкости до криптоаналітичних атак, ніж AES.

ВИСНОВКИ:

1. Блокові шифри є одним із найбільш поширених криптографічних примітивів, які використовуються як для забезпечення конфіденційності основного потоку інформації, що передається відкритими каналами зв'язку, а також як основний конструктивний елемент в ході побудови інших перетворень, таких як функції гешування, коди автентифікації повідомлень та ін.

2. ДСТУ ГОСТ 28147:2009 (ГОСТ 28147-89) використовується в Україні з 1990 р. Він все ще забезпечує практичну стійкість, тим не менш, для цього алгоритму відомі ефективні методи криптоаналізу, які мають складність значно меншу, ніж переборні атаки. Цей стандарт вже виведений із дії в Білорусії та планується до модифікації у РФ у 2015 р. З точки зору швидкодії, на сучасних обчислювальних архітектурах загального призначення ДСТУ ГОСТ 28147:2009 суттєво поступається іноземним аналогам.

3. Заміна ДСТУ ГОСТ 28147:2009 на AES не є вирішенням проблеми нового національного стандарту для України, бо світові тенденції вже свідчать про поступову відмову від AES: як на рівні міжнародних криптографічних конкурсів щодо розробки перспективних перетворень, так і нових рішень світових лідерів IT-індустрії, що застосовують нові алгоритми для заміни AES в мережевих протоколах захищеної передачі інформації.

4. Національний відкритий конкурс симетричних блокових криптографічних алгоритмів, проведений Державною службою спеціального зв'язку та захисту інформації України з врахуванням позитивного світового досвіду розробки криптографічних стандартів для США, ЕС, Японії та інших країн, дозволив відзначити перспективний блоковий шифр, на основі якого і був розроблений ДСТУ 7624:2014.

5. Розробка нового національного стандарту України вимагала вирішення складної задачі побудови швидкого криптографічного перетворення, яке водночас забезпечує високий і надвисокий рівень стійкості, в умовах обмеження часових, дослідницьких і обчислювальних ресурсів порівняно з іншими технологічно розвиненими країнами. Тим не менш, ефективне застосування вітчизняними науковцями наявних ресурсів і накопиченого світового досвіду відкритих криптографічних конкурсів дозволило створити сучасне стійке та продуктивне перетворення.

6. Блоковий шифр "Калина", визначений ДСТУ 7624:2014, забезпечує нормальний, високий і надвисокий рівень стійкості, із довжинами блока і ключа 128, 256 і 512 бітів. На момент написання статті це єдиний в світі національний стандарт, який визначає блоковий алгоритм шифрування із симетричним ключем довжиною 512 бітів.

7. У якості високорівневої конструкції шифру на основі аналітичного порівняння обрана SPN-структура як більш ефективна порівняно з ланцюгом Фейстеля і схемою Лей-Мессі. Крім того, додатковим аргументом на користь саме цієї конструкції є неможливість використання недокументованих властивостей з несюр'єктивними S-блоками, що є припустимим для двох останніх перетворень.

8. В рамках консервативного і прозорого підходу до проектування блокового шифру, шар нелінійного перетворення циклової функції реалізований на базі S-блоків. Розмір S-блоку був обраний виходячи з можливості ефективної реалізації на процесорах загального призначення, а

при формуванні враховувались показники, що впливають на стійкість шифру до диференційного, лінійного, алгебраїчного криптоаналізу та відсутність нерухомих точок. Стандарт передбачає використання чотирьох S-блоків, які не є CCZ-еквівалентними. При порівнянні характеристик підстановок алгоритму «Калина» та інших блокових і потокових шифрів, геш-функцій, в т.ч. нових білоруських і російських перетворень можна відзначити, що саме національний стандарт України забезпечує найбільшу нелінійність булевих функцій S-блоку, що дає додатковий запас стійкості до лінійного криптоаналізу, одночасно забезпечуючи стійкість і до алгебраїчних атак. Крім того, у стандарті допускається використання іншого набору S-блоків (від одного до восьми), що можуть бути використані як додатковий довготерміновий ключовий елемент.

9. Для реалізації блоку лінійного розсіювання було обране множення на МДВ-матрицю як найбільш ефективний метод реалізації впливу кожного вхідного символу на кожний вихідний. Для блокового шифра «Калина» задана МДВ-матриця розміром 64x64 біта (8x8 над полем $GF(2^8)$) як така, що забезпечує необхідні криптографічні властивості і вимоги щодо швидкодії на сучасних програмних 64-бітових архітектурах – настольних і серверних системах та мобільних пристроях.

10. В алгоритмі реалізована нова односпрямована конструкція схеми розгортання ключів, що використовує циклове перетворення і забезпечує стійкість до переборних атак та відомих методів аналізу, які орієнтовані на схему розгортання ключів, так і додатковий захист від низки методів криптоаналізу, спрямованого, в тому числі, і на апаратну або програмну реалізацію перетворення. Обчислювальна і просторова складність формування циклових ключів однакова як для зашифрування, так і розшифрування.

11. Оцінка криптографічної стійкості показала, що шифр забезпечує захист від відомих методів криптоаналізу і має запас стійкості із врахуванням можливого вдосконалення криптоаналітичних атак і перспектив розвитку масових напівпровідникових технологій.

12. Новий національний стандарт забезпечує швидкодію шифрування 2611,77 Мбіт/с (128-бітовий ключ), 2017,97 Мбіт/с (256-бітовий) і 1386,46 Мбіт/с (512-бітовий) при програмній реалізації мовою C++ (gcc v4.9.2) на 64-бітовій платформі Intel Core i5-4670@3.40GHz. Це перевищує показники AES на 1-3% (до 86 Мбіт/с). При відключеній оптимізації компілятора перевага швидкодії Калини над AES складає від 12,5% до 27% в залежності від розміру блока та довжини ключа. Додатково слід зазначити, що «Калина» забезпечує суттєво більш високий запас стійкості до криптоаналітичних атак, ніж AES. Продуктивність нового національного стандарту України на цій платформі приблизно у 2 рази вища, ніж у нових стандартів шифрування Білорусії і Росії, та в 3,16 рази вища, ніж у старого стандарту ДСТУ ГОСТ 28147:2009, при однаковій довжині ключа.

ЛІТЕРАТУРА

[1]. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. – Введ. 01–07–1990. – М. : Изд-во стандартов, 1989. – 28 с.

[2]. Державна служба спеціального зв'язку та захисту інформації України, Інститут кібернетики імені В.М. Глушкова Національної академії наук України. Положення про проведення відкритого конкурсу криптографічних алгоритмів. [Electronic resource] Mode of access : www. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/printable_article?art_id=48383.

[3]. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.

[4]. Казимиров О.В. Методи та засоби генерації нелінійних вузлів заміни для симетричних криптоалгоритмів. Дисертація на здобуття наукового ступеня кандидата технічних наук по спеціальності 05.13.21 – системи захисту інформації. Харківський національний університет радіоелектроніки, Харків, 2014.

[5]. Кайдалов Д.С., Олейников Р.В.. Оценка эффективности SPN-структуры блочного симметричного шифра. Восточно-Европейский журнал передовых технологий. – 2014. – №6/9 (72). – С. 4–10.

[6]. Олійников Р. В. Криптоаналіз на основі передобчислень: уточненення ефективності rainbow-таблиць [Текст] / Р. В. Олійников // Спеціальні телекомунікаційні системи та захист інформації. – 2010. – № 2 (18). – С. 26–32.

[7]. Олійников Р. В. Оцінка стійкості симетричних блокових шифрів на базі ланцюга Фейстеля при використанні несюр'єктивних S-блоків [Текст] / Р. В. Олійников // Спеціальні телекомунікаційні системи та захист інформації. – 2010. – № 1 (17). – С. 77–84.

[8]. Олійников Р.В. Методи аналізу і синтезу перспективних симетричних криптографічних перетворень. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. –

Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2014.

[9]. Проект национального стандарта Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры. М. : Стандартинформ, 2015. – 25 с. [Electronic resource]. – Mode of access : www. URL: http://www.tc26.ru/standard/draft/GOSTR-bsh.pdf.

[10]. СТБ 34.101.31–2011. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. – Взамен СТБ П 34.101.31–2007; введ. 31–01–2011. – Минск, 2011. – 35 с.

[11]. Шеннон К. Теория связи в секретных системах [Текст] / Клод Шеннон // Работы по теории информации и кибернетике. – М., 1963. – С. 333–369.

[12]. Advanced Encryption Standard (AES) [Electronic resource] : FIPS PUB 197. – 2001 – Mode of access : www. URL: http://csrc.nist.gov/ publications/fips/fips197/fips-197.pdf.

[13]. Advanced Encryption Standard (AES) Development Effort [Electronic resource]. – Mode of access: http://csrc.nist. gov/ archive/ aes/ index2.html #overview.

[14]. K. Aoki et al. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis [Text] // Selected Areas in Cryptography. – Berlin ; Heidelberg : Springer, 2001. – P. 39–56.

[15]. Barkan E. Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs [Text] / Elad Barkan, Eli Biham, Adi Shamir // Advances in Cryptology – CRYPTO 2006 : proceedings of the 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2006. – Berlin ; Heidelberg : Springer, 2006. – P. 1–21. – (Lecture Notes in Computer Science ; vol. 4117).

[16]. Beaulieu R. et al. The SIMON and SPECK Families of Lightweight Block Ciphers //IACR Cryptology ePrint Archive. – 2013. – Т. 2013. – С. 404.

[17]. D.J. Bernstein. ChaCha, a variant of Salsa20. [Electronic resource] / The University of Illinois at Chicago. Mode of access : www. URL: http://cr.yp.to/chacha/chacha-20080128.pdf.

[18]. Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) [Electronic resource] / National Institute of Standards and Technology. – Mode of access : www. URL: http://csrc.nist.gov/groups/ST/hash/sha-3.

[19]. Daemen J. AES proposal: Rijndael [Text] / J. Daemen, V. Rijmen // First Advanced Encryption Standard (AES) Conference, Ventura, CA, August 20–22, 1998.

[20]. Daemen J. The block cipher Square [Text] / J. Daemen , L. Knudsen, V. Rijmen // Fast Software Encryption. – Berlin ; Heidelberg : Springer, 1997. – P. 149–165.

[21]. Data Encryption Standard (DES) [Electronic resource] : FIPS 46–3 / National Bureau of Standards, USA. – 1993. – Mode of access: www. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[22]. CRYPTREC Cryptography Research and Evaluation Committees [Electronic resource]. – Mode of access : www. URL: http://www.cryptrec. go.jp/ english/ about. html.

[23]. ISO/IEC 18033-3:2010. International standard. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. Swithzerland, ISO copyright office, 2010.

[24]. Junod P. FOX: a new family of block ciphers [Text] / P. Junod, S. Vaudenay // Selected Areas in Cryptography. – Berlin ; Heidelberg : Springer, 2005. – P. 114–129.

[25]. Karsten N. GSM: SRSLY? [Text] / Nohl Karsten, Chris Paget // Proceedings of the 26th Chaos Communication Congress (26C3), Berlin, Germany, December 27–30, 2009.

[26]. Menezes A. J. Handbook of applied cryptography [Text] / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC press, 2010.

[27]. National Security Agency of the U.S. Domestic Surveillance Directorate. Utah Data Center. [Electronic resource] Mode of access : www. URL: https://nsa.gov1.info/utah-data-center/

[28]. New European Schemes for Signatures, Integrity, and Encryption (NESSIE), IST-1999-12324 [Electronic resource]. – Mode of access : www. URL: https://www.cosic.esat.kuleuven.be/nessie.

[29]. Oechslin P. Making a Faster Cryptanalytic Time-Memory Trade-Off [Text] / Philippe Oechslin // Advances in Cryptology – CRYPTO 2003 : proceedings of the 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 2003. – Berlin ; Heidelberg : Springer, 2003. – P. 617–630. – (Lecture Notes in Computer Science ; vol. 2729).

[30]. R. V. Oliynykov, I. D. Gorbenko, et al. Results of Ukrainian national public cryptographic competition [Text] // Tatra Mountains Mathematical Publications. – 2010. – Vol. 47. – P. 99–114.

[31]. Roman Oliynykov, Oleksandr Kazymyrov, Olena Kachko, Ruslan Mordvinov, et al. Source code for performance estimation of 64-bit optimized implementation of the block ciphers Kalyna, AES, GOST, BelT, Kuznyechik. [Electronic resource] : 2015. – Mode of access : www. URL: https://github. com/ Roman-Oliynykov /ciphers-speed/

[32]. Rudskoy V. On zero practical significance of key recovery attack on full GOST block cipher with zero time and memory [Electronic resource] : report 2010/111 / Vladimir Rudskoy // Cryptology ePrint Archive. – 2010. – Mode of access : www. URL: http://eprint.iacr.org/2010/111.

[33]. B Schneier et al. The Twofish encryption algorithm: a 128-bit block cipher [Text] / John Wiley & Sons, Inc., 1999. – 186 p.

[34]. Schnorr C. P. Black box cryptanalysis of hash networks based on multipermutations [Text] / C. P. Schnorr, S. Vaudenay // Advances in Cryptology – EUROCRYPT'94 : proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9–12, 1994. – Berlin ; Heidelberg : Springer, 1995. – P. 47–57. – (Lecture Notes in Computer Science ; vol. 950).

REFERENCES

[1]. GOST 28147-89. Systems obrabotku information. Zashchita kryptohrafycheskaya. Algorithm kryptohrafycheskoho transformation [text]. - Key. 07.01.1990. - Moscow: Publishing House of standartov, 1989. - 28 p.

[2]. State Service of Special Communication and Information Protection of Ukraine, Institute of Cybernetics of VM Glushkov National Academy of Sciences of Ukraine. Terms and conditions of open competition cryptographic algorithms. [Elec-tronic resource] Mode of access: www. URL: http://www. dstszi. gov. ua/ dstszi/control/uk/ publish/ printable_article?art_id = 48383.

[3]. ISO 7624: 2014. Information Technology. Cryptographic protection of information. The algorithm is a symmetric block conversion. [Text], Key. 01.07.2015, K: Minister of Ukraine, 2015.

[4]. Kazimirova OV Methods and tools for generation of nonlinear units replacement for symmetric-toalhorytmiv creeps. The thesis for the degree of candidate of technical sciences on 05.13.21 specialty - information security. Kharkiv National University of Radio Electronics, Kharkiv, 2014.

[5]. Kaydalov DS, Oleynikov R.V .. Evaluation of the effectiveness SPN-structure symmetrychnoho block cipher. East Evropeyskyy magazine peredovыh technology. - 2014. - №6 / 9 (72). - P. 4-10.

[6]. Oliynykov RV Kryptoanaliz on the basis of redobchyslen: utochnenennya rainbow-efficiency tables [Text] / RV Oliynykov // telekomunikatsiyni are special systems and protection of information. - 2010. - № 2 (18). - P. 26-32.

[7]. Oliynykov R. Evaluation of stability symmetrical block shyfriv on the basis Feystelya chain when using nesyur'yektyvnyh S-blocks [Text] / RV Oliynykov // telekomunikatsiyni are special systems and protection of information, 2010, № 1 (17), P. 77-84.

[8]. RV Olejnikov Methods of analysis and synthesis of first-symmetric crypto for Policy ne-retvoren. The thesis for the degree of doctor of technical sciences, specialty 05.13.05 - Computer Systems and Components. - Kharkiv National University of Radio, Ministry of Education and Science of Ukraine, Kharkiv, 2014.

[9]. Project of National-standard Russian Federation. Ynformatsyonnaya technology. Kryptohrafycheskaya protection of information. Blochnыe shyfrы. MM: Standartynform, 2015. - 25 p. [Electronic resource]. - Mode of access: www. URL: http://www. tc26. ru/standard/draft/GOSTR-bsh.pdf.

[10]. STB 34.101.31-2011. Information Technology and security. Zashchita information. Kryptohrafycheskye encryption algorithms and control integrity. - Instead STB P 34.101.31-2007; intr. 31.01.2011, Minsk, 2011, 35 p.

[11]. Shannon K. Theory sekretnыh in communication systems [Tekst] / Claude Shannon // work on the theory of information and cybernetics, M., 1963, P. 333-369.

[12]. Advanced Encryption Standard (AES) [Electronic resource]: FIPS PUB 197. - 2001 - Mode of ac-cess: www. URL: http://csrc.nist.gov/ publica-tions / fips / fips197 / fips-197.pdf.

[13]. Advanced Encryption Standard (AES) Develop-ment Effort [Electronic resource], Mode of ac-cess: http://csrc.nist.gov/archive/aes/index2.html#overview.

[14]. K. Aoki et al. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Anal-ysis [Text] // Selected Areas in Cryptography. - Berlin; Heidelberg: Springer, 2001. - R. 39-56.

[15]. E. Barkan Rigorous Bounds on Cryptanalytic Time / Memory Tradeoffs [Text] / Elad Barkan, Eli Biham, Adi Shamir // Advances in Cryptology - CRYPTO 2006: rroceedings of the 26th Annual International Cryptology Conference, Santa Barba-ra, California, USA, August 20-24, 2006. - Berlin; Heidelberg: Springer, 2006. - R. 1-21. - (Lecture Notes in Computer Science; vol. 4117).

[16]. Beaulieu R. et al. The SIMON and SPECK Families of Lightweight Block Ciphers // IACR Cryptology ePrint Archive. - 2013. - T. 2013. - P. 404.

[17]. D.J. Bernstein. ChaCha, a variant of Salsa20. [Electronic resource] / The University of Illinois at Chicago. Mode of access: www. URL: http://cr.yp.to/chacha/chacha-20080128.pdf.

[18]. Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) [Electronic resource] / National Institute of Standards and Technology. - Mode of access: www. URL: http://csrc.nist.gov/groups/ST/hash/sha-3.

[19]. Daemen J. AES proposal: Rijndael [Text] / J. Daemen, V. Rijmen // First Advanced Encryption Standard (AES) Conference, Ventura, CA, August 20-22, 1998.

[20]. Daemen J. The block cipher Square [Text] / J. Daemen, L. Knudsen, V. Rijmen // Fast Software Encryption. - Berlin; Heidelberg: Springer, 1997. P. 149-165.

[21]. Data Encryption Standard (DES) [Electronic resource]: FIPS 46-3 / National Bureau of Stand-ards, USA. - 1993. - Mode of access: www. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips 46- 3.pdf.

[22]. CRYPTREC Cryptography Research and Evaluation Committees [Electronic resource]. - Mode of

access: www. URL: http://www.cryptrec.go.jp /english/ about.html.
[23]. ISO / IEC 18033-3: 2010. International standard. Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers. Swithzerland, ISO copyright office, 2010.
[24]. Junod P. FOX: a new family of block ciphers / Robert Junod, S. Vaudenay /Selected Areas in Cryp-tography, Berlin; Heidelberg: Springer, 2005. P. 114-129.
[25]. Karsten N. GSM: SRSLY? [Text] / Nohl Karsten, Chris Paget // Rroceedings of the 26th Chaos Communication Congress (26C3), Berlin, Germa-ny, December 27-30, 2009.
[26]. Menezes AJ Handbook of applied cryptography [Text] / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. - CRC press, 2010.
[27]. National Security Agency of the US Domestic Surveillance Directorate. Utah Data Center. [Elec-tronic resource] Mode of access: www. URL: https://nsa.gov1.info/utah-data-center/
[28]. New European Schemes for Signatures, Integrity, and Encryption (NESSIE), IST-1999-12324 [Electronic resource]. - Mode of access: www. URL: https://www.cosic.esat.kuleuven.be/nessie.
[29]. R. Oechslin Making a Faster Cryptanalytic Time-Memory Trade-Off [Text] / Philippe Oechslin // Advances in Cryptology - CRYPTO 2003: ™ Proceedings of the 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17 -21, 2003. - Berlin; Heidelberg: Spring-er, 2003. P. 617-630. - (Lecture Notes in Com-puter Science; vol. 2729).
[30]. R. V. Oliynykov, I. D. Gorbenko, et al. Results of Ukrainian national public cryptographic competition [Text] // Tatra Mountains Mathematical Publications., 2010, Vol. 47, P. 99-114.
[31]. Roman Oliynykov, Oleksandr Kazymyrov, Olena Kachko, Ruslan Mordvinov, et al. Source code for performance estimation of 64-bit optimized implementation of the block ciphers Kalyna, AES, GOST, BelT, Kuznyechik. [Electronic resource]: 2015. - Mode of access: www. URL: https://github.com/Roman-Oliynykov/ciphers-speed/
[32]. Rudskoy V. On zero practical significance of key recovery attack on full GOST block cipher with zero time and memory [Electronic resource]: report 2010/111 / Vladimir Rudskoy // Cryptology ePrint Archive. - 2010. - Mode of access: www. URL: http://eprint.iacr.org/2010/111.
[33]. B. Schneier et al. The Twofish encryption algorithm: a 128-bit block cipher [Text] / John Wiley & Sons, Inc., 1999. - 186 p.
[34]. Schnorr CP Black box cryptanalysis of hash networks based on multipermutations [Text] / CP Schnorr, S. Vaudenay // Advances in Cryptology - EUROCRYPT'94: rroceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994. - Berlin; Heidelberg: Springer, 1995. - R. 47-57. - (Lecture Notes in Computer Science; vol. 950).

ПРИНЦИПЫ ПОСТРОЕНИЯ И ОСНОВНЫЕ СВОЙСТВА НОВОГО НАЦИОНАЛЬНОГО СТАНДАРТА БЛОЧНОГО ШИФРОВАНИЯ УКРАИНЫ

С 1-го июля 2015 г. в Украине вводится в действие криптографический стандарт блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр «Калина» и режимы его работы для обеспечения конфиденциальности и целостности. Национальный стандарт разработан как результат сотрудничества Государственной службой специальной связи и защиты информации Украины и ведущих украинских ученых на основе проведения открытого конкурса криптографических алгоритмов. В сравнении с известным международным стандартом AES, алгоритм ДСТУ 7624:2014 обеспечивает более высокий уровень криптографической стойкости (с возможностью применения блока и ключа шифрования до 512 битов включительно) и сравнимое или более высокое быстродействие на современных и перспективных программных и программно-аппаратных платформах, существенно превышая показатели ДСТУ ГОСТ 28147:2009 (ГОСТ 28147-89), используемый уже более 25 лет. В статье рассмотрены современные проблемы разработки блочных шифров и их решения, внедренные разработчиками в новом национальном стандарте Украины.

Ключевые слова: ДСТУ 7624:2014, блочный шифр, криптоанализ, быстродействие шифрования, национальный стандарт.

DESIGN PRINCIPLES AND MAIN PROPERTIES OF THE NEW UKRAINIAN NATIONAL STANDARD OF BLOCK ENCRYPTION

On the 1st of July, 2015 Ukraine adopts new cryptographic standard of symmetric block transformation DSTU 7624:2014 which defines "Kalyna" cipher and its confidentiality and integrity modes of operation. The national standard is developed as collaboration result of State Service of Special Communication of Ukraine and leading Ukrainian scientists based on the public cryptographic algorithms competition. In comparison to well-known standard AES, DSTU 7624:2014 provides higher level of cryptographic strength (with possibility of application of block and key length up to 512 bits) and comparable or higher performance on modern software or software-hardware platforms, essentially exceeding rates of DSTU GOST 28147:2009 (GOST 28147-89) which have been used over 25 years. It is considered modern problems of block cipher development and their solutions implemented by the developers in the new national standard of Ukraine.

Index terms: DSTU 7624:2014, block cipher, cryptanalysis, encryption performance, national standard.

Олійников Роман Васильович, доктор техічних наук, Начальник відділу наукових досліджень Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: ROliynykov@gmail.com.
Олейников Роман Васильевич, доктор технических наук, начальник отдела научных исследований закрытого акционерного общества «Институт информационных технологий».
Oliynykov Roman, doctor of technical sciences, head of scientific research department of joint-stock company «Institute of information technologies».

Горбенко Іван Дмитрович, доктор техічних наук, Головний конструктор Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: GorbenkoI@iit.kharkov.ua.
Горбенко Иван Дмитриевич, доктор технических наук, главный конструктор закрытого акционерного общества «Институт информационных технологий».
Gorbenko Ivan, doctor of technical sciences, chief designer of joint-stock company «Institute of information technologies».

Казимиров Олександр Володимирович, кандидат технічних наук, Технічний тест-аналітик у компанії EVRY Norge AS.
E-mail: okazymyrov@gmail.com.
Казимиров Александр Владимирович, кандидат технических наук, технический тест-аналитик в компании EVRY Norge AS.
Kazymyrov Oleksandr, candidate of technical sciences, Technical Test Analyst in the company EVRY Norge AS.

Руженцев Віктор Ігорович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Харківського національного університета радіоелектроніки.
E-mail: vityazik@rambler.ru.
Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники.
Ruzhentsev Victor, candidate of technical sciences, Assossiate Professor of The Department of Information Technology Security, Kharkiv National University of Radio Electronics.

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: GorbenkoU@iit.kharkov.ua.
Горбенко Юрий Иванович, кандидадт технических наук, технический директор закрытого акционерного общества «Институт информационных технологий».
Gorbenko Iurii, candidate of technical sciences, technical director of joint-stock company «Institute of information technologies».

УДК 004.056

МОДЕЛІ ДЛЯ ОРГАНІЗАЦІЇ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ

Андрій Дудатьєв

Поняття інформаційної безпеки доцільно розглядати з позиції оцінювання та забезпечення комплексної інформаційної безпеки в умовах ведення інформаційної війни. Фактично констатується необхідність урахування специфіки технологій проведення спеціальних інформаційних операцій з боку об'єкта впливу на етапах проектування, впровадження і супроводу комплексних систем захисту інформації. Досвід останніх років і подій показує, що ефективність застосування інформаційної зброї у сучасних умовах інформатизації суспільства достатньо велика і за своїми кількісними показниками може бути порівняна зі зброєю масового знищення. У статті представлені дві математичні моделі, які дозволяють оцінити потужність інформаційного впливу з урахуванням специфіки джерела та механізму реалізації впливу, а також запропонувати управлінські рішення для підготовки і подальшого проведення спеціальних інформаційних контроперацій. Аналіз запропонованих моделей дозволив сформулювати узагальнені етапи методики для прийняття ефективних рішень щодо управління інформаційною безпекою на об'єкті захисту в умовах інформаційної війни.
Ключові слова: *інформаційна війна, інформаційна зброя, інформаційно-психологічний вплив, комплексна система захисту інформації.*

Вступ. Моделювання інформаційної взаємодії двох або більшої кількості суб'єктів за умови їхньої життєдіяльності в умовах інформаційної війни зводиться до розробки математичних моделей інформаційного протиборства. При цьому якість розроблених моделей визначається ґрунтовністю теоретичних розробок і адекватним математичним апаратом. Конкуруючі об'єкти у більшості випадків практикують проведення інформаційних операцій для боротьби за різноманітні