10. Гончаров, А. В. Оцінка амплітуди радіосигналу при асиметрично-ексцесній адитивній заваді із застосуванням усічених поліномів Кунченка [Текст] / А. В. Гончаров, В. М. Уманець // Вісник ЧДТУ – 2013. – № 2. – С. 111–118.
11. Кунченко, Ю. П. Генерація псевдовипадкових послідовностей на основі бігаусового розподілу [Текст] / Ю. П. Кунченко, С. В. Заболотній, О. С. Гавриш, А. Ю Іванченко// Комп'ютерні технології друкарства. – 2000. – № 4. – С. 343–351.
12. Палагін, В. В. Комп'ютерне моделювання сумісних алгоритмів розрізнення радіосигналів та оцінювання їх параметрів на фоні негаусівських завад [Текст] / В. В. Палагін, А. В. Гончаров, В. М. Уманець // PREDT-2013: праці III міжнародної науково-практичної конференції, 24-26 жовтня 2013 р.: тези доп. – Чернівці: ЧНУ імені Юрія Федьковича, 2013. – С. 109–110.

Розглядаються структура, базові перетворення та режими застосування перспективного криптографічного алгоритму симетричного блокового перетворення «Калина». Досліджуються математичні та програмні моделі криптоалгоритму для перевірки правильності реалізації. Для виключення джерела загальних помилок у різних компонентах шифру застосовується багатоверсійна розробка. Обґрунтовується методика перевірки правильності програмної реалізації криптографічного перетворення включаючи режими застосування та тестові приклади

Ключові слова: блоковий симетричний шифр, криптографічне перетворення, правильність програмної реалізації, тестові приклади

Рассматриваются структура, базовые преобразования и режимы использования перспективного криптографического алгоритма симметричного блочного преобразования «Калина». Исследуются математические и программные модели криптоалгоритма для проверки правильности реализации. Для исключения источники общих ошибок в различных компонентах шифра применяется многоверсионная разработка. Обосновывается методика проверки правильности программной реализации криптографического преобразования включая режимы применения и тестовые примеры

Ключевые слова: блочный симметричный шифр, криптографическое преобразование, правильность программной реализации, тестовые примеры

УДК 004.056.55
DOI:10.15587/1729-4061.2014.28010

РОЗРОБКА МАТЕМАТИЧНИХ ТА ПРОГРАМНИХ МОДЕЛЕЙ ПЕРСПЕКТИВНОГО АЛГОРИТМУ ШИФРУВАННЯ ДЛЯ ПЕРЕВІРКИ ПРАВИЛЬНОСТІ РЕАЛІЗАЦІЇ

Ю. І. Горбенко
Кандидат технічних наук, старший науковий співробітник, лауреат державної премії в галузі науки та техніки*
E-mail: GorbenkoU@iit.com.ua
Р. І. Мордвінов
Аспірант*
E-mail: RMordvinov@gmail.com
О. О. Кузнецов
Доктор технічних наук, професор
Кафедра безпеки інформаційних систем та технологій
Харківський національний університет ім. В. Н. Каразіна
пл. Свободи, 4, м. Харків, Україна, 61022
E-mail: kuznetsov_alex@rambler.ru
*Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
пр. Леніна, 14, м. Харків, Україна, 61000

1. Вступ

Важливою складовою безпеки сучасних інформаційно-комунікаційних систем є механізми криптографічного захисту, зокрема блокове симетричне шифрування (БСШ), яке полягає у перетворенні інформації з використанням ключових даних з метою приховування (відновлення) змісту інформаційного повідомлення, підтвердження його справжності, цілісності, авторства.

У напрямку розроблення вітчизняних методів і засобів захисту інформації для забезпечення взаємної

сумісності результатів криптоперетворень у засобах криптографічного захисту інформації (КЗІ) різних виробників [1], з метою забезпечення інформаційної безпеки України Адміністрацією Держспецзв'язку забезпечено розроблення вітчизняного криптографічного алгоритму симетричного блокового перетворення. Впровадження цього НД спрямоване на забезпечення належного виконання вимог Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22.05.98 № 505 [2], тісно пов'язано із виконанням завдань та основних положень Доктрини інформаційної безпеки, законів України «Про основи національної безпеки України» [3], «Про інформацію» [4], «Про захист інформації в інформаційно-телекомунікаційних системах» [5], «Про Національну систему конфіденційного зв'язку» [6] та інших нормативно-правових актів із захисту національного інформаційного простору України.

Одним з важливих питань, пов'язаних з використанням засобів КЗІ, є забезпечення правильності роботи реалізованого БСШ, взаємна сумісність результатів криптоперетворень у засобах різних виробників. Основними завданнями, що вирішуються в цій роботі, є розробка математичних та програмних моделей перспективного алгоритму шифрування, обгрунтування методики перевірки правильності його реалізації.

2. Аналіз літературних джерел та постановка проблеми

Специфікацію нового алгоритму БСШ «Калина» наведено в проекті національного стандарту ДСТУ «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» [7–9]. Ця специфікація визначає базове перетворення (шифрування електронної кодової книги (ECB) або простої заміни) та різні режими застосування, зокрема гамування (CTR), гамування зі зворотнім зв'язком за шифр текстом (CFB), вироблення імітовставки (CMAC), зчеплення шифрблоків (CBC), гамування зі зворотнім зв'язком за шифргамою (OFB), вибіркового гамування із прискореним виробленням імітовставки (GCM ТА GMAC), вироблення імітовставки і гамування (CCM), індексованої заміни (XTS), захисту ключових даних (KEY WRAPPING) [9, 10].

В досліджено теоретичні та практичні аспекти аналізу та синтезу симетричних криптоперетворень. Зокрема, в монографіях вітчизняних вчених [11, 12] та закордонних авторів [13, 14] системно викладаються загальнотеоретичні питання побудови симетричних криптографічних систем захисту інформації в тому числі і симетричних блокових шифрів. В роботі [15] детально описаний алгоритм БСШ AES, який переміг на відкриоому конкурсі симетричних криптоалгоритмів США та став новим стандартом шифрування 21 сторіччя. В [16] розвинуто технологію диференційного, а в [17] лінійного криптоаналізу, в роботі [18] викладено питання реалізації інтегральної атаки. В звіті [19] підсумовано результати великого європейського проекту криптографічних алгоритмів NESSIE, а ресурс [20] присвячено для обговорення результатів відкритого конкурсу БСШ США. Монографію [21] присвячено викладенню нової технології оцінки стійкості БСШ на основі аналізу зменшених моделей шифрів. Це невеликий перелік сучасних наукових публікацій звісно не охоплює всі результати проведених досліджень, але містить найбільш значущі та відомі досягнення.

Обґрунтуванню сучасних вимог та принципів проектування перспективного БСШ України, його структури та основних криптографічних примітивів присвячено роботи [22–27]. Зокрема, в [22, 23] сформульовані основні вимоги до перспективного БСШ та принципи його проектування. В [24] обґрунтовано показники криптографічної стійкості. Роботи [25, 26] присвячено дослідженню диференційних та лінійних властивостей БСШ України, зокрема із застосуванням зменшених моделей шифрів. В [27] узагальнюються результати досліджень певних властивостей шифрів в порівнянні із властивостями випадкової підстановки.

Однак аналіз публікацій [22–27] свідчить, що завдання забезпечення правильності роботи реалізованого БСШ, взаємної сумісності результатів криптоперетворень у засобах різних виробників на сьогоднішній день не вирішені. Таким чином, актуальною науково-практичною проблемою, що тісно пов'язана із виконанням низки важливих державних програм і проектів [1–8], є дослідження специфікації нового БСШ «Калина», розробка математичних та програмних моделей та методики перевірки правильності програмної реалізації криптографічного перетворення включаючи режими застосування та еталонні копії для перевірки правильності реалізації.

3. Ціль та задачі дослідження

Метою дослідження є розробка математичних та програмних моделей перспективного алгоритму шифрування, обґрунтування методики перевірки правильності програмної реалізації криптографічного перетворення включаючи режими застосування та еталонні копії.

Для досягнення поставленої мети в роботі вирішувалися наступні задачі:

– розробка та використання методики перевірки правильності реалізації БСШ «Калина» у відповідних режимах роботи;

– створення еталонної програмної реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування;

– реалізація тестових прикладів БСШ «Калина» у відповідних режимах роботи;

– розробка незалежних програмних реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування для перевірки правильності реалізації шляхом багатоверсійної розробки.

4. Матеріали та методи досліджень

4. 1. Призначення та структура методики перевірки правильності реалізації блокового симетричного криптоперетворення

Методика перевірки правильності реалізації БСШ «Калина» визначає вимоги до перевірки правильності програмної реалізації основних процедур, визначених у перспективному проекті національного стандарту

блокового симетричного криптографічного перетворення.

Криптографічний алгоритм симетричного блокового перетворення використовує базове перетворення як основний елемент при забезпеченні конфіденційності та (або) цілісності. Базове перетворення реалізує пряме перетворення (зашифрування) та обернене перетворення (розшифрування). Базове перетворення зашифрування $T_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням $T_{l,k}^{(K)}: V_l \to V_l$, $K \in V_k$, $l,k \in \{128,256,512\}$ при цьому $k = l$ або $k = 2 \cdot l$, що реалізоване у вигляді ітеративного застосування низки функцій, які обробляють вхідний аргумент $x \in V_l$ як матрицю внутрішнього стану розміром $8 \times c$ байтів, що містить елементи поля $GF(2^8)$. Базове перетворення розшифрування $U_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням, оберненим до $T_{l,k}^{(K)}$, також реалізованим у вигляді ітеративного перетворення. Залежність кількості ітерацій (t) при реалізації перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$, кількості стовпців матриці внутрішнього стану (c) від розміру блоку (l) і довжини ключа шифрування (k) наведено у табл. 1.

Режими роботи криптографічного алгоритму, визначеного в проекті перспективного національного стандарту, їх позначення та послуги безпеки, які забезпечує відповідний режим, визначені у табл. 2

Режим простої заміни є компонентом усіх інших режимів роботи криптографічного алгоритму симетричного блокового перетворення. Без додаткових перетворень, визначених іншими режимами, використання простої заміни для захисту повідомлень не рекомендується.

Таблиця 1

Основні параметри базового перетворення БСШ «Калина»

№ з/п	Розмір блоку (l)	Довжина ключа (k)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

Режим роботи криптографічного алгоритму, визначеного у проекті перспективного національного стандарту, позначається наступним чином: «Калина-l/k-позначення режиму-параметри режиму» (для деяких режимів параметри відсутні), де l – розмір блоку базового перетворення, k – довжина ключа.

Наприклад, Калина-256/512-CCM-32,128 визначає використання базового перетворення з розміром блоку 256 бітів, довжиною ключа 512 бітів, застосування у режимі вироблення імітовставки і гамування, довжина конфіденційної (та відкритої) частини повідомлення завжди менша 2^{32} байтів, довжина імітовставки дорівнює 128 бітам.

Режим простої заміни збігається з базовим перетворенням, тому крім позначення «Калина-l/k-ECB» може використовуватись позначення «Калина-l/k».

Методика перевірки правильності реалізації блокового симетричного криптографічного перетворення складається з наступних частин:

1) перевірка виконання загальних вимог до реалізації криптографічного перетворення;

2) перевірка правильності реалізації базових процедур, визначених у БСШ «Калина» (функції розгортання циклових ключів та базових перетворень зашифрування і розшифрування) за допомогою тестових прикладів;

3) перевірка правильності реалізації режимів роботи, визначених визначених у БСШ «Калина» (гамування (CTR); гамування зі зворотнім зв'язком за шифр текстом (CFB); вироблення імітовставки (CMAC); зчеплення шифрблоків (CBC); гамування зі зворотнім зв'язком за шифр гамою (OFB); вибіркове гамування із прискореним виробленням імітовставки (GCM, GMAC); вироблення імітовставки і гамування (CCM); індексованої заміни (XTS); захисту ключових даних (KW)) за допомогою тестових прикладів.

Таблиця 2

Назва, позначення та послуги безпеки режимів застосування БСШ «Калина»

№ режиму	Назва режиму	Позначення	Послуга безпеки
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотнім зв'язком за шифртекстом	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифрблоків	CBC	Конфіденційність
6	Гамування зі зворотнім зв'язком за шифргамою	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	цілісність і конфіденційність
9	Індексованої заміни	XTS	конфіденційність
10	Захисту ключових даних	KW	конфіденційність і цілісність

Набори тестових векторів складені відповідно до відомостей, наведених безпосередньо в проекті перспективного національного стандарту, а також з урахуванням необхідності забезпечення повноти тестування, виходячи з особливостей структури алгоритму БСШ «Калина».

4. 2. Перевірка виконання загальних вимог до криптографічних модулів

Для проведення перевірки правильності реалізації БСШ «Калина» за розробленою методикою повинні бути представлені:

– еталонна програмна модель БСШ «Калина» у відповідних режимах роботи;

– тестові приклади БСШ «Калина» у відповідних режимах роботи;

Програмні модулі та додаткове програмне забезпечення повинне надаватися у вигляді інсталяційних пакетів на носіях інформації.

Супроводжувальна документація повинна бути надана у твердій копії (надрукована) та у вигляді електронних документів на носієві інформації.

Під час перевірки виконання загальних вимог програмних модулів, що реалізують алгоритм симетричного блокового криптоперетворення та режими його застосування виконується:

1) перевірка наявності та відповідності вимогам програмної документації на програмні модулі;

2) перевірка наявності, відповідності вимогам та працездатності додаткового програмного забезпечення;

3) перевірка наявності, відповідності вимогам та працездатності програмних модулів.

Перевірка відповідності вимогам та працездатності додаткового програмного забезпечення виконується шляхом інсталяції програмного забезпечення в ОС, підключенням та завантаженням програмного забезпечення і перевірки коректності функціонування.

Дана перевірка також включає:

– перевірку відповідності програмних модулів вимогам технічних завдань та зазначеним апаратним платформам і ОС (середовищу експлуатації);

– перевірку програмних (інтерфейсів бібліотек);

– перевірку вихідних кодів програмних модулів (окремих або складових частин).

4. 3. Перевірка правильності реалізації за допомогою тестових прикладів

Перевірка правильності реалізації симетричного блокового криптоперетворення та режимів його застосування за допомогою тестових прикладів виконується шляхом тестування з використанням програмного модуля.

Перевірка правильності реалізації включає:

1) перевірку правильності реалізації базових процедур, визначених у проекті перспективного (функції розгортання циклових ключів та базових перетворень зашифрування і розшифрування) за допомогою тестових прикладів;

2) перевірку правильності реалізації режимів застосування, визначених у проекті перспективного національного стандарту (режими гамування (CTR); гамування зі зворотнім зв'язком за шифр текстом (CFB); вироблення імітовставки (CMAC); зчеплення шифрблоків (CBC); гамування зі зворотнім зв'язком за шифр гамою (OFB); вибіркове гамування із прие скореним виробленням імітовставки (GCM, GMAC); вироблення імітовставки і гамування (CCM); індексованої заміни (XTS); захисту ключових даних (KW)) за допомогою тестових прикладів.

Перевірка виконується послідовно – спочатку базових процедур, а потім режимів застосування алгоритму симетричного блокового криптоперетворення. Реалізація вважається перевіреною, якщо пройдене тестування базових процедур та всіх реалізованих режимів роботи алгоритму.

Перевірка реалізації базових перетворень та режимів роботи алгоритму здійснюється для різних довжин ключів: 128, 256 або 512 бітів. А також для різних довжин блоків: 128, 256 або 512 бітів.

5. Результати перевірки правильності реалізації перспективного алгоритму шифрування «Калина»

Для вирішення завдань перевірки правильності реалізації криптографічного блокового симетричного перетворення було використано багатоверсійний підхід (рознесена розробка), який передбачає створення двох або більше компонентів програмного забезпечення для реалізації однієї і тієї ж функції способами, що виключають джерела загальних помилок у кількох компонентах. Багатоверсійність реалізована шляхом незалежної рознесеної програмної реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування на високорівневих мовах Java та Python.

В ході дослідження було розроблено тестові вектори для розгортання ключа у циклові ключі, для функцій за шифрування, разшифрування та/або імітовставки (де це використовується) для всіх режимів роботи: проста заміна (ECB); гамування (CTR); гамування зі зворотнім зв'язком за шифр текстом (CFB); вироблення імітовставки (CMAC); зчеплення шифрблоків (CBC); гамування зі зворотнім зв'язком за шифр гамою (OFB); вибіркове гамування із прискореним виробленням імітовставки (GCM, GMAC); вироблення імітовставки і гамування (CCM); індексованої заміни (XTS); захисту ключових даних (KW)) за допомогою тестових прикладів. При створенні тестових векторів були враховані все розміри блоку та ключа шифрування, можливість шифрування неповних блоків, до яких використовується функція доповнення блока, різні розміри параметрів, таких як розмір імітовставки (CMAC, GMAC, CCM) та режим гамування у CFB.

В результаті проведеної роботи тестові вектори мають наступний вигляд.

На початку описується режим використання БСШ «Калина» з вхідними параметрами, наприклад: «Перетворення $N_Б = 4$, $q = 128$ (Калина-128/128-CCM-32,128)». Тут вказується розмір блоку, ключа та, при наявності, інші параметри, наприклад, розмір імітовставки.

Далі йде перелік функцій, до яких належать вектори, наприклад, «Вироблення імітовставки для відкритої та конфіденційної частини повідомлення».

Наступними описуються вхідні дані у hex (шістнадцятковому) форматі, наприклад:

KEY:
000102030405060708090A0B0C0D0E0F
IV:
101112131415161718191A1B1C1D1E1F
AUTHTEXT:
202122232425262728292A2B2C2D2E2F
PLAINTEXT (N = 128):
303132333435363738393A3B3C3D3E3F;

та детально описується проміжний внутрішній стан та інші змінні перетворення на кожному кроці алгоритму для кожної функції режиму:

G1:
101112131415161718191A10000000B3
lambda_0:
10000000
b [1]:
0C5EC98C81929257F2CA491219D8924E
...
h:
26A936173A4DC9160D6E3FDA3A974060.

В наведеному прикладі спершу було розраховано значення імітовставки (h), після чого починається обчислення шифртексту:

Пряме перетворення
KEY:
000102030405060708090A0B0C0D0E0F
IV:
101112131415161718191A1B1C1D1E1F
PLAINTEXT (N = 128):
303132333435363738393A3B3C3D3E3F
h:
26A936173A4DC9160D6E3FDA3A974060
...
CIPHERTEXT:
B91A7B8790BBCFCFE65D04E5538E98E2
704454C9DD39ADACE0B19D03F6AAB07E
Зворотне перетворення
KEY:
000102030405060708090A0B0C0D0E0F
IV:
101112131415161718191A1B1C1D1E1F
AUTHTEXT:
202122232425262728292A2B2C2D2E2F
CIPHERTEXT (N = 256):
B91A7B8790BBCFCFE65D04E5538E98E2
704454C9DD39ADACE0B19D03F6AAB07E
...
PLAINTEXT:
303132333435363738393A3B3C3D3E3F
26A936173A4DC9160D6E3FDA3A974060
h:
26A936173A4DC9160D6E3FDA3A974060
RETURNED_PLAINTEXT:
303132333435363738393A3B3C3D3E3F.

Такий самий або ідентичний набір даних отримується для базових функцій (розгортання циклових ключів) та всіх режимів роботи алгоритму і вважається еталонним.

При наявності еталонних тестових векторів розробник має можливість перевірити правильність реалізації алгоритму та його режимів.

Перевірка правильності реалізації функції розгортання циклових ключів має наступний або ідентичний набір кроків:

1. Вхідними даними до функції перетворення є:
– ключі довжиною 128, 256 та 512 біт.

2. Перевіряються наступні вихідні дані після виконання функції перетворення:
– циклові ключі шифрування;
– циклові ключі розшифрування (якщо базове перетворення розшифрування реалізоване у альтернативному представлені).

Реалізація вважається такою, що пройшла тестування, якщо всі вихідні значення, отримані в процесі виконання тесту, співпали з еталонними (очікуваними).

Перевірка правильності реалізації базових перетворень зашифрування і розшифрування має наступний або ідентичний набір кроків:

1. Вхідними даними до функції перетворення є:
– ключі довжиною 128, 256 та 512 біт;
– блоки відкритого (зашифрованого) тексту.

2. Перевіряються наступні вихідні дані після виконання функції перетворення:
– блоки зашифрованого (відкритого) тексту.

Реалізація вважається такою, що пройшла тестування, якщо всі вихідні значення, отримані в процесі виконання тесту, співпали з еталонними (очікуваними).

Перевірка правильності реалізації режимів застосування БСШ за шифрування/розшифрування/імітовставка має наступний або ідентичний набір кроків:

1. Вхідними даними до функції перетворення є:
– ключі довжиною 128, 256 та 512 біт;
– блоки відкритого (зашифрованого) тексту;
– значення лічільника (для режимів CTR, CCM, XTS);
– синхропосилка (для режимів CTR, CFB, CBC, OFB, GCM/GMAC, CCM, XTS).

2. Перевіряються наступні вихідні дані після виконання функції перетворення:
– блоки зашифрованого (відкритого) тексту;
– імітовставка (для режимів CMAC, GCM/GMAC).

Реалізація вважається такою, що пройшла тестування, якщо всі вихідні значення, отримані в процесі виконання тесту, співпали з еталонними (очікуваними).

Для перевірки правильності реалізації можливо використання вбудованих засобів порівняння даних у язиках програмування, наприклад memcmp, або, при необхідності, реалізовані самостійно. Також тестові вектори можливо використовувати для перевірки правильності роботи програмного, програмно-апаратного чи апаратного засобу криптографічного перетворення, наприклад розраховуючи необхідні вектори та порівнюючи їх з еталонними при увімкнені та/або під час роботи при необхідності, або автоматизовано через певний проміжок часу тощо.

6. Обговорення результатів дослідження

Під час проведення досліджень математичних та програмних моделей перспективного алгоритму шифрування «Калина» обґрунтовано методику перевірки правильності програмної реалізації криптографічного перетворення включаючи режими застосування та еталонні копії. Розроблена методика визначає певні вимоги до перевірки правильності програмної реалізації основних процедур, визначених у специфікації БСШ «Калина». Крім того, запропонована методика включає відповідні процедури та визначені набори тестових векторів для перевірки правильності реалізації алгоритму симетричного блокового криптографічного перетворення різних режимів застосування БСШ.

Для перевірки правильності реалізації було використано багатоверсійний підхід (рознесена розробка), який передбачає створення двох або більше компонентів програмного забезпечення для реалізації однієї і тієї ж функції способами, що виключають джерела загальних помилок у кількох компонентах. Багатоверсійність реалізована шляхом незалежної рознесеної програмної реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування на високорівневих мовах Java та Python.

7. Висновки

1. Для забезпечення взаємної сумісності результатів криптоперетворень у засобах КЗІ різних виробників, з метою забезпечення інформаційної безпеки України Адміністрацією Держспецзв'язку забезпечено розроблення вітчизняного криптографічного алгоритму симетричного блокового перетворення. Запропонований перспективний криптографічний алгоритм «Калина» передбачає можливість одночасного забезпечення конфіденційності та цілісності повідомлення шляхом послідовного застосування відповідних перетворень.

2. Впровадження нового стандарту при реалізації механізмів безпеки спрямоване на вирішення завдань із застосування криптографічного алгоритму симетричного блокового перетворення, а саме:

– забезпечення конфіденційності інформації та повідомлень на усіх етапах їх життєвого циклу;

– забезпечення цілісності інформації та повідомлень на усіх етапах їх життєвого циклу;

– шифрування інформації в інформаційно-телекомунікаційних системах в різних (десяти) режимах роботи у залежності від вимог що висуваються;

– генерація псевдовипадкових послідовностей;

– криптографічні протоколи автентифікації, встановлення таємниці та ключів, узгодження таємниці та ключів, розподілу таємниці тощо, коли висуваються складні вимоги до складності (швидкодії);

– криптографічні протоколи електронного цифрового підпису тощо.

2. В якості основних режимів роботи, визначені специфікацією алгоритму, визначаються такі:

– простої заміни (базове перетворення) (ECB);

– гамування (CTR);

– гамування зі зворотнім зв'язком за шифр текстом (CFB);

– вироблення імітовставки (CMAC);

– зчеплення шифр блоків (CBC);

– гамування зі зворотнім зв'язком за шифр гамою (OFB);

– вибіркового гамування із прискореним виробленням імітовставки (GCM, GMAC);

– вироблення імітовставки і гамування (CCM);

– індексованої заміни (XTS);

– захисту ключових даних (KW).

3. Для вирішення завдань перевірки правильності реалізації нового БСШ «Калина» були розроблені:

– методика перевірки правильності реалізації БСШ «Калина» у відповідних режимах роботи;

– еталонна програмна реалізація базових перетворень БСШ «Калина» та відповідних режимів застосування;

– тестові приклади БСШ «Калина» у відповідних режимах роботи;

– незалежні програмні реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування для перевірки правильності реалізації.

4. Еталонну програмну реалізацію базових перетворень БСШ «Калина» та відповідних режимів застосування було розроблено із використанням високорівневої мови програмування С. Для перевірки правильності реалізації було застосовано багатоверсійний підхід (рознесена розробка), який передбачає створення двох або більше компонентів програмного забезпечення для реалізації однієї і тієї ж функції способами, що виключають джерела загальних помилок у кількох компонентах. Багатоверсійність реалізована шляхом незалежної рознесеної програмної реалізації базових перетворень БСШ «Калина» та відповідних режимів застосування на високорівневих мовах Java та Python.

Література

1. Указ Президента України «Про положення про порядок здійснення криптографічного захисту інформації в Україні» від 22.05.98 № 505/98 [Текст] / Л. Д. Кучма, 1998.
2. Указ Президента України «Про Доктрину інформаційної безпеки України» від 08.07.2009 № 514 [Текст] / В. А. Ющенко, 2009.
3. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV [Текст] / Верховна Рада України, 2003.
4. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Текст] / Верховна Рада України, 1992.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [Текст] / Верховна Рада України, 1994.
6. Закон України «Про Національну систему конфіденційного зв'язку» від 10.01.2002 № 2919-III [Текст] / Верховна Рада України, 2002.
7. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації від 30.07.2007 р. № 862/14129 [Текст] / Державна служба спеціального зв'язку та захисту інформації України, 2007.
8. Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100 зареєстроване в Міністерстві юстиції України 16 липня 2008 р. за № 651/15342 [Текст] / Державна служба спеціального зв'язку та захисту інформації України, 2008.
9. ДСТУ. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. - Проект стандарту друга (остаточна) редакція. – Харків: АТ «ІІТ», 2014. - 238 с.
10. Розробка нового блокового симетричного шифру [Текст]: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІІТ»; кер. І.Д. Горбенко – Харків, 2014, Том 4. – 304 с.
11. Горбенко, І. Д. Прикладна криптологія [Текст] : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків, ХНУРЕ, Форт, 2012. – 868 с.
12. Есин, В. І. Безпека інформаційних систем і технологій [Текст] / В. І. Есин, О. О. Кузнецов, Л. С. Сорока. – Харків, ХНУ ім. В.Н. Каразіна, 2013. – 632 с.

13. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. [Текст] / Б. Шнайер. – М.: «Триумф», 2002. – 797.
14. Menezes, A. J. Handbook of Applied Cryptography [Text] / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – CRC Press, 1997. – 794. doi: http://dx.doi.org/10.5860/choice.34-4512
15. Daemen, J. Annex to AES Proposal Rijndael [elEctronic resource] / J. Daemen, V. Rijmen. –National Institute of Standards and Technology. – Available at: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf – 9.04.2003.
16. Biham, E. Differential Cryptanalysis of the Data Encryption Standard [Текст] / E. Biham, A. Shamir. – SpringeriVerlag, New York, 1993. – 77 p. doi: http://dx.doi.org/10.1007/978-1-4613-9314-6_4
17. Matsui, M. Linear Cryptanalysis Method for DES Cipher [Text] / M. Matsui. – EUROCRYPT'93, 1993. – P. W112-W123. doi: http://dx.doi.org/10.1007/3-540-48285-7_33
18. Knudsen, L. R. Integral Cryptanalysis, NESSIE internal report [Electronic resource] / L. R. Knudsen. – New European Schemes for Signatures, Integrity, and Encryption. – Available at: https://www.cosic.esat.kuleuven.be/nessie/reports/phase2/uibwp5-015-1.pdf, 2001
19. NESSIE security report [Electronic resource] / New European Schemes for Signatures, Integrity, and Encryption. – Available at: https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf, 2003
20. AES discussion forum [Electronic resource] / Available at: http://aes. nist. gov.
21. Долгов, В. И. Блочные симметричные шифры. Методология оценки стойкости к атакам дифференциального и линейного криптоанализа [Текст]: монографія / В. И. Долгов, И. В. Лисицкая. – Харков, ХНУРЭ, Форт, 2013. – 455 с.
22. Горбенко, И. Д. Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования [Текст] / И. Д. Горбенко, В. И. Долгов, Р. В. Олейников, В. И. Руженцев, М. С. Михайленко, Ю. И. Горбенко // Известия ЮФУ. Технические науки. – 2007. – № 1 (76). – С. 238–241.
23. Горбенко, И. Д. Принципы построения и свойства блочного симметричного шифра «Калина» [Текст] / И. Д. Горбенко, В. И. Долгов, Р. В. Олейников, В. И. Руженцев, М. С. Михайленко, Ю. И. Горбенко, А. В. Нейванов // Прикладная радиоэлектроника. – 2007. – № 2.
24. Горбенко, И. Д. Криптостойкость шифра «Калина» [Текст] / И. Д. Горбенко, В. И. Долгов, Р. В. Олейников, В. И. Руженцев, М. С. Михайленко, Ю. И. Горбенко, С. В. Чичмарь // Прикладная радиоэлектроника. – 2007. – № 2.
25. Долгов, В. И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс [Текст] / В. И. Долгов, А. А. Кузнецов, С. А. Исаев. // Электронное моделирование. – 2011. – Т. 33, № 6. – С. 81–99.
26. Кузнецов, А. А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс [Текст] / А. А. Кузнецов, И. В. Лисицкая, С. А. Исаев // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 135–140.
27. Лисицкая, И. В. Большие шифры – случайные подстановки. [Текст] / И. В. Лисицкая, А. А. Настенко // Межведомственный научн. технический сборник «Радиотехника». – 2011. – Вып. 166. – С. 50–55.