МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

ІНФОРМАЦІЙНА БЕЗПЕКА

Науковий журнал

№3 (31) 2018

№4 (32) 2018

Северодонецьк 2018

Інформаційна безпека

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

№3 (31) 2018

№4 (32) 2018

НАУКОВИЙ ЖУРНАЛ

ЗАСНОВАНО У 2009 РОЦІ

ВИХІД З ДРУКУ – ЧОТИРИ РАЗИ НА РІК

ЗАСНОВНИК

Східноукраїнський національний університет ім. Володимира Даля

Журнал зареєстровано Міністерством юстиції України

Свідоцтво про державну реєстрацію **серія КВ №15063-3635Р**

Information security

VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY

№3 (31) 2018

№4 (32) 2018

THE FIRST ISSUE OF THE JOURNAL WAS PUBLISHED IN 2009

THE JOURNAL IS PUBLISHED QUARTERLY

FOUNDER

Volodymyr Dahl East Ukrainian National University

REGISTERED by the Ministery of Justice of Ukraine registration **sertificate KB №15063-3635P**

ISSN 2224-9613

Відповідальний за випуск: проф., д.т.н. О.С. Петров.

До журналу увійшли статті студентів, аспірантів, докторантів Східноукраїнського національного університету імені Володимира Даля, вищих навчальних закладів України, Росії та закордонних країн.
Журнал підготовлено кафедрою безпеки інформаційних систем СНУ ім. В. Даля.
Рекомендовано до друку Вченою радою Східноукраїнського національного університету імені Володимира Даля (протокол №2 від 26.09.2018 р.).
Занесений до "Переліку фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук" ***з технічних наук***, затверджений постановою президії ВАК України від 14.05.2010 р., №1-05/3.
Матеріали номера друкуються мовою оригіналу.

ЗМІСТ ЖУРНАЛУ №3 (31) 2018

УДК 681.3.06
[1]Євсеєв С.П., [1]Король О.Г.,[2]Корольов Р.В., [2]Піх Ю.Р.
[1]Харьківський національний економічний університет ім. С. Кузнеця
[2]Харьківський університет Повітряних Сил ім. Івана Кожедуба

СТАТИСТИЧНИЙ МЕТОД ОЦІНКИ СТІЙКОСТІ НА ОСНОВІ ЕНТРОПІЙНОГО МЕТОДУ

В роботі розглядається метод оцінки стійкості і якості програмної реалізації криптографічних алгоритмів на основі методі ентропійної оцінки випадковості вихідної послідовності після криптоперетворень.
Ключові слова:криптостійкість, програмне забезпечення, ентропійна оцінка випадковості.

Постановка проблеми в загальному вигляді та її зв'язок із важливими практичними завданнями. Розвиток криптології тісно пов'язаний з вдосконаленням методології оцінки блокових шифрів, що набули широкого поширення в протоколах забезпечення безпеки банківської інформації та інших комунікаційних системах, і мережах завдяки високій продуктивності і низькій складності реалізації. Крім забезпечення конфіденційності (захисту даних при передачі від пасивних атак), симетричні алгоритми використовуються для забезпечення цілісності на основі кодів автентичності повідомлень (MAC-кодів) і формування геш-функцій, як компоненти електронного цифрового підпису, генерації псевдовипадкових пост-послідовностей в складі протоколів підтвердження автентичності і т.п.

Для порівняльної оцінки ефективності (криптостійкості) симетричних криптоалгоритмів, як правило використовують методи лінійного і диференціального криптоаналізу. Порівняння механізмів безпеки на алгоритмах традиційної криптографії, криптографії з відкритим ключем, гібридних криптосистем можливо на підставі якісного показника, що враховує критерії криптостійкості та якості програмної реалізації. Саме тому для оцінки стійкості криптоалгоритмів різних моделей криптосистем пропонується використовувати експрес-аналіз на основі ентропійного методу.

Аналіз останніх досліджень [1 – 10] показав, що зазвичай для дослідження якості механізмів шифрування інформаційних систем використовують досить складні, але в той же час дієві методи. Ці метрикиоцінки безпеки базуються на складному математичному апараті, що, в свою чергу, вимагає для отримання і трактування результатів спеціальні знання та додаткові кошти. Серед найпоширеніших метрик безпеки є їх наступні таксономії: Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, ErkanKahraman. Але використання більш простого і відомого ентропійного методуоцінювання випадковості вихідної величини дозволить середньостатистичному спеціалісту з IT-технологій на інтуїтивному рівні визначити перевагу того чи іншого криптоалгоритму та його програмній реалізації.

Метою статті є дослідження можливості використання запропонованого експрес-методу, який дозволяє без значних обчислювальних, енергетичних витрат на інтуїтивному рівні порівняти не тільки стійкість різних криптоалгоритмів (криптосистем), але і їх програмну реалізацію.

Викладення основного матеріалу. Аналіз методик оцінювання ризиків. Для побудови систем менеджменту інформаційної безпеки, комплексних систем захисту інформації та інших систем безпеки необхідно проводити аналіз і оцінку ризиків. Існуючі засоби оцінки в більшості своїй засновані на статистичних підходах. У багатьох країнах, як на рівні підприємств, так і на державному рівні подібна статистика не ведеться. Це обмежує можливості існуючих засобів, наприклад, щодо використання різних типів вхідних даних для оцінки. Відомий інструментарій не дає можливості застосування для аналізу та оцінки ризиків широкого спектра початкових параметрів.

Специфічною особливістю імовірнісних показників безпеки, що відрізняють їх від більшості інших показників якості продукції, є принципова неможливість їх прямого виміру. Для отримання чисельних значень показників безпеки необхідна вихідна

інформація, що отримується методами вимірювань (наприклад, напрацювання) і спостережень. Значення показників безпеки визначаються шляхом математичної обробки вихідної інформації. оскільки показники безпеки відносяться до імовірнісних категоріях, то найбільш адекватний математичний апарат, що дозволяє обчислювати їх, спирається на методи теорії ймовірностей і математичної статистики. Сукупність ймовірнісно-статистичних методів обчислення показників безпеки та аналізу безпеки на їх основі називається імовірнісним аналізом безпеки.

У сучасній практиці методи імовірнісного аналізу безпеки (ІАБ) служать цілям дослідження таких типів завдань, як:

визначення ризику (на стадії проектування і на стадії експлуатації);

оптимізація проектних рішень шляхом порівняльного аналізу декількох варіантів об'єкта;

виділення найбільш значущих з точки зору безпеки відмов і порушень нормальної експлуатації для цілеспрямованого впровадження коригувальних заходів щодо підвищення безпеки об'єкта.

У той же час ІАБ не може бути підмінений іншими формами і методами дослідження, так як дозволяє отримати комплексну кількісну міру безпеки – ймовірність злому з певними наслідками, тобто ризик.Методи ІАБ, необхідні для розрахунку показників безпеки, повинні, звичайно, як можна більш повно відображати суть реальних об'єктів. Однак, маючи в своєму розпорядженні недостовірні вихідні дані, особливо на стадії проектування, не слід прагнути до дуже точного опису системи, застосовуючи складні методи ІАБ, які можуть породити оманливу видимість точності. У той же час, не можна робити невиправданий висновок про недоцільність застосування ІАБ через можливу невизначеності його результатів. У кожному конкретному випадку необхідно виходити з потреб практики, враховуючи, що чим раніше за допомогою ІАБ виявити недоробки проекту або порушення при експлуатації, тим ефективніше будуть коригувальні заходи щодо забезпечення безпеки систем.

Існує велика кількість програмних продуктів, які вже реалізують набір тестів статистичного аналізу інформаційної безпеки. Основними представниками яких є: NIST, FAIR, IT-Grundshutz, OCTAVE, IRAM, EBIOS, RISK WATCH, MEHARI, MAGERIT, CRAMM, Методика НБУ.В табл. 1, 2 наведені результати досліджень основних методик оцінки ризиків, які часто використовуються.

Проведений аналіз стандартів показав, що ключовим моментом принципів управління ІБ є оцінювання ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно наявні засоби захисту здатні протистояти інформаційним атакам. Практика показує, що сьогодні можна чітко виділити дві основні групи методів оцінювання ризиків безпеки. Перша група методів дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог щодо забезпечення інформаційної безпеки. Друга група методів оцінювання ризиків ІБ базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. В даному випадку значення ризику обчислюється окремо для кожної загрози і в загальному випадку є як добуток імовірності реалізації загрози на величину потенційних збитків від цієї загрози.Значення шкоди визначається власником інформації, а ймовірність реалізації загрози обчислюється групою експертів, які проводять процедуру аудиту [11,12].

Таблиця 1

Методики оцінки ризиків

Методика оцінки	Переваги	Недоліки	Підходи
NIST	- Детальний опис можливих ризиків інформаційних активів - Для підприємств різного розміру	- Довготривалий процес аналізу - Деякі функції не автоматизовано	Евристичний
FAIR	- Комплексний аналіз - Симуляційна модель - Висока ефективність	- Для крупних банків та підприємств	Ймовірнісний
IT-Grundshutz	- Гнучкість методу надає змогу проводити аналіз для будь-якої організації - Налаштовується на нові або існуючі активи	- Потребує теоретичної обізнаності процесу аналізу ризиків - Висока вартість ліцензії	Евристичний
OCTAVE	- Швидке впровадження - Обслуговує малі та середні за розміром підприємства	- Відсутність автоматизації - Не враховує специфіку банківської сфери	Евристичний
IRAM	- Відносна простота впровадження - Легкість в експлуатації менеджерами банківських установ	- Висока вартість ліцензії - Робота тільки з існуючими інформ. активами	Інформаційний
EBIOS	-Велика кількість користувачів - Генерація звітів	- Лише для комерційних та державних установ	Інформаційний
RISK WATCH	- Простота впровадження та експлуатації - Гнучкість - Висока ефективність	- Аналіз ризиків лише на програмно-технічному рівні - Висока вартість ліцензії	Інформаційний
MEHARI	- Заснований на аналізі формул та параметрів - Формує оптимальну множину контрзаходів - У вільному доступі	- Застосовуваний до систем, що побудовані тільки за стандартом ISO	Евристичний
MAGERIT	- Систематичний метод аналізу - Кількісна оцінка - Гнучкість	- Результуючі дані залежать від людського фактору	Евристичний
CRAMM	- Детальне визначення існуючих ризиків - Ефективність використання	- Важкість у розумінні - Висока вартість ліцензії. - Робота тільки з існуючими інформ. активами	Ймовірнісний
Методика НБУ	- Детальний аналіз ресурсів банківської системи - Використання ризик-орієнтованого підходу	- Заснований на множині стандартів - Враховує специфіку лише українських банківських систем	Інформаційний

Таблиця 2

Результати досліджень методик оцінки ризиків

Методика	Атрибути							
	Якісна оцінка	Кількісна оцінка	Комплексна оцінка	Країна походження	Застосування у ОБС	Програмна реалізація	Ефективність контрзаходів	Простота розуміння
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франція	+	+	+	-
MEHARI			+	Франція				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Німеччина			+	
IRAM	+			Європа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобританія	+	+	+/-	+/-
MAGERIT	+	+		Іспанія	+	+		
Методика НБУ	+			Україна	+		-	+

Дослідження експрес-методу оцінювання криптоалгоритмів на основі ентропійного методу. Для оцінки стійкості криптоалгоритмів різних моделей криптосистем пропонується використовувати експрес-аналіз на основі ентропійного методу, використовуваного в пакеті статистичних досліджень випадкової величини *NISTSTS* 822 [**Ошибка! Источник ссылки не найден.**]. Запропонований експрес-аналіз дозволяє без значних обчислювальних, економічних та людських витрат на інтуїтивному рівні порівняти не тільки стійкість різних криптоалгоритмів (криптосистем), але і їх програмну реалізацію.

Алгоритм ентропійного методу оцінки криптостійкості наведено на рис. 1. У табл. 3 наведені результати досліджень стійкості і програмної ефективності реалізації блокових і потокових шифрів різної складності.

Для проведення досліджень використовувалися БСШ: *DES*, 3*DES*, ГОСТ-28147-2009, Калина-256, *AES*-256. Для реалізації потокового шифру використовувалися генератори псевдовипадкової послідовності двох різних типів: на правилі “60” клітинних автоматів в його класичному вигляді без модифікацій і криптографично стійкий генератор *SecureRandom* з криптобібліотеки *Java*, який позиціонується як придатний для криптографічних застосувань; для оцінки несиметричного криптоалгоритму використовувався алгоритм *RSA*.

Таблиця 3

Результати досліджень стійкості криптоалгоритмом експрес-методом

№	Шифр	Ентропія вхідного тексту	Ентропія криптограми	різниця між ентропіями	% ентропії, який додається шифром
1	Клітинні автомати, правило “60”	0,469276	0,6820179 (6,820179)	0,1796404 (1,796404)	35,7580505
2	Криптостійкий генератор *SecureRandom* з *Java*	0,469276	0,7999982 (7,999982)	0,2976215 (2,976215)	59,2426958
3	*DES*	0,469276	0,812043	0,342767	73,0416642
4	*3DES*	0,469276	0,812043	0,342767	73,0416642
5	ГОСТ 28147-2009	0,469276	0,811348	0,342072	72,8935637
6	Калина-256	0,469276	0,954519	0,485243	103,4024753
7	*AES*-256	0,469276	0,95454	0,485264	103,4069503
8	*RSA*	0,469276	1	0,530724	113,094213214

У табл. 3 підраховувалася ентропія вхідного і зашифрованого тексту, різниця, а також відсоток ентропії, що додається до ентропії відкритого тексту самим шифром. Аналіз табл. 3 дає можливість оцінити внесок самого шифру в підсумкову ентропію зашифрованого повідомлення. Оскільки всі вони тестувалися в однакових умовах, можна судити про їх відносні показники.

У цьому сенсі варто відзначити *AES*-подібні шифри (*SPN*-системи, підстановочно-переставні схеми). Обидва таких шифру, і Калина-256, і *AES*-256 внесли найбільший вклад, понад 103% в ентропію відкритого тексту. Таким чином, обидва шифри володіють найкращим розсіюванням. Приблизно однакові показники продемонстрував блоково-симетричний шифр ГОСТ-28147-2009 – 72,89% проти 73,04% у *DES* / 3*DES*. Ймовірно, це тільки підтверджує висновки про максимально можливу міру розсіювання, як характеристику архітектури БСШ.

Для порівняння було проведено експерименти з використанням потокових шифрів на основі двох різних генераторів псевдовипадкової ключової послідовності. Шифрування проводилося за правилом додавання за “модулем два”.

У першому випадку – це генератор на основі клітинних автоматів (правило “60”). Це не криптостійкий генератор, послідовність якого не проходить тестування NIST STS 822, а другий позиціонується як криптостійкий генератор *SecureRandom* з криптобібліотеки *Java*. В обох випадках отримані значення ентропії, набагато менші, ніж у класичних БСШ, що не дозволяє говорити про якісне шифруванні з їх допомогою.

Алгоритм несиметричної криптографії забезпечує найвищий досліджений показник понад 113% в ентропію відкритого тексту, що підтверджує його доказову криптостійкість.

Таким чином, наведені результати дозволяють стверджувати, що простий експрес-метод на основі ентропійного методу оцінювання випадковості криптограми дає можливість експрес-оцінки якості використовуваних шифрів без залучення експертних оцінок, великих економічних, обчислювальних та людських затрат. Така експрес-методика доступна будь-якому користувачеві, що має мінімальні знання з теорії інформації. Більше того, таким чином можна оцінювати різні реалізації шифрів, що дозволить вибрати найкращу (оптимальну) програмну реалізацію, яка підходить для умов і вимог користувача.

Наприклад, комп'ютерних експериментах використані дві реалізації алгоритму *DES*. Одна з них, показана в табл. 4 під номером 3, демонструвала приріст ентропії після шифрування в 73,04% від вхідного тексту, інша – 64,4%.

Природно, для практичних цілей має сенс вибрати першу реалізацію, оскільки, очевидно, що її характеристики розсіювання кращі. Таким чином, експрес-аналіз дозволяє оцінити якість реалізації класичних (та інших) криптоалгоритмів з метою вибору оптимальної криптобібліотеки з множини існуючих на ринку.

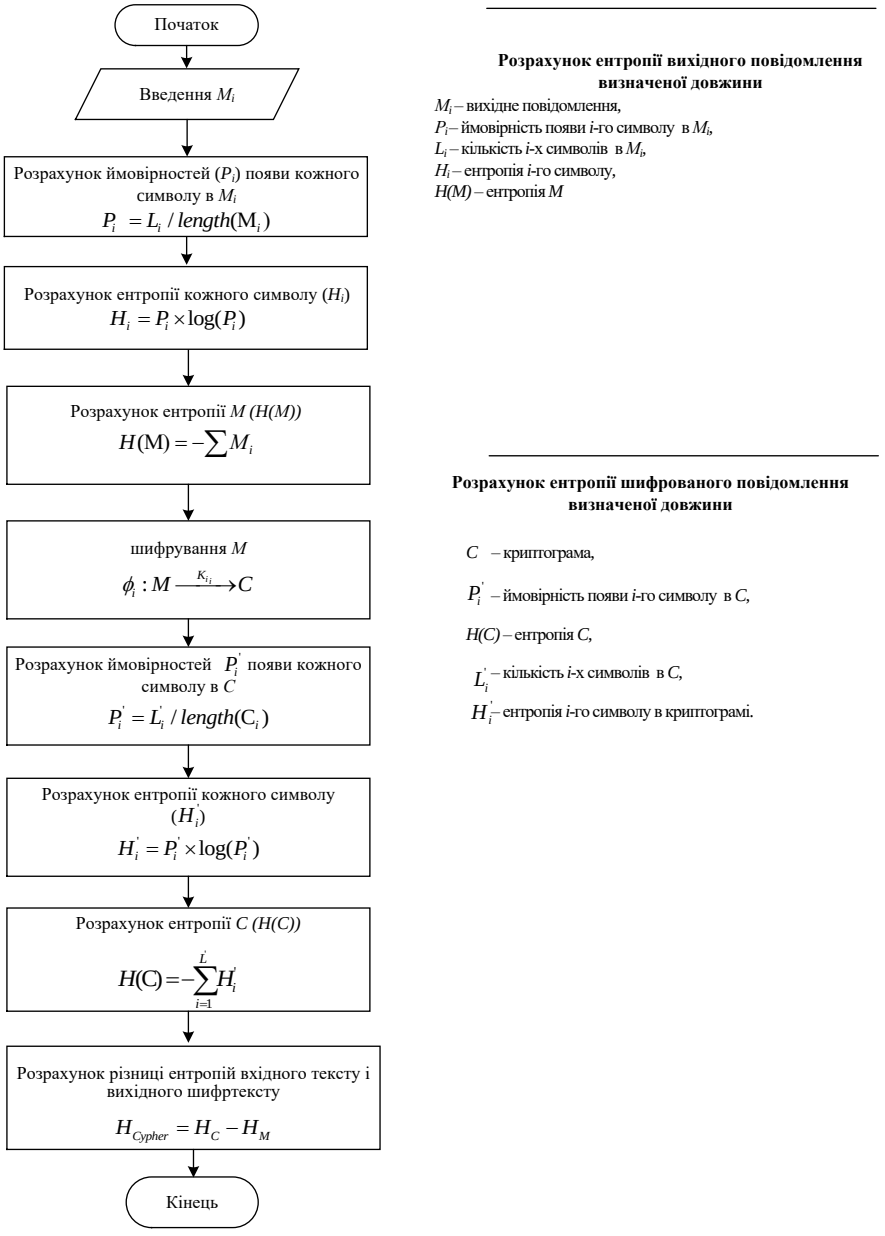

Рис.1. Алгоритм тестування криптосистеми на стійкість на основі ентропійного методу оцінки випадковості

Розглянемо отримані результати з точки зору максимального криптографічного захисту інформації. Показником такого захисту буде ентропія зашифрованого виконуваного файлу, що наведено в табл. 4.

Таблиця 4

Оцінка максимального криптографічного захисту інформації

№	Шифр	Ентропія вхідного тексту	Ентропія криптограми	Ймовірність крипто-захисту, P_c
1	Клітинні автомати, правило “60”	0,469276	0,637079949	0,637079949
2	Криптостійкий генератор *SecureRandom* з *Java*	0,469276	0,747287753	0,747287753
3	*DES*	0,469276	0,812043	0,812043
4	*3DES*	0,469276	0,812043	0,812043
5	ГОСТ 28147-2009	0,469276	0,811348	0,811348
6	Калина	0,469276	0,954519	0,954519
7	*AES*-256	0,469276	0,95454	0,95454
8	*RSA*	0,469276	1,000	1,000
9	Ідеальний шифр		1,000	1,000

Відомо, що максимально можливий криптографічний захист дає так званий “Ідеальний шифр” за Шеноном, який в результаті шифрування дає випадкове число [13]. Такий файл матиме максимальну ентропію, яка в бінарному випадку дорівнює одиниці. Будемо вважати, що шифрування таким шифром дасть максимальний криптографічний захист, і приймемо її за 1. Ймовірність захисту таким шифром дорівнює одиниці. Природно, неідеальні шифри не дають такої ймовірності криптографічного захисту.

На рис. 2 наведені результати досліджень усередненої ентропії криптограм різних БСШ осмисленого відкритого тексту довжиною $M = 10^8$ біт, з інтервалом $N = 5 \times 10^6$ біт.

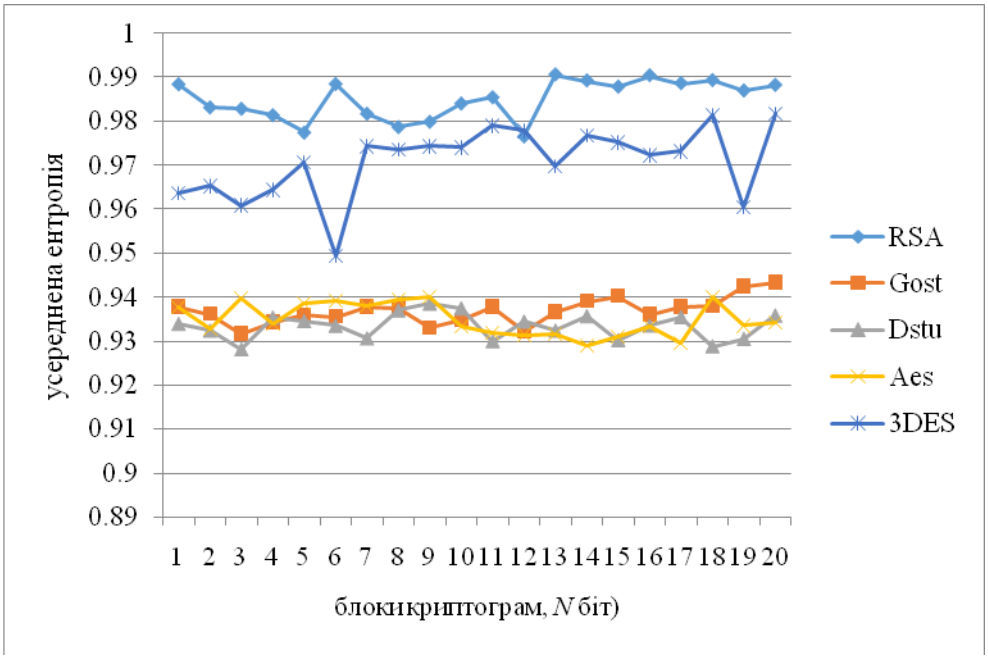

Рис. 2. Результати досліджень усередненої ентропії блоків криптограм

Аналіз рис. 2 практично підтверджує можливість використання експрес-методу щодо вибору програмного забезпечення механізмів безпеки на основі криптоалгоритмів.

Висновки і перспективи подальших досліджень. Таким чином, запропонованийекспрес-метод оцінювання стійкості криптоалгоритмів дає можливість ранжувати всі досліджені шифри через ймовірність криптографічного захисту. При цьому він не потребує значних обчислювальних, енергетичних та людських затрат, отримані результати інтуїтивно доказові Цей показник можна використовувати для різних методик оцінки захищеності комплексних систем захисту різних комп'ютерних мереж технологій, що свідчить про його універсальність.

Литература:

1. Євсеєв С. П. Використання міні-версій для оцінки стійкості блоково-симетричних шифрів / С. П. Євсеєв, С. Е. Остапов, Р. В. Корольов // Науково-технічний журнал "Безпека інформації". том.23. № 2. Київ. – 2017. – с. 100 – 108.
2. И.Д. Горбенко"Новаяидеологияоценкистойкостиблочныхсимметричныхшифров к атакам дифференциального и линейного криптоанализа"Прикладнаярадиоэлектроника. Том 9, № 3, С. 312 – 320, 2010.
3. В.И. Долгов, И.В. Лисицкая "Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа": монография, Харьков: Издательство «Форт», 420 с., 2013.
4. И.В. Лисицкая "О новойметодикеоценкистойкостиблочныхсимметричныхшифров к атакам дифференциального и линейного криптоанализа" Системи обробки інформації. Вип. 4 (94), С. 167-173, 2011.
5. И.В. Лисицкая "Методологияоценкистойкостиблочныхсимметричныхшифров" [Электронный ресурс] .– Режим доступа : https://cyberleninka-.ru/article/n/metodologiya-otsenki-stoykosti-blochnyh-simmetrichnyh-shifrov.
6. NIST STS [Electronicresource] : Downloaddocumentationandsoftware., Electronicdata: NIST, 2014, Modeofaccess: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.
7. OntheInterpretationofResultsfromthe NIST StatisticalTestSuite / Marek SYS, Zdenek RIHA, Vashek MATYAS, Kinga MARTON, Alin SUCIU // Romanianjournalofinformationscienceandtechnology, Vol. 18, № 1, 2015, P. 18-32.
8. А.В. Потий, С.Ю. Орлова, Т.А. Гриненко «Статистическоетестированиегенераторовслучайных и псевдослучайных чисел с использованием набора статистическихтестов NISTSTS», Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, 2001, Вип. 2, С. 206-214.
9. A StatisticalTestSuitefortheValidationofRandomNumberGeneratorsandPseudoRandomNumberGeneratorsforCryptographicApplications. NIST SpecialPublication 800-22, May 15, 2001, 164 p.
10. С.О. Гнатюк, Т.О. Жмурко, Ю.Я. Поліщук, Н.А. Сєйлова, Розширена класифікація квантових методів безпечної комунікації. Наукоемкие технологи в инфокоммуникациях: обработкаинформации, кибербезопасность, информационнаяборьба: Монография [под. ред. В.М. Безрука, В.В. Баранника]. Х. : Лидер, 2017, С. 467-482.
11. Бурячок В. Л. Політика інформаційної безпеки [Текст] : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.
12. С. Евсеев, О. Король, и А. Сочнева, "Анализоценкирисков кибербезопасности банковскойинформации", Сборниканаучныхтрудов НАУ "Защитаинформации", вып. 23, с. 109 – 128, 2016.
13. K. Shennon, Rabotypoteoriiinformacii i kibernetike. M. IL. 1963.

Рецензент: д.т.н., проф. Петров О.С., д.т.н., проф. Казакова Н.Ф. Надійшла 21.06.2018

Евсеев С.П., Король О.Г., Королев Р.В., Пих Ю.Р.

СТАТИСТИЧЕСКИЙ МЕТОД ОЦЕНКИ СТОЙКОСТИ НА ОСНОВЕ ЭНТРОПИЙНОГО МЕТОДА

В работе рассматривается метод оценки стойкости и качества программной реализации криптографических алгоритмов на основе методе энтропийной оценки случайности выходной последовательности после криптопреобразования.

Ключевые слова: криптостойкость, программное обеспечение, энтропийная оценка случайности.

Yevseiev S., Korol O., Korolev R., Pih Y.

STATISTICAL METHOD OF ASSESSING RESISTANCE BASED ON THE ENTROPY METHOD

The article considers a method for estimating the persistence and quality of software implementation of cryptographic algorithms based on the method of entropy estimation of the randomness of the output sequence after crypto-transformation.

Keywords: cryptostability, software, entropy estimation of randomness.