МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МОРДВІНОВ РУСЛАН ІГОРОВИЧ

УДК 004.056.55

МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ДОСЛІДЖЕННЯ РЕЖИМІВ РОБОТИ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ПО КРИТЕРІЯМ СТІЙКІСТЬ – СКЛАДНІСТЬ

05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2015

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України, м. Харків.

Науковий керівник: доктор технічних наук, професор,
Горбенко Іван Дмитрович
професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Міністерство освіти і науки України, м. Харків.

Офіційні опоненти: доктор технічних наук, професор
Толюпа Сергій Васильович,
директор інституту захисту інформації, Міністерство освіти і науки України, м. Київ;

кандидат технічних наук, доцент,
Неласа Ганна Вікторівна,
доцент кафедри програмних засобів Запорізького національного технічного університету, Міністерство освіти і науки України, м. Запоріжжя.

Захист відбудеться "__" _____ 2015 р. о __-__ годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розіслано "___" _____ 2015 р.

Вчений секретар

спеціалізованої вченої ради І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Останні події у світі чітко показують, що необхідність протидії порушникам та спробам ведення інформаційної боротьби є все більш важливою у сучасному інформаційному світі. Для захисту інформації необхідним є використання криптографічних методів захисту, які дозволяють отримати високий рівень безпеки та основні послуги – конфіденційність, цілісність, захист від НСД, доступність, неспростовність тощо, забезпечуючи при цьому криптографічну стійкість, цілісність, швидкодію криптографічних перетворень та певні вимоги, які висуваються додатками.

В ході використання сучасних методів передачі інформації, швидкість яких вже досягає десятків гігабіт за секунду, критерій швидкодії переходить в стан безумовної вимоги, забезпеченість якої постає в один рядок з криптографічною стійкістю. Насамперед це актуально для таких криптоперетворень, як блоковий симетричний шифр, що є основним засобом забезпечення конфіденційності інформації.

Сьогодні в Україні для здійснення швидкісного симетричного шифрування в основному використовується ДСТУ ГОСТ 28147:2009, який, за показниками стійкості, відповідає тільки задовільному рівню, а за швидкодією він уступає перспективним шифрам в 2 або більше разів. Зазначений стандарт використовується на регіональному рівні, але деякі держави, наприклад Російська Федерація та Білорусь практично відмовились від його використання – Білорусь ввела новий стандарт, а РФ опублікувала проект БСШ.

У цих умовах особливо важливою проблемою для України є прийняття національного стандарту БСШ, який відповідав би найвищим сучасним вимогам відносно рівня безпеки та міг би застосовуватися практично у всіх необхідних режимах роботи. Тому дана дисертаційна робота, що присвячена розробці моделей, методів і засобів дослідження властивостей нового стандарту ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» (у подальшому «Калина») в режимах його використання з оптимізацією їх за критеріями стійкості та швидкодії слід вважати надзвичайно актуальною та своєчасною.

Тема дисертаційної роботи спрямована на розробку математичних моделей, методів і засобів дослідження властивостей БСШ та режимів його застосування за критеріями стійкості та швидкодії.

Зв'язок роботи з науковими програмами, темами. Дисертаційна робота виконана в рамках: держбюджетної НДР № 262-1 "Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП, на національному та міжнародному рівнях" за наказом МОНУ № 1177 від 30.11.2010 р. (ДР № 0111U002628); госпдоговірної НДР № 11-06 "Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій" (ДР №.0111U002634), держбюджетної НДР № 275-1 "Аналіз стану, визначення напрямів розвитку, стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП"

(ДР № 0113U000363), у розробці яких автор брав участь як виконавець.

Мета і задачі дослідження. *Метою дисертаційної роботи є* розробка моделей, методів і засобів дослідження властивостей нового алгоритму БСП «Калина» в режимах його використання з оптимізацією їх за критеріями стійкості і швидкодії.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- побудова математичних моделей нового алгоритму БСШ і режимів його застосування;
- розробити та обґрунтувати практичні рекомендації щодо специфікації режимів застосування БСШ;
- обґрунтування і побудова вдосконаленого методу оцінки ефективності генераторів ПВП;
- розробити та експериментально дослідити і перевірити програмні моделі ДГВП на основі нового БСШ;
- обґрунтувати режими роботи (застосування) в новому алгоритмі БСШ на національному рівні та дослідити статистичні властивості гами шифрування.

Об'єкт досліджень – процеси блокового симетричного шифрування інформації у визначених стандартом режимах роботи з використанням нового алгоритму БСП «Калина» в умовах обмежень на його характеристики, властивості та умови застосування.

Предмет досліджень – методи та моделі аналізу властивостей і характеристик нового алгоритму БСП «Калина» та режимів його застосування.

Методи досліджень ґрунтуються на теорії чисел, теорії полів Галуа, теорії обробки результатів, теорії ймовірності, теорії похибок, математичній статистиці, методах математичного та імітаційного моделювання, комп'ютерному моделюванні з використанням високорівневої мови програмування С.

Наукова новизна отриманих результатів полягає в тому, що:

1. Отримала подальший розвиток математична модель базового криптографічного перетворення алгоритму блокового симетричного перетворення «Калина», яка відрізняється від існуючої тим, що має оптимізований з точки зору використання передобчислень порядок та спосіб застосування основних елементів алгоритму, що дозволяє значно прискорити швидкодію основного криптографічного перетворення алгоритму «Калина».

2. Отримали подальший розвиток режими застосування блокових симетричних шифрів, які відрізняються від відомих урахуванням теоретично обґрунтованих обмежень на кількість викликів функції шифрування, сумарну довжину повідомлень, які захищаються з використанням одного ключа, значень певних констант та внутрішніх станів, зміненими процедурами обробки вихідних даних та проміжних значень, що дозволяє застосовувати нові режими шифрування для різних довжин блоків відкритого тексту та ключових даних у шифросистемах високої та надвисокої стійкості.

3. Удосконалено метод статистичного тестування генераторів ПВП, який

відрізняється від відомих урахуванням похибок у результатах досліджень окремих вихідних послідовностей, що дозволяє із заданою точністю та достовірністю оцінювати показники статистичної безпеки досліджуваного генератора. Зокрема встановлено, що функціонування генератора ПВП, який побудовано із використаним різних режимів застосування нового алгоритму блокового симетричного перетворення «Калина», описується випадковим стаціонарним ергодичним процесом.

Практичне значення отриманих результатів.

1. Розроблено програмну реалізацію базового криптографічного перетворення нового алгоритму блокового симетричного перетворення «Калина». Встановлено, що за показниками швидкодії та ресурсомісткості розроблений криптоалгоритм володіє покращеними властивостями, зокрема:

– на 64-й платформі intel операційної системи Windows 7 x64 швидше за ГОСТ до 335% та до 7 % за американський стандарт шифрування AES;

– на 64-й платформі intel операційної системи ubuntu 14.10 LTS x64 швидше за ГОСТ до 291% та до 6 % за американський стандарт шифрування AES.

2. Розроблено програмну реалізацію різних режимів застосування нового алгоритму блокового симетричного перетворення «Калина». Зокрема були перероблені окремі режими застосування для можливості застосовуватися з блоковими симетричними перетвореннями високої та надвисокої стійкості.

3. Вперше отримано результати дослідження статистичної безпеки нового алгоритму блокового симетричного перетворення «Калина» у різних режимах застосування. Зокрема встановлено, що БСП «Калина» при будь-якому встановленому режимі генерує псевдовипадкові послідовності, тобто з високою вірогідністю і точністю можна стверджувати, що досліджуваний алгоритм блокового симетричного криптоперетворення буде статистично безпечним у будь-якому практичному застосуванні.

4. Отримано оцінки статистичної безпеки БСШ AES (FIPS-197) та ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009) в ході використання різних режимів застосування, проведено порівняні дослідження із БСП «Калина». Результати порівняльного аналізу свідчать про високі показники статистичної безпеки всіх досліджуваних шифрів, практично кожний криптоалгоритм може розглядатися як генератор псевдовипадкових послідовностей, робота якого гарно апроксимується випадковим процесом. Відмічається незначна перевага БСП «Калина», бо мінімальне значення числа пройдених статистичних тестів у БСП «Калина» є найвищим серед досліджуваних криптоалгоритмів.

5. За результатами порівняльних досліджень обґрунтовано практичні рекомендації щодо режимів застосування БСП «Калина» у різних криптографічних додатках. Загальну сумарну довжину повідомлень, які захищаються з використанням одного ключа, кількість викликів функції шифрування рекомендується обмежити в залежності від розміру блоку базового перетворення.

Основні результати досліджень впроваджені Приватним акціонерним товариством «Інститут інформаційних технологій», у Харківському національному університеті радіоелектроніки та у Харківському національному університеті імені В.Н. Каразіна, що підтверджується відповідними актами.

Достовірність і обґрунтованість отриманих наукових результатів підтверджуються: математичною коректністю введених моделей; несуперечливістю з відомими результатами теорії чисел, теорії полів Галуа, теорій ймовірності, математичної статистики; несуперечливістю з результатами, отриманими в приватних теоріях та їх збігом з відомими чи отриманими експериментально.

Особистий внесок здобувача. Нові наукові результати отримано здобувачем особисто. У роботах, виконаних у співавторстві, здобувачу належать такі результати: в [1] проведено аналіз та класифікацію методів генерування псевдовипадкових послідовностей; в [2] реалізовано перевірку теоретичних результатів за допомогою створення імітаційної моделі ДГВП; в [3] надано опис та результати тестування детермінованих генераторів на основі ґеш-функцій та БСШ; в [4] надано опис та аналіз вимог до випадкових послідовностей та їх тестування; в [6] розроблено метод статистичного дослідження та отримано результати тестування режимів БСП; в [7] розроблено реалізацію режимів БСП та методики верифікації.

Апробація результатів дисертації. Основні результати роботи представлені та обговорювалися на таких науково-технічних конференціях: науково-технічна конференція з міжнародною участю «Наукові дослідження молоді - вирішенню проблем європейської інтеграції». 7 квітня 2011р. – м. Харків [8]; 15-й, 16-й Ювілейний Міжнародний молодіжний форум «Радиоэлектроника и молодежь в XXI веке». – м. Харків [9,12]; II-га Міжнародна науково-технічна конференція «Компьютерные науки и технологии». 3-5 жовтня 2011р. – Бєлгород, РФ [10]; Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями». 2 грудня 2011р. – м. Дніпропетровськ [11]; Науково-технічна конференція із міжнародною участю «Комп'ютерне моделювання в наукоємних технологіях» (КМНТ-2012). 24-27 квітня 2012р. – м. Харків [13]; XV-та, XVI-та Міжнародна науково-практична конференція «Безопасность информации в информационно-телекоммуникационных системах». – м. Київ [14,15,17,18]; II-га Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем». 30 травня – 01 червня 2013р. – м. Львів [16]; Міжнародна наукова конференція «Питання оптимізації обчислень (ПОО-XL)», присвячена 90-річчю від дня народження академіка В.М. Глушкова, 30 вересня – 4 жовтня 2013р. – м. Київ [19].

Публікації. Основні наукові результати за темою дисертації опубліковані в семи статтях у періодичних виданнях, які входять до переліку фахових видань України, стаття [7] опублікована в журналі «Восточно-европейский журнал передовых технологий», який включено до міжнародних науково-метричних

баз Ulrich's Periodicals Directory, Bielefeld Academic Search Engine (BASE), Index Copernicus, Directory of Open Access Journals, EBSCO, CrossRef , видано 12 тез доповідей на наукових конференціях.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, п’яти розділів, висновків, списку використаних джерел та 2 додатків. Повний обсяг дисертації складає 168 сторінок. Основний обсяг дисертації міститься на 150 сторінці та має 7 ілюстрацій за текстом, 20 таблиць за текстом, у тому числі 7 ілюстрацій на 7 сторінках, 2 додатки на 10 сторінках, список використаних джерел із 80 найменувань на 9 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовані об’єкт, предмет, мета та задачі дослідження, описано наукову новизну та практичне значення отриманих результатів, показано зв’язок дисертаційної роботи з науково-дослідницькими роботами, визначено особистий внесок автора в друкованих публікаціях і впровадження основних результатів роботи.

У першому розділі проаналізовано та обґрунтовано вибір методів для тестування статистичних властивостей послідовностей. Після порівняння основних міжнародних практик тестування випадкових послідовностей, таких як FIPS-PUB-140, AIS20, AIS31, NIST 800-22 та NIST 800-90 було вирішено, що основним критерієм, який висувається для оцінки послідовності є повнота аналізу. Тому за основу було обрано набір тестів з NIST 800-22, тому що він найбільш повно охоплює найпоширеніші статистичні тести, які існують сьогодні.

Також обрано ряд режимів роботи, які використовуватимуться та мають пройти аналіз з подальшою розробкою пропозицій щодо виду використання режиму. До цих режимів відносяться ECB, CTR, CFB, CBC, OFB, CMAC, GCM/GMAC, CCM, KW, XTS згідно з NIST 800-38 A-F.

Крім того описано критерії та показники оцінки, які висуваються до випадкових послідовностей.

До основних безумовних критеріїв можна віднести такі:

– надійність математичної бази;
– практична захищеність від відомих атак;
– реальна захищеність від усіх відомих та потенційно можливих крипто-аналітичних атак;
– статистична безпечність;
– непередбачуваність ПВП (вперед і назад);
– відсутність слабких таємних (особистих) ключів;
– складність генерування носить не вище за поліноміальний характер.

Кількісна оцінка генераторів може бути зроблена з використанням таких показників, як:

– складність обернення ПВП, тобто знаходження початкового значення (ключа), що використовується;

– ентропія джерела ключів $H_к$, у тому числі для випадку, коли ДГВП використовується як джерело ключів;

– період l_n (довжина) повторення ПВП та безпечний час t_b;

– основа алфавіту m послідовності, що генерується;

– ймовірність перекриття в просторі або в часі двох сегментів бітів Y_r та Y_μ, тобто в різних абонентів або в одного абонента протягом часу, так, що $Y_r = Y_\mu$;

– відстань рівнозначності l_0 конкретної послідовності бітів Y_υ;

– просторова I_n та часова складності $I_ч$ формування послідовності бітів Y тощо.

У другому розділі надано критерії, показники оцінки та вимоги до сучасних БСШ. До безумовних критеріїв можна віднести такі, як:

- захищеність від усіх відомих та потенційно можливих криптоаналітичних атак;
- статистична безпечність алгоритму шифрування;
- надійність математичної бази;
- практична захищеність алгоритму шифрування від силових атак;
- для блокового симетричного шифру з повним числом циклів криптографічного перетворення не існують або невідомі теоретичні аналітичні атаки, складність яких менше, ніж складність типу груба сила;
- відсутність слабких початкових ключів та підозр на існування ключів, за яких складність криптоаналітичної атаки є меншою ніж, складність атаки груба сила;
- складність $I_{пр}$ прямого та складність $I_{зв}$ зворотного перетворень не перевищують допустимої величини $I_д$.

Як умовні критерії пропонується використовувати такі:

- реальна захищеність від відомих криптоатак при зменшеному числі циклів ітеративного шифрування;
- оцінка тимчасової складності програмної, апаратної, програмно-апаратної реалізації;
- оцінка просторової складності програмної, апаратної, програмно-апаратної реалізації.

Для оцінки статистичної безпеки БСШ візьмемо підхід, який використовується для тестування випадкових послідовностей, де як випадкова послідовність будуть шифротексти БСШ. Для цього пропонується використовувати методику NIST STS. Але NIST STS надає оцінку тільки для конкретної послідовності, а не для джерела цієї послідовності. Тому було розроблено метод, що дозволяє із заданою імовірністю та вірогідністю отримати оцінки для джерела послідовності.

Для забезпечення заданої достовірності результатів статистичного тестування пропонується оцінювати математичне сподівання числа пройдених тестів досліджуваним криптоалгоритмом. Оцінкою для математичного

сподівання m випадкової величини X є середнє арифметичне її спостережуваних значень (або статистичне середнє):

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i ,$$

де N – кількість реалізацій випадкової величини X.

Оцінка дисперсії випадкової величини X визначається виразом

$$\tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N} (X_i - \tilde{m})^2 .$$

Беручи припущення про незалежність результатів статистичного тестування і достатню їхню кількість, при великих значеннях кількості реалізацій N середнє арифметичне $\tilde{m}$ випадкової величини X матиме розподіл, близький до нормального з математичним очікуванням

$$m[\tilde{m}] \approx m$$

і середньоквадратичним відхиленням

$$\sigma[\tilde{m}] \approx \frac{\sigma}{\sqrt{N}},$$

де σ – середньоквадратичне відхилення оцінюваного параметра.

При цьому імовірність того, що оцінка $\tilde{m}$ відхилиться від свого математичного очікування менше, ніж на ε (довірча ймовірність), дорівнює

$$P_д(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right),$$

де $\Phi(x)$ – функція Лапласа, що визначається виразом

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}} dt .$$

Величина ε задає точність експериментальних даних, величину максимального відхилення отриманої оцінки від істинного значення, тобто ε є абсолютним значенням помилки у визначенні значення шуканої характеристики. При цьому довірча ймовірність $P_д$ вказує на те, з якою ймовірністю задана точність ε досягається.

Результати тестування БСП «Калина» показали, що математичне очікування результатів тестування статистичних властивостей вихідних послідовностей є незмінним від часу та реалізації, що дозволяє стверджувати про стаціонарність та ергодичність процесу БСП «Калина».

У третьому розділі аналізуються математичні моделі та вимоги до перспективного БСШ. Порівнюються основні схеми блокового шифрування та схеми розгортання ключів на прикладі таких шифрів, як «Калина», AES, ГОСТ, IDEA.

Математична модель БСП «Калина» має такий вигляд:

$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \left(\prod_{v=1}^{t-1}\left(k_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi'_l\right)\right) \circ \eta_l^{(K_0)},$$

де l – розмір внутрішнього стану блокового шифру (у бітах);

K – ключ шифрування;

k – довжина ключа шифрування (у бітах);

$\eta_l^{K_v}$ – функція додавання циклового ключа K_v за модулем 2^{64};

π_l'–шар нелінійного бієктивного відображення (байтова підстановка);

τ_l– перестановка елементів внутрішнього стану (циклічний зсув рядків вправо при матричному поданні);

ψ_l– лінійне перетворення (множення на матрицю);

$K_l^{K_v}$–функція додавання циклового ключа K_v за модулем 2.

На основі стандартної математичної моделі була побудована математична модель з прискореними швидкісними характеристиками, які були отримані за рахунок генерації таблиці передобчислень, що дозволило отримати рівень швидкодії не гірший ніж в AES та майже в 4 рази швидше за існуючий та використовуваний сьогодні ДСТУ ГОСТ 28147:2009 за умови використання 64-бітної архітектури (табл. 1).

Таблиця 1 – Показники швидкодії базових перетворень БСШ

Алгоритм	Швидкодія Mb/s	
	Стандартна реалізація	Прискорена реалізація
Калина-128/128	1042.12	1880.79
Калина-128/256	762.283	1306.53
Калина-256/256	860.5	1368.51
Калина-256/512	670.575	1110.12
Калина-512/512	426.128	968.103
AES-128/128	891.102	1753.13
AES-128/256	684.08	1391.88
ГОСТ-28147:2009	242.843	481.824

В ході оцінки швидкодії було використано ноутбук на процесорі Intel 3517U-1.90 GHz, який працював на швидкості 2.8 GHz. Операційна система Ubuntu 14.10, компілятор GCC 4.9.2.

Алгоритм розгортання ключів БСШ «Калина» описується наступним чином.

Кожен з циклових ключів $K_0, K_1, ..., K_t$ має розмір внутрішнього стану шифру (l бітів), подається як матриця розміром $8 \times c$ байтів і формується на основі ключа шифрування K, допоміжного ключа K_σ та власного індексу i. Циклові ключі K_i з парними індексами ($i \in \{0,2,..,t\}$) формуються за допомогою перетворення $\Xi^{(K,K_\sigma,i)}$:

$$\Xi^{(K,K_\sigma,i)} = \eta_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \kappa_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \eta_l^{(\varphi_i(K_\sigma))},$$

де l – розмір внутрішнього стану блокового шифру (у бітах);

K – ключ шифрування;

K_σ – допоміжний ключ;

$\eta_l^{K_v}$– функція додавання циклового ключа K_v за модулем 2^{64};

π_l'–шар нелінійного бієктивного відображення (байтова підстановка);

τ_l– перестановка елементів внутрішнього стану (циклічний зсув рядків вправо при матричному поданні);

ψ_l– лінійне перетворення (множення на матрицю);

$K_l^{K_v}$– функція додавання циклового ключа K_v за модулем 2.

Кожен з циклових ключів з непарними індексами обчислюється із попереднього ключа з парним індексом відповідно до співвідношення: $K_i = \left(K_{i-1} <<< \left(\frac{l}{4} + 24 \right) \right)$, де l – розмір внутрішнього стану блокового шифру (у бітах), $i \in \{1,3,..,t-1\}$.

З точки зору статистичних властивостей раундових ключів, кращі показники отримала схема розгортання, яка застосована в БСП «Калина». В табл. 2 записано результати статистичного тестування з використанням удосконаленого методу. На вхід до схеми розгортання було подано послідовність, згенеровану згідно з описом з другого розділу. Схема БСП «Калина» має значно вищі оцінки у порівнянні з іншими протестованими схемами розгортання ключів. Крім того, основна частина значень за результатами тестування, які не пройшли значення 0.96, були у проміжку 0.6 – 0.7, що значно краще, а ніж у AES, де значення знаходилися нижче рівня 0.2.

Таблиця 2 – Результати статистичного тестування схем розгортання ключів

M099	D099	S099	P099	M096	D096	S096	P096	MIN	Алгоритм
0	0	0	1	0	0	0	1	0	Оригінальна послідовність
0.75	0.01	0.08	1.00	1.00	0.00	0.00	1.00	1	AES
0.73	0.01	0.08	1.00	1.00	0.00	0.00	1.00	1	IDEA
0	0	0	1	0	0	0	1	0	ГОСТ 28147
9.68	3.60	1.90	1.00	28.42	0.50	0.71	1.00	24	Kalyna2

Недоліком цієї схеми є час роботи, який значно більший за інші протестовані схеми, але це не є критичним через те, що операція розгортання ключа рідко використовується і може бути виключена після першого розгортання з подальшим збереженням розгорнутого ключа.

У четвертому розділі досліджуються режими використання БСП «Калина» з обґрунтуванням їх відмінностей від стандартних режимів, що описані в NIST SP 800-38 (A-F). Основні зміни торкнулися режимів, які створювалися для стандартів FIPS (DES і AES) та проектувалися для використання з розміром блоку 64 та 128 біт відповідно. Через те, що БСП «Калина» використовує розміри блоку 128, 256 та 512 біт було прийнято рішення про модифікацію ряду режимів роботи у зв’язку з накладенням на них певних обмежень, пов’язаних з розміром блоку.

Наведено результати статистичних досліджень(табл. 3) з використанням модифікованого методу, описаному у розділі 3.

Таблиця 3 – Результати досліджень ПВП із застосуванням БСП «Калина» та AES

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Kalyna_ECB	132.47	35.73	5.98	1.00	186.73	0.13	0.36	1.00	184
AES_ECB	132.06	19.34	4.40	1.00	186.62	0.66	0.81	1.00	181
Kalyna_CTR	132.09	22.79	4.77	1.00	186.74	0.83	0.91	1.00	181
AES_CTR	132.73	30.31	5.51	1.00	186.83	1.70	1.31	1.00	176
Kalyna_CBC	132.53	20.17	4.49	1.00	186.63	1.06	1.03	1.00	179
AES_CBC	132.31	32.30	5.68	1.00	186.89	0.29	0.54	1.00	183
Kalyna_CFB	132.50	25.79	5.08	1.00	186.50	0.44	0.66	1.00	182
AES_CFB	133.63	18.23	4.27	1.00	186.72	0.60	0.77	1.00	181
Kalyna_OFB	132.35	20.53	4.53	1.00	186.63	0.57	0.76	1.00	181
AES_OFB	131.98	29.01	5.39	1.00	186.89	0.29	0.54	1.00	183
Kalyna_CMAC	131.62	24.72	4.97	1.00	186.79	0.51	0.71	1.00	182
AES_CMAC	132.82	21.35	4.62	1.00	186.78	0.84	0.92	1.00	181
Kalyna_GCM	132.35	27.86	5.28	1.00	186.81	0.51	0.72	1.00	182
AES_GCM	133.26	38.43	6.20	1.00	186.74	1.44	1.20	1.00	176
Kalyna_CCM	132.09	22.79	4.77	1.00	186.74	0.83	0.91	1.00	181
AES_CCM	131.97	15.65	3.96	1.00	186.59	0.46	0.68	1.00	182
Kalyna_KW	131.34	29.03	5.39	1.00	186.77	0.74	0.86	1.00	180
AES_KW	133.20	30.17	5.49	1.00	186.76	0.50	0.71	1.00	182
Kalyna_XTS	132.71	30.35	5.51	1.00	186.72	0.82	0.91	1.00	181
AES_XTS	132.09	22.28	4.72	1.00	186.58	0.46	0.68	1.00	182

– «Назва алгоритму» – отримані результати статистичних досліджень в ході реалізації БСШ «Калина» та AES у відповідному режимі з використанням розміру блоку 128 біт та розміру ключа 256 біт;

– «M096», «M099» – оцінки математичного сподівання (вибіркові середні) числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ і за критерієм $P_j \geq 0{,}99$, відповідно;

– «D096», «D099» («S096», «S099») – оцінки дисперсії (середньо-квадратичного відхилення) результатів тестування числа пройдених статистичних тестів за критеріями $P_j \geq 0{,}96$ і $P_j \geq 0{,}99$, відповідно;

– «P099» – розраховане значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}99$ і точності $\varepsilon = 2$;

– «P096» – розраховане значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ і точності $\varepsilon = 1$;

– "Min096" – наведені мінімальні значення числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$.

У п’ятому розділі наведено дослідження та науково-методичні верифікації реалізації алгоритму БСП «Калина», визначено і обґрунтовано обмеження на використання для кожного з режимів при значенні розміру блоку шифру 128, 256 та 512 біт відповідно (табл. 4).

Таблиця 4 – Обмеження на кількість блоків, що захищаються на одному ключі

Позначення режиму	Розмір блоку (l)		
	128	256	512
CTR, CFB, CBC, OFB, XTS	2^{60} (16 млн ТБ)	2^{124}	2^{251}
CMAC, CCM, GCM, GMAC, KW	2^{46} (64 ТБ)	2^{109}	2^{237}

Проведено аналіз з метою визначення необхідного набору режимів, який дає можливість використовувати шифр у широкому спектрі задач для різних застосувань з можливістю надання послуг конфіденційності та/або цілісності даних. Описано і обґрунтовано всі 10 режимів роботи з пропозиціями до їх можливого застосування та потенційними недоліками.

Для забезпечення взаємної сумісності результатів криптоперетворень у засобах КЗІ різних виробників були створені математичні та програмні моделі верифікації реалізації.

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

1) перевірка виконання загальних вимог до реалізації крипто-графічного перетворення:

– перевірка наявності та відповідності вимогам програмної документації на програмні модулі;

– перевірка наявності, відповідності вимогам та працездатності додаткового програмного забезпечення;

– перевірка наявності, відповідності вимогам та працездатності програмних модулів.

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

3) перевірка правильності реалізації режимів роботи, визначених у БСП «Калина» за допомогою тестових прикладів.

Перевірка за допомогою тестових прикладів має наступний вигляд. На початку описується режим використання БСП «Калина» з вхідними параметрами, наприклад: «Перетворення $N_Б = 4$, $q = 128$ (Калина-128/128-CCM-32,128)». Тут вказується розмір блоку, ключа та, за 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: *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.*

Такий опис використовується для всіх розмірів блоку та ключа шифрування БСШ для функцій зашифрування та розшифрування для кожного з режимів використання та для функції розгортання ключа.

ВИСНОВКИ

Дисертація є дослідженням нового криптографічного алгоритму блокового симетричного перетворення «Калина» в усіх його режимах застосування за напрямками стійкості та швидкодії. Результати досліджень дали можливість проаналізувати статистичні властивості алгоритму БСП «Калина» та порівняти їх з існуючими. БСП «Калина» має кращі показники з статистичної безпеки та швидкодії ніж міжнародний AES та набагато кращі показники, ніж існуючий державний стандарт України БСШ ДСТУ ГОСТ 28147:2009.

В області теорії:

1. Отримала подальший розвиток математична модель базового криптографічного перетворення алгоритму блокового симетричного перетворення «Калина», яка відрізняється від існуючої тим, що має оптимізований з точки зору використання передобчислень порядок та спосіб застосування основних елементів алгоритму, що дозволяє значно прискорити швидкодію основного криптографічного перетворення алгоритму «Калина».

2. Отримали подальший розвиток режими застосування блокових симетричних шифрів, які відрізняються від відомих урахуванням теоретично обґрунтованих обмежень на кількість викликів функції шифрування, сумарну довжину повідомлень, які захищаються з використанням одного ключа, значень певних констант та внутрішніх станів, зміненими процедурами обробки вихідних даних та проміжних значень, що дозволяє застосовувати нові режими шифрування для різних довжин блоків відкритого тексту та ключових даних у шифросистемах високої та надвисокої стійкості.

3. Удосконалено метод статистичного тестування генераторів ПВП, який відрізняється від відомих урахуванням похибок у результатах досліджень

різних (окремих) вихідних послідовностей, що дозволяє із заданою точністю та достовірністю оцінювати показники статистичної безпеки досліджуваного генератора. Зокрема встановлено, що функціонування генератора ПВП, який побудовано із використаним різних режимів застосування нового алгоритму блокового симетричного перетворення «Калина», описується випадковим стаціонарним ергодичним процесом.

В області практичних розробок та експериментальних досліджень:

1. Розроблено програмну реалізацію базового криптографічного перетворення нового алгоритму блокового симетричного перетворення «Калина». Встановлено, що за показниками швидкодії та ресурсомісткості розроблений криптоалгоритм володіє покращеними властивостями, зокрема:

– на 64-й платформі intel операційної системи Windows 7 x64 швидше за ГОСТ до 335% та до 7 % за американський стандарт шифрування AES;

– на 64-й платформі intel операційної системи ubuntu 14.10 LTS x64 швидше за ГОСТ до 291% та до 6 % за американський стандарт шифрування AES.

2. Розроблено програмну реалізацію різних режимів застосування нового алгоритму блокового симетричного перетворення «Калина». Зокрема були перероблені окремі режими застосування для можливості застосовуватися з блоковими симетричними перетвореннями високої та надвисокої стійкості.

3. Вперше отримано результати дослідження статистичної безпеки нового алгоритму блокового симетричного перетворення «Калина» у різних режимах застосування. Зокрема встановлено, що БСП «Калина» при будь-якому встановленому режимі генерує псевдовипадкові послідовності, тобто з високою вірогідністю і точністю можна стверджувати, що досліджуваний алгоритм блокового симетричного криптоперетворення буде статистично безпечним у будь-якому практичному застосуванні.

4. Отримано оцінки статистичної безпеки БСШ AES (FIPS-197) та ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009) в ході використання різних режимів застосування, проведено порівняні дослідження із БСП «Калина». Результати порівняльного аналізу свідчать про високі показники статистичної безпеки всіх досліджуваних шифрів, практично кожний криптоалгоритм може розглядатися як генератор псевдовипадкових послідовностей, робота якого гарно апроксимується випадковим процесом. Відмічається незначна перевага БСП «Калина», бо мінімальне значення числа пройдених статистичних тестів у БСП «Калина» є найвищим серед досліджуваних криптоалгоритмів.

5. За результатами порівняльних досліджень обґрунтовано практичні рекомендації щодо режимів застосування БСП «Калина» у різних криптографічних додатках. Загальну сумарну довжину повідомлень, які захищаються з використанням одного ключа, кількість викликів функції шифрування рекомендується обмежити в залежності від розміру блоку базового перетворення.

Наукові та практичні результати досліджень, які отримано в дисертації, доцільно використовувати: в науково-дослідницьких організаціях, для

отримання можливості отримання оцінки та порівняння між собою статистичних властивостей джерел даних (генераторів, шифрів, ґеш-функцій тощо), прогнозування властивостей вихідних послідовностей із заданою імовірністю та вірогідністю; на підприємствах для оцінки властивостей фізичних та детермінованих генераторів випадкових послідовностей; у вищих навчальних закладах за спеціальностями з захисту інформаційних технологій.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Мордвінов, Р.І. Методи та засоби генерування псевдовипадкових послідовностей / Ю.І. Горбенко, Н.В. Шапочка, Т.О. Гріненко, А.В. Нейванов, Р.І. Мордвінов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 141–152.

2. Мордвінов, Р.І.Властивості та перспективи застосування генераторів псевдовипадкових послідовностей на еліптичних кривих / Т.О. Гріненко, Ю.І. Горбенко, Р.І. Мордвінов // Системи оборони інформації. – 2011. – Вип. 2 (92). – С. 76–80.

3. Мордвінов, Р.І. Порівняльний аналіз алгоритмів генерації псевдовипадкових послідовностей / І.Д. Горбенко, Р.І. Мордвінов // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 188–190.

4. Мордвінов, Р.І. Сущность и анализ криптографических требований стандарта SP 800-90B / Ю.І. Горбенко, Р.І. Мордвінов // Радиотехника. – 2012. – Вип. 171. – С. 99–108.

5. Мордвінов, Р.І. Порівняльний аналіз методів та засобів тестування випадкових послідовностей NIST 800-22 та NIST 800-90B / Р.І. Мордвінов // Прикладная радиоэлектроника. – 2013. – Т. 12, № 2. – С. 250–253.

6. Мордвінов, Р.І. Дослідження режимів застосування блокових симетричних шифрів відповідно до ISO/IEC 10116-2006 / О.О. Кузнецов, Р.І. Мордвінов, Є.П. Колованова, А.В. Самойлова // Радиотехника. – 2014. – Вип. 176. – С. 45–54.

7. Мордвінов, Р.І. Розробка математичних та програмних моделей перспективного алгоритму шифрування для перевірки правильності реалізації / Ю.І. Горбенко, Р.І. Мордвінов, О.О. Кузнецов // Восточно-европейский журнал передовых технологий. – 2014. – Т. 5/9 (71) – С. 39–45.

Наукові праці апробаційного характеру:

8. Мордвінов, Р.І. Використання генераторів псевдовипадкових послідовностей у банківській сфері / Р.І. Мордвінов // Наукові дослідження молоді - вирішенню проблем європейської інтеграції: зб. наук. статей. – К. : УБС НБУ, 2011. – 1 електрон. опт. диск (CD-ROM). – Назва з екрана.

9. Мордвінов, Р.І. Генератори ПВП, що базуються на багатомодульному перетворенні у розширенні поля / Р.І. Мордвінов // 15-й Ювілейний Міжнародний молодіжний форум Харківського національного університету

«Радиоэлектроника и молодежь в XXI веке», 18-20 травня 2011р. – Харків, Україна. – 2011. – Т.5. – С. 171–172.

10. Мордвінов, Р.І. Сравнительный анализ алгоритмов генерации псевдослучайных последовательностей / Ю.І. Горбенко, Гріненко Т.О., Р.І. Мордвінов // Вторая Международная научно-техническая конференция «Компьютерные науки и технологии», 3-5 жовтня 2011 р. – Бєлгород, РФ. – 2011. – С. 476–480.

11. Мордвінов, Р.І. Усовершенствование генератора псевдослучайной последовательности для цифровых подписей / І.Д. Горбенко, Р.І. Мордвінов // Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями» Академії митної служби України, 2 грудня 2011р. – Дніпропетровськ, Україна. – 2011. – С. 149–151.

12. Мордвінов, Р.І. Класифікація і обґрунтування вимог до генерації випадкових послідовностей / Р.І. Мордвінов, І.Д. Горбенко // 16-й Міжнародний молодіжний форум Харківського національного університету «Радиоэлектроника и молодежь в XXI веке», 17-19 квітня 2012р. – Харків, Україна. – 2011. – Т.5. – С. 100–101.

13. Мордвінов, Р.І. Метод генерации псевдослучайных последовательностей в кольцах срезанных полиномов и их свойства [Електронний ресурс] / Р.І. Мордвінов, І.Д. Горбенко // Науково-технічна конференція з міжнародною участю «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2012)» Харківського національного університету ім. В.Н. Каразіна, 24 квітня 2012р. – 2012 - 1 електрон. опт. диск (CD-R).

14. Мордвінов, Р.І. Сравнительный анализ существующих методов исследования случайных/псевдослучайных последовательностей / Р.І. Мордвінов // Пятнадцатая юбилейная международная научно-практическая конференция «Безопасность информации в информационно-телеком-муникационных системах» НТУУ «КПИ», 22-25 травня 2012р. – Київ, Україна. - 2012. – С. 41–42.

15. Мордвінов, Р.І. Обоснование нормативно-правовой базы и требований к исследованиям псевдослучайных последовательностей / Р.І. Мордвінов // Пятнадцатая юбилейная международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных сис-темах» НТУУ «КПИ», 22-25 травня 2012р. – Київ, Україна. - 2012. – С. 55–56.

16. Мордвінов, Р.І. Дослідження властивостей нового режиму шифрування Galois/Counter Mode and GMAC / О.О. Кузнецов, Є.П. Колованова, Р.І. Мордвінов // 2-га Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» Національного університету «Львівська політехніка», 30 травня – 01 червня 2013р. – Львів, Україна. - 2013. - С.64-65.

17. Мордвінов, Р.І. Анализ режимов работы блочных симметричных шифров / Р.І. Мордвінов // Шестнадцатая международная научно-практическая

конференция «Безопасность информации в информационно-телекоммуникационных системах» НТУУ «КПИ», 21-24 травня 2013р. – Київ, Україна. – 2013. – С. 29–30.

18. Мордвінов, Р.І. Анализ и применение стандарта NIST 800-90B / Р.І. Мордвінов // Шестнадцатая международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» НТУУ «КПИ», 21-24 травня 2013р. – Київ, Україна. – 2013. – С. 39–40.

19. Мордвінов, Р.І. Сравнительный анализ существующих методов и средств тестирования случайных последовательностей / Р.І. Мордвінов // Міжнародна наукова конференця «Питання оптимізації обчислень (ПОО-XL)» Інститута кібернетики імені В.М. Глушкова, 30 вересня – 4 жовтня 2013р. – Київ, Україна. – 2013. – С. 181.

АНОТАЦІЯ

Мордвінов Р.І. Моделі, методи та засоби дослідження режимів роботи блокових симетричних шифрів по критеріям стійкість – складність. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків, 2015.

У дисертаційній роботі запропоновано та обґрунтовано методи дослідження статистичних властивостей випадкових послідовностей. Запропоновано метод статистичного тестування, який заснований на наборі тестів NIST STS, але відрізняється тим, що враховує похибки вихідних послідовностей та дає оцінку не тільки послідовності зокрема, а й джерелу послідовності в цілому. Це стало можливим завдяки використанню теорії ймовірності та проходженню тестів на великій кількості (100 шт.) послідовностей для одного джерела даних.

Отримано результати статистичного тестування для БСШ ДСТУ ГОСТ 28147:2009, AES, Belt, Camellia, та БСП «Калина». Отримані результати показали високі статистичні властивості з точки зору випадковості, що є гарним показником для БСШ. Крім того тестування показало, що отримана оцінка є дуже точною, адже повторне тестування з іншими вхідними даними отримали майже таку саму оцінку під час тестування.

Розроблено прискорену математичну модель, яка дозволяє значно прискорити швидкодію БСП «Калина» за рахунок використання таблиці передобчислень, яка замінює елементи, що часто використовуються у алгоритмі.

Ключові слова: блоковий симетричний шифр, статистичний портрет, математичне очікування, оцінка статистичних властивостей.

АННОТАЦИЯ

Мордвинов Р.И. Модели, методы и средства исследования режимов работы блочных симметричных шифров по критериям стойкость – сложность. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет радиоэлектроники, Харьков, 2015.

В диссертационной работе предложен и обоснован метод исследования статистических свойств блочных симметричных преобразований, позволяющий с заданной точностью и вероятностью получить количественную оценку в виде математического ожидания количества пройденных тестов с учетом дисперсии и среднеквадратичного отклонения.

Получены результаты, составляющие основу решения для важной теоретико-практической задачи исследования стойкости блочного симметричного шифра с получением количественной оценки его статистических свойств с последующей возможностью проведения объективного сравнения с другими блочными симметричными шифрами. Предлагаемый подход отличается от существующих тем, что позволяет с заданной точностью и вероятностью получить статистический портрет не какой-либо отдельно взятой последовательности шифротекста, которые могут весомо отличаться между собой в зависимости от входных данных и ключа, а получить общую картину для непосредственного источника выходных данных.

Разработана математическая модель, позволяющая уменьшить сложность алгоритма за счет использования таблиц предвычислений, что позволяет получить значительное (от 1.6 до 2.2 раза) увеличение скоростных характеристик блочного симметричного преобразования «Калина».

Модернизирован ряд режимов использования БСШ из NIST SP 800-38 (A-F) с целью улучшения совместимости с алгоритмом блочного симметричного преобразования «Калина» в целом, и возможности использовать режимы для длин блоков отличных от 128 бит в частности.

Результаты диссертационных исследований позволяют расширить научные знания в области оценки стойкости блочных симметричных шифров, а точнее – дать оценку статистических свойств не для конкретной последовательности, а для всего шифра в целом. Кроме того были расширены границы применения ряда режимов шифрования с точки зрения ограничения на размер блока шифрования, связанные с тем, что эти режимы были разработаны для AES, использующего всего один размер блока 128 бит.

Ключевые слова: блочный симметричный шифр, статистический портрет, математическое ожидание, оценка статистических свойств.

ABSTRACT

Mordvinov RI Models, methods and tools for the study of symmetric modes of the block cipher criteria for stability - complexity. - Manuscript.

Thesis for the degree of candidate of technical sciences, specialty 05.13.21 - Information protection systems. - Kharkiv National University of Radio Electronics, Kharkiv, 2015.

In the thesis proposed and proved methods of statistical properties of random sequences. The method of statistical testing, which is based on a set of tests NIST STS, but differs in that takes into account the error output sequences and evaluates not only the sequence in particular, but also the source of a whole sequence. This is made possible through the use of probability theory and testing on a large number (100 pcs.) Sequences for a data source.

The results of statistical tests for SBC GOST 28147:2009, AES, Belt, Camellia, and SBC "Kalina". The results showed high statistical properties in terms of cases, which is a good indicator for SBC. Besides testing has shown that the resulting score is very accurate, because retest with other inputs received nearly the same assessment in testing.

Developed accelerated mathematical model that can significantly accelerate the speed of the SBC "Kalina" by using the precomputing table which replaces often usable elements of the algorithm.

Keywords: symmetric block cipher, a statistical portrait, expectation, estimation of statistical properties.