КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.935
УДК 004.056.55: 003.26

Грищук Руслан Валентинович
Лауреат Національної премії України імені Бориса Патона,
Заслужений діяч науки і техніки України,
доктор технічних наук, професор полковник
Заступник начальника Військової академії (м. Одеса)
Військова академія (м. Одеса), Одеса, Україна
ORCID ID: 0000-0001-9985-8477
Prof.hry@gmail.com

Грищук Ольга Михайлівна
доктор філософії, підполковник
Слухачка Національного університету оборони України
Національний університет оборони України, Київ, Україна
ORCID ID: 0000-0001-6957-4748
Hry.olha@gmail.com

ОЦІНЮВАННЯ КРИПТОСТІЙКОСТІ КРИПТОСИСТЕМИ ФРЕДГОЛЬМА: МЕТОДОЛОГІЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

Анотація. Стрімкий розвиток технологій квантового криптоаналізу в найближчому майбутньому ставить під загрозу зламу існуючі асиметричні та симетричні криптосистеми. Саме тому в світі та в Україні досить інтенсивно розвивається новітній напрям в галузі постквантової криптографії. Ведеться розроблення як нових криптоалгоритмів, так і інноваційних криптосистем на нетрадиційних математичних принципах. Однією з таких криптосистем є криптосистема Фредгольма. Вона одночасно інноваційна, але найменш досліджена з позицій кібербезпеки. Її особливість полягає у тім, що на відміну від відомих технічних рішень, які ґрунтуються на методах дискретної математики, дана система функціонує на основі методів інтегрального числення. Через відсутність відомостей про теоретичну та практичну криптостійкість згаданої криптосистеми її подальше практичне впровадження стримується. Для заповнення цього наукового пробілу в статті розроблено методологію оцінювання криптостійкості зазначеної криптосистеми. Запропонована методологія ґрунтується на оцінюванні криптостійкості найслабкішої ланки криптосистеми Фредгольма — стійкості її ключа шифрування до зламу методом перебору (кібератаки грубої сили). Основним критерієм оцінювання теоретичної криптостійкості при цьому обрано кількість операцій, необхідних для перебору варіантів ключа шифрування. На основі методів комбінаторного аналізу, як результат, доведено лему про її теоретичну криптостійкість. Показано, що вона залежить тільки від кількості дискрет диференціального спектра ключа шифрування, які визначають обчислювальну складність з його підбору, а не від порядку їх перестановки. Як додатковий критерій обрано час зламу ключа шифрування. Основним критерієм практичної криптостійкості обрано норму рішення оберненої некоректної задачі дешифрування (задачі криптоаналізу). Вона використовується для визначення параметра регуляризації, який і впливає на стійкість та точність розв'язку оберненої некоректної задачі. Додатковим критерієм оцінювання практичної криптостійкості обрано ймовірність підбору ключа шифрування. У результаті оцінювання показано й доведено, що практична криптостійкість криптосистеми Фредгольма підвищується зі зростанням кількості операцій, необхідних для підбору кількості дискрет диференціального спектра ключа шифрування. На основі аналізу одержаних результатів зроблено висновки про переваги та недоліки криптосистеми Фредгольма. Також запропоновано рекомендації з її подальшого впровадження в практику захисту інформації, яка циркулює в інформаційно-комунікаційних системах критичного призначення.

Ключові слова: диференціальні перетворення; кібератака; кібербезпека; криптосистема; криптостійкість; ключ шифрування; параметр регуляризації

ВСТУП

Вперше ідею створення інноваційних криптосистем, принципи роботи яких ґрунтуються на методах інтегральної криптографії закладено в працях українських вчених Г. Броншпака, І. Громики, С. Доценка та Є. Перчика [1]. Дана робота послугувала поштовхом для подальшого розвитку цього підходу як в Україні [2]–[5], так і за кордоном. В Україні переважна частина досліджень і наукових публікацій стосується питання побудови криптосистеми Фредгольма для захисту мовної інформації в інформаційно-комунікаційних системах критичного призначення [3]–[5]. Також у науковій літературі доступна інформація про її застосування для криптографічного захисту відеопотоку та текстових даних [6]. Зарубіжні напрацювання в основному стосуються підвищення криптостійкості безпекових механізмів протоколу розподілу ключів шифрування BB84, який використовується в квантових лініях зв'язку. Інших відомостей про прикладні застосунки цієї криптосистеми у відкритому доступі немає.

Постановка проблеми. Основним проблемним питанням, яке стримує практичне використання криптосистеми Фредгольма, є недостатня вивченість її безпекових властивостей, зокрема криптостійкості.

Аналіз останніх досліджень і публікацій. Світовий досвід створення засобів криптографічного захисту інформації [7], [8] свідчить про те, що практичному провадженню та введенню в експлуатацію інноваційних криптосистем, зокрема й тих, які ґрунтуються на нетрадиційних математичних принципах, має передувати технічний регламент, пов'язаний з оцінюванням їх криптостійкості. Правову основу технічного регламенту в нашій державі становлять державні стандарти України, гармонізовані з міжнародними та європейськими нормативними документами. Базисом таких документів є безпекові стандарти ISO/IEC [8]–[18]. Зважаючи на належність криптосистеми Фредгольма до класу симетричних криптографічних систем потокового шифрування [19], дослідження її криптостійкості на сучасному етапі розвитку науки і техніки може бути проведено з використанням таких основних методів криптоаналізу як: криптоаналіз генератора ключів шифрування [20]; диференціальний криптоаналіз [21]; лінійний криптоаналіз [22]; криптоаналіз через технічні канали витоку інформації [23]; перебір ключів (кібератака грубої сили) [24]. Якщо порівнювати дані методи, то останній з наведених — перебір ключів шифрування можна вважати найбільш ефективним. Його використання під час оцінювання криптостійкості досліджуваної криптосистеми дозволить охопити всі можливі варіанти ключів шифрування.

Мета статті. Стаття має на меті розроблення методології оцінювання криптостійкості криптосистеми Фредгольма. Одержані результати слугуватимуть підґрунтям для подальшого проходження криптосистемою технічного регламенту перед її практичним впровадженням.

ТЕОРЕТИЧНІ ОСНОВИ

Узагальнивши [2]–[5] та [19] у даному розділі стисло викладемо концептуальні та фундаментальні засади функціонування криптосистеми Фредгольма.

Концептуальні засади функціонування криптосистеми Фредгольма.

Нехай захисту підлягатиме інформація I. При використанні ключа шифрування K вона за деяким криптографічним алгоритмом E перетворюється в шифрограму S. Тоді

рівняння шифрування та розшифрування можуть бути описані системою рівнянь загального вигляду [19]

$$\begin{cases} S = E(K, I); \\ I = E(K, S). \end{cases} \quad (1)$$

Припущення. Ключ шифрування K зберігається в таємниці обома сторонами інформаційного обміну — і Алісою, і Бобом. Об'єктом захисту виступає мовна інформація I. Під криптостійкістю в статті розуміється стійкість шифру до криптоаналізу. У досліджуваній криптосистемі вона забезпечується за рахунок використання алгоритмів на основі інтегральних рівнянь Фредгольма першого роду [2].

Обмеження. Для шифрування та розшифрування використовується один ключ K, а оцінювання криптостійкості обмежується класом обернених некоректних задач. Для розшифрування зашифрованої мовної інформації I повинен використовуватися метод регуляризації Тихонова [25].

Фундаментальні засади функціонування криптосистеми Фредгольма.

З урахуванням (1) та прийнятих припущень й обмежень **процедура шифрування** мовної інформації описуватиметься системою рівнянь вигляду [19]:

$$\begin{cases} z(t) = A_m \cos(2\pi f_m t + \varphi_m(t) + \varphi_m); \\ \int_a^b K(f,t)\, z(t)\, dt = z(f); \\ Z^f(k) = \dfrac{H^k}{k!}\left[\dfrac{d^k z^*(t)}{dt^k}\right]_{t=0}, \end{cases} \quad (2)$$

де $z(t)$ — мовна інформація, яка підлягає шифруванню та розшифруванню (вихідні дані);

A_m — амплітуда сигналу, *В*;

f_m — частота модулюючого коливання, *Гц*;

t — тривалість сигналу, *с*;

$\varphi_m(t)$ — фазова функція, *рад/с*;

φ_m — початкова фаза, *рад*;

$K(f,t)$ — таємний ключ, який є ядром інтегрального рівняння Фредгольма першого роду в області оригіналів;

$z(f)$ — шифрограма в області оригіналів, яка підлягає диференціальним перетворенням Пухова [26], $z(f) \equiv z^*(t) \approx z(t)$;

$Z^f(k)$ — шифрограма в області зображень (диференціальний спектр шифрограми), яка після аналогово-цифрового перетворення передається від Аліси до Боба відкритим каналом;

k — цілочисловий аргумент, $k =: 0, 1, 2, ..., m$;

H — масштабна стала, яка має розмірність аргументу t, $t = H$, *с*.

Процедура розшифрування мовної інформації набуватиме вигляду:

$$\begin{cases} Z_\alpha^f(k) = \dfrac{1}{\alpha} Z^f(k) - \dfrac{1}{\alpha} \sum\limits_{k=0}^{k=n} \dfrac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \dfrac{W(k)}{H^k}; \\ z(t) = \lim\limits_{\alpha \to 0} \sum\limits_{k=0}^{k=\infty} \left(\dfrac{t}{H}\right)^k Z_\alpha^f(k), \end{cases} \quad (3)$$

де $Z_\alpha^f(k)$ — розшифрована мовна інформація в області зображень, яка є рішенням зворотної некоректної задачі з точністю до параметра регуляризації α, знайденого на основі відповідного методу Тихонова [25];

$W(k)$ — згортка диференціальних спектрів підінтегральних функцій в області зображень, $W(k) = K(f,k) * Z^f(k) = \sum\limits_{l=0}^{l=k} K(f,k-l) Z^f(l)$ ($K(f,k)$ — таємний ключ, який є ядром інтегрального рівняння Фредгольма першого роду в області зображень).

МЕТОДОЛОГІЯ

Виходячи з концептуальних (1) та фундаментальних засад (2) й (3) функціонування криптосистеми Фредгольма, а також опираючись на приведені вище результати аналізу останніх досліджень і публікацій, на рис. 3 розроблену методологію подано у вигляді структурно-логічної схеми (рис. 1).

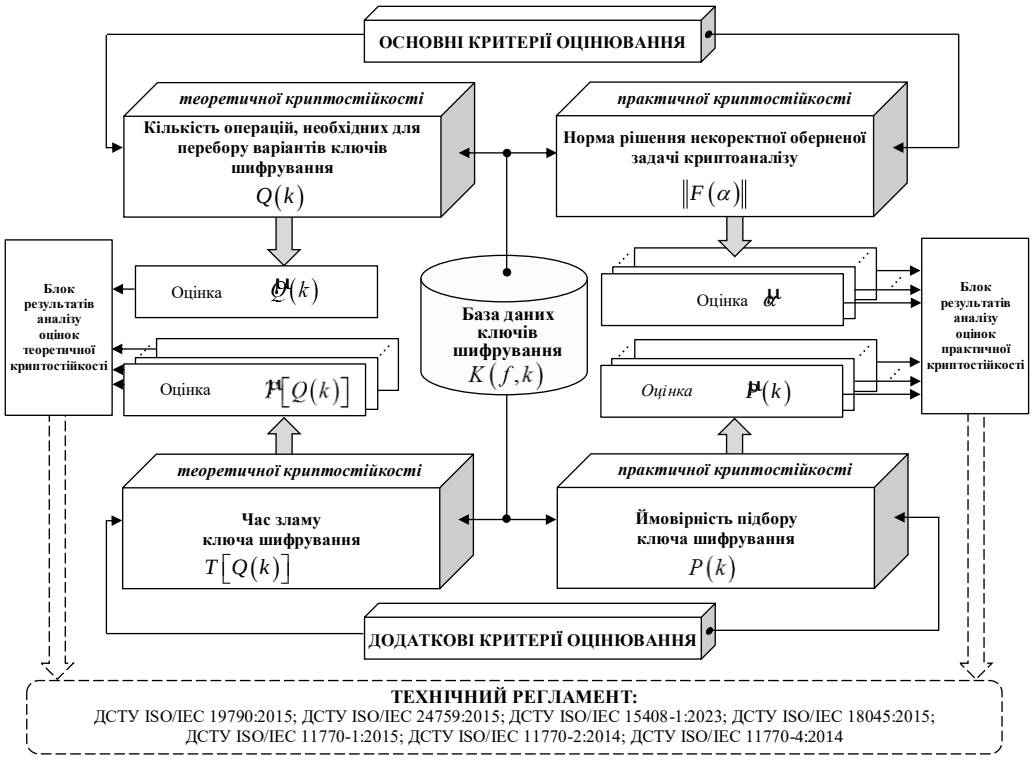

Рис. 1. Структурно-логічна схема методології оцінювання криптостійкості криптосистеми Фредгольма

Опис методології (див. рис. 1).

Оцінювання теоретичної криптостійкості. Теоретична криптостійкість криптосистеми Фредгольма є однією з її фундаментальних безпекових характеристик. Віднесення криптосистеми Фредгольма до класу теоретично стійких криптографічних систем дозволить стверджувати або навпаки спростувати твердження про наявність у неї такої властивості, як гарантована (в межах заданих обмежень) криптостійкість. Під теоретичною криптостійкістю криптосистеми Фредгольма розуміється її стійкість до криптоаналізу, що може бути оцінена всіма відомими методами за необмеженого часу та обсягу обчислювальних ресурсів [27].

Відомо, що в основу досліджуваної криптосистеми [19] покладено інтегральне рівняння Фредгольма першого роду [25] та диференціальні перетворення [26]. З цього випливає, що її теоретична криптостійкість забезпечуватиметься за рахунок зведення задачі криптоаналізу до класу задач з комбінаторною складністю. Доведемо це.

Лема про надекспоненціальну (гіпер-) складність задачі криптоаналізу криптосистеми Фредгольма.

Твердження: задача криптоаналізу криптосистеми Фредгольма відноситься до класу задач з надекспоненціальною (гіпер-) складністю.

Доведення. Нехай для класичних симетричних криптосистем, наприклад A5/1 або A5/2 при проведенні кібератаки повного перебору на ключ шифрування довжиною n біт обчислювальна складність їх криптоалгоритму $Q(n)$ визначається кількістю операцій, необхідних для перебору всіх можливих варіантів ключів. Тобто кількість згаданих операцій пов'язана з довжиною ключа в бітах виразом вигляду $Q(n)=2^n$. Тоді, виходячи з теорії складності алгоритмів [28], задачі такого класу в криптології відносять до класу задач з експоненціальною складністю.

Додержуючись викладеної вище логіки, описаної для класичних криптосистем і спираючись на базові положення комбінаторики визначимо складність підбору ключа шифрування для криптосистеми Фредгольма. Виходячи з того, що ключ шифрування є набором доданків у вигляді дискрет диференціального спектру [4], то, очевидно, при генеруванні ключа перестановка комбінації дискрет, тобто доданків, не змінює сам ключ. Тоді кількість можливих комбінацій ключа визначатиметься лише їх числом, тобто

$$C_k^{k-1}=\frac{k!}{(k-(k-1))!(k-1)!}=\frac{k!}{(k-1)!}=\frac{(k-1)!k}{(k-1)!}=k, \qquad (4)$$

де C_k^{k-1} — кількість можливих комбінацій ключа шифрування.

З виразу (4) випливає, що криптосистем Фредгольма може бути віднесена до теоретично стійких криптосистем, адже кількість операцій, необхідних для перебору ключа $Q(k)$ залежатиме лише від кількості дискрет k, тобто

$$Q(k)=k^k. \qquad (5)$$

Таким чином, на відміну від відомих класичних симетричних криптосистем складність криптоаналізу у криптосистемі Фредгольма, як випливає з виразу (5), визначається лише кількістю врахованих дискрет k. Оскільки в науковій фаховій літературі відсутня загальноприйнята назва класу задач вигляду (5) [29], то пропонуємо його назвати класом задач з надекспоненціальною (гіпер-) складністю.

Отже, лему доведено.

Вираз (5), зважаючи на доведеність леми, обрано як основний критерій оцінювання теоретичної складності (див. рис. 1).

Додатковим критерієм оцінювання теоретичної складності обрано час зламу ключа шифрування $T\left[Q(k)\right]$. На добовому інтервалі він може бути визначений виразом вигляду

$$T\left[Q(k)\right]=\frac{Q(k)}{60\times 60\times 24},\ доб. \tag{6}$$

Як видно з виразу (6) час зламу ключа шифрування $T\left[Q(k)\right]$ прямо пропорційно залежить від його складності $Q(k)$ на досліджуваному часовому інтервалі.

Оцінювання практичної криптостійкості.

Основним критерієм оцінювання практичної криптостійкості обрано норму рішення некоректної оберненої задачі криптоаналізу $\left\|F(\alpha)\right\|$:

$$\left\|F(\alpha)\right\|=\arg\min_{\alpha\to 0}\left\|Z^{f}_{\alpha_m}(k)-Z^{f}_{\alpha_{m-1}}(k)\right\|, \tag{7}$$

де α — параметр регуляризації, що є оцінкою (показником) практичної криптостійкості $\alpha>0$;

$Z^{f}_{\alpha_m}(k)$, $Z^{f}_{\alpha_{m-1}}(k)$ — регуляризація шифрограми на m- му та $m-1$- му раундах розшифрування відповідно.

Критерій (7) у науковій літературі називається критерієм квазіоптимальності, тобто евклідовою нормою або ще L^2- нормою [30]. Його знаходження забезпечує одночасно стійкість та точність розв'язку задачі розшифрування.

Перевагою обраного критерію (7) є відсутність потреби в додатковій інформації про діапазон зміни параметра регуляризації α, а також високою точністю його визначення внаслідок компромісу між точністю та стійкістю розв'язку оберненої некоректної задачі на основі інтегрального рівняння Фредгольма першого роду [30]. За критерієм (7) параметр регуляризації α знаходиться стабільно, навіть при незначних змінах у вихідній шифрограмі внаслідок зміни кількості дискрет ключа шифрування $K(f,k)$ та кількості дискрет диференціального спектра мовної інформації $Z^{f}(k)$, яка захищається.

В якості додаткового критерію оцінювання практичної криптостійкості використано ймовірність підбору ключа шифрування в області зображень $P(k)$. Ймовірність підбору ключа шифрування залежить від кількості всіх операцій, необхідних на його підбір та визначається як

$$P(k)=\frac{1}{Q(k)}. \tag{8}$$

У результаті одержані оцінки теоретичної $\left\{Q(k),T\left[Q(k)\right]\right\}$ та практичної криптостійкості $\left\{\alpha,P(k)\right\}$ після їх аналізу є підґрунтям для проведення технічного регламенту криптосистеми (див. рис. 1).

АНАЛІЗ РЕЗУЛЬТАТІВ

Для перевірки достовірності розробленої методології оцінювання криптостійкості, проведемо порівняння одержаних з її використанням оцінок для криптосистеми

Фредгольма (2), (3) та класичної криптосистеми потокового шифрування А5/1 за тих же вихідних умов.

Оцінювання теоретичної криптостійкості.

У табл. 1 приведено результати оцінювання *за критерієм обчислювальної складності* для найпростіших ключів шифрування на тестовій вибірці довжиною від 2 до 8 біт та від 2 до 8 дискрет відповідно.

Таблиця 1

Оцінки теоретичної криптостійкості за основним критерієм

Довжина ключа шифрування n, ***біт***	**Обчислювальна складність** $Q(n)$, ***кіл. оп.***	**Довжина ключа шифрування** k, ***дискрет***	**Обчислювальна складність** $Q(k)$, ***кіл. оп.***	**Ефективність,** ***рази***
2	4	2	4	1
4	16	4	256	16
6	64	6	46 656	729
8	256	8	16 777 216	65 536

Вибір ключів визначеної довжини (див. табл. 1) та одержані при цьому числові результати забезпечили розкриття принципової відмінності між відомою та досліджуваною криптосистемою. Таким чином, обчислювальна складність варіантів підбору ключа шифрування для криптосистеми Фредгольма зростає згідно з принципом надекспоненціальної (гіпер-) складності, що було доведено у лемі вище.

На рис. 2 наведено візуалізацію результатів оцінювання, поданих у табл. 1. Для наочності оцінки обчислювальної складності вісь ординат подано в логарифмічному масштабі.

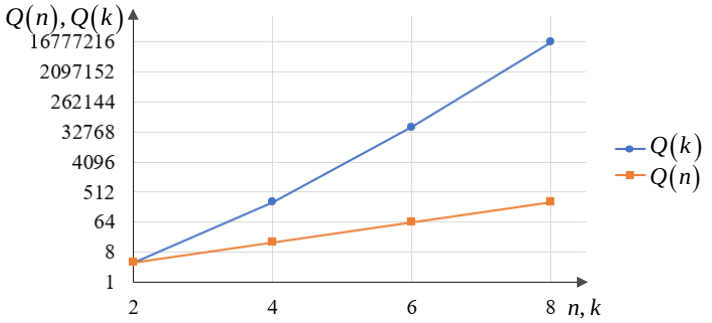

Рис. 2. Порівняльна характеристика теоретичної криптостійкості за критерієм обчислювальна складність

З результатів аналізу рис. 2 можна зробити висновок про те, що перші відмінності в обчислювальній складності між відомою криптосистемою потокового шифрування А5/1 та досліджуваною криптосистемою починають проявлятися на довжині ключа в 4 біти та 4 дискрети відповідно. Чим довший ключ шифрування в бітах та дискретах відповідно, тим різниця за кількістю операцій перебору варіантів ключа є більш вагомою. Виграш для досліджуваної криптосистеми має накопичувальний ефект $E(k,n)$ (див. рис. 2). Він може бути визначений згідно виразу вигляду $E(k,n)=k^k/2^n$, $k=0,1,\text{K},m$, $n=0,1,\text{K},m$.

У табл. 2 приведено *результати оцінювання за критерієм часу зламу ключа шифрування* для тих же вихідних умов.

Таблиця 2

Оцінки теоретичної криптостійкості за додатковим критерієм

Довжина ключа шифрування n, ***біт***	**Обчислювальна складність** $T_{\text{ч}}[Q(n)]$, ***діб***	**Довжина ключа шифрування** k, ***дискрет***	**Обчислювальна складність** $T_{\text{ч}}[Q(k)]$, ***діб***
2	0.000	2	0.000
4	0.000	4	0.003
6	0.001	6	0.540
8	0.003	8	194.181

Результати оцінювання приведені в табл. 2 дозволяють зробити такий основний висновок. У практичних застосунках криптосистема Фредгольма на восьми дискретах забезпечуватиме захищеність мовної інформації (конфіденційності) до 194 *діб*. У разі необхідності забезпечення вищих показників захищеності за заначений, кількість дискрет при побудові системи може бути збільшена. Слід зауважити, що при цьому зростуть вимоги до апаратної реалізації засобу шифрування, а відповідно і його вартості.

Оцінювання практичної криптостійкості.

Під час оцінювання практичної криптостійкості *за основним критерієм* використано гармонічну математичну модель, запропоновану в [19]. Знайшовши норму рішення (7) на кожному раунді розшифрування з використанням системи аналітичної математики *Maple* нижче побудовано графік функції $\|F(\alpha)\|$ (рис. 3).

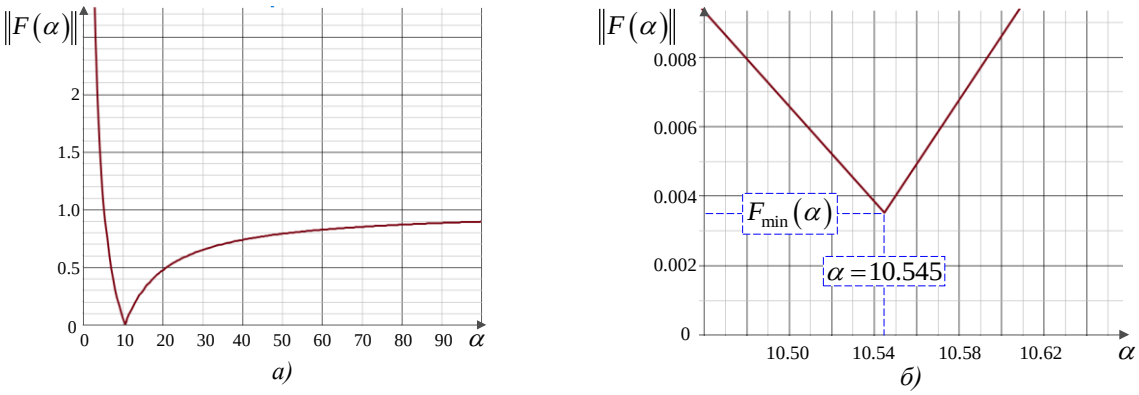

Рис. 3. Результати оцінювання практичної криптостійкості за критерієм норми рішення некоректної оберненої задачі криптоаналізу: а — на всьому діапазоні регуляризації $\alpha = 0..100$*; б — на діапазоні регуляризації* $\alpha = 10.46..10.64$

Побудований графік (див. рис. 3) використовується для визначення шуканого параметру регуляризації α за мінімумом функції $\|F(\alpha)\|$.

Результати оцінювання практичної криптостійкості *за додатковим критерієм* — критерієм ймовірності підбору ключа шифрування, приведено в табл. 3. На рис. 4 подано результати візуалізації одержаних оцінок.

Таблиця 3

Оцінки практичної криптостійкості за додатковим критерієм

Довжина ключа шифрування n, *біт*	**Ймовірність підбору ключа шифрування для класичної криптосистеми, $P(n)$**	**Довжина ключа шифрування k, *дискрет***	**Ймовірність підбору ключа шифрування для криптосистеми Фредгольма, $P(k)$**
2	0.25	2	0.25
4	0.06	4	4×10^{-3}
6	0.02	6	0.21×10^{-6}
8	4×10^{-3}	8	0.6×10^{-8}

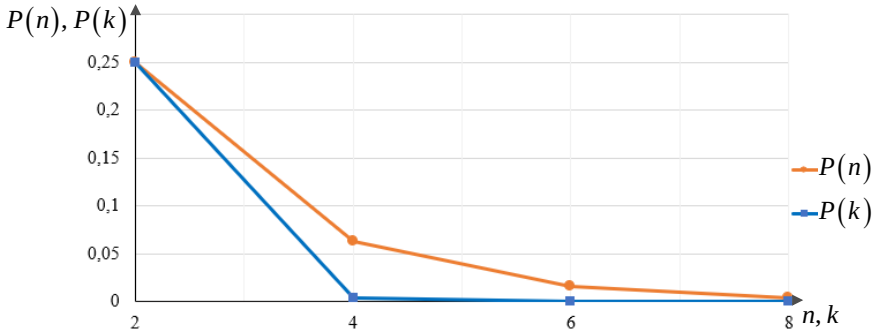

Рис. 4. Порівняльна характеристика практичної криптостійкості за додатковим критерієм

З аналізу графіка (див. рис. 4) випливає, що криптосистема Фредгольма є більш практично захищеною, порівняно з досліджуваним аналогом. Ефект криптостійкості для неї починає проявлятися вже на перших чотирьох дискретах, а на восьми дискретах відмінність вже сягає шести порядків.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження доведено, що криптосистема Фредгольма є теоретично стійкою. Даний висновок накладає суттєве обмеження на її практичне застосування. Наприклад, на практиці для захисту мовної інформації яка описується класом гармонічних математичних моделей наразі поки можливо реалізувати криптосистему лише на восьми дискретах. Така криптосистема забезпечуватиме конфіденційність мовної інформації не більше 197 діб від моменту її шифрування. Інші прикладні застосунки потребують додаткових досліджень, що і вважатиметься подальшою перспективою розвитку даної роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Броншпак, Г., Громико, І., Доценко, С., та ін. (2014). Криптографія нового покоління: Інтегральні рівняння як альтернатива алгебраїчної методології. *Прикладна електроніка*, 3, 337–349.
2. Грищук, Р. В., & Грищук, О. М. (2019). Узагальнена модель криптосистеми Фредгольма. *Кібербезпека: освіта, наука, техніка*, 4(4), 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423.
3. Hryshchuk, O. (2024). Mathematical model of a symmetrical cryptographic system for the protection of speech information based on differential transformations. *Cybersecurity: Education, Science, Technique,* 1(25), 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409.
4. Грищук, О. М. (2024). Алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень. *Сучасний захист інформації*, 4(60), 6–15. https://doi.org/10.31673/2409-7292.2024.040001.
5. Корченко, О. Г., & Грищук, О. М. (2024). Метод криптографічного захисту мовної інформації на основі диференціальних перетворень. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць*, 27(I), 4–19. https://doi.org/10.46972/2076-1546.2024.27.01.
6. Сукнов, М., Громико, І., & Перчик, Є. (2020). Спосіб криптологічних перетворень даних. *Cybersecurity and Computer Science*, *2*(18), 33–40. https://doi.org/10.26565/2519-2310-2020-2-04
7. Marinakis, G. (2022). Evaluating the security of cryptographic systems. *Scientific Press International Limited*. https://surl.li/bkhsrj.
8. Gorbenko, I. D., Kuznetsov, O. O., Gorbenko, Y. I., Vdovenko, S. V., Tymchenko, V. V., & Lutsenko, M. V. (2021). Studies on statistical analysis and performance evaluation for some stream ciphers. International *Journal of Computing*, 20(1). https://www.computingonline.net/computing/article/view/1277.
9. ДСТУ ISO/IEC 19790:2015. Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (ISO/IEC 19790:2012, IDT). Київ: ДП «УкрНДНЦ», 2016. – 88 с. – Набув чинності 01.01.2017. – На заміну: ДСТУ ISO/IEC 19790:2014.
10. ДСТУ ISO/IEC 24759:2015. Інформаційні технології. Методи захисту. Вимоги до тестування криптографічних модулів (ISO/IEC 24759:2012, IDT). Київ: ДП «УкрНДНЦ», 2016. – 104 с. – Набув чинності 01.01.2017. – На заміну: ДСТУ ISO/IEC 24759:2014.
11. ДСТУ ISO/IEC 15408-1:2023. Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT). Київ: ДП «УкрНДНЦ», 2023. – 56 с. – Набув чинності 01.07.2023. – На заміну: ДСТУ ISO/IEC 15408-1:2015.
12. ДСТУ ISO/IEC 18045:2015. Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (ISO/IEC 18045:2008, IDT). Київ: ДП «УкрНДНЦ», 2016. – 112 с. – Набув чинності 01.01.2017. – На заміну: ДСТУ ISO/IEC 18045:2014.
13. ДСТУ ISO/IEC 11770-1:2015. Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення (ISO/IEC 11770-1:2010, IDT). Київ: ДП «УкрНДНЦ», 2016. – 56 с. – Набув чинності 01.01.2017. – На заміну: ДСТУ ISO/IEC 11770-1:2014.
14. ДСТУ ISO/IEC 11770-2:2014. Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 2. Механізми, що використовують симетричні методи (ISO/IEC 11770-2:2008, IDT). Київ: ДП «УкрНДНЦ», 2015. – 72 с. – Набув чинності 01.01.2016. – На заміну: ДСТУ ISO/IEC 11770-2:2006.
15. ДСТУ ISO/IEC 11770-3:2014. Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 3. Механізми, що використовують асиметричні методи розроблення (ISO/IEC 11770-3:2008, IDT). Київ: ДП «УкрНДНЦ», 2015. – 64 с. – Набув чинності 01.01.2016. – На заміну: ДСТУ ISO/IEC 11770-3:2006.
16. ДСТУ ISO/IEC 11770-4:2014. Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 4. Механізми, засновані на нестійких секретах (ISO/IEC 11770-4:2007, IDT). Київ: ДП «УкрНДНЦ», 2015. – 48 с. – Набув чинності 01.01.2016. – Новий стандарт.
17. ДСТУ ISO/IEC 11770-5:2014. Інформаційні технології. Методи забезпечення безпеки. Керування ключами. Частина 5. Група керування ключами (ISO/IEC 11770-5:2011, IDT). Київ: ДП «УкрНДНЦ», 2015. – 52 с. – Набув чинності 01.01.2016. – Новий стандарт.
18. ДСТУ ISO/IEC 29115:2014. Інформаційні технології. Методи забезпечення безпеки. Схема забезпечення автентифікації безпеки (ISO/IEC 29115:2013, IDT). Київ: ДП «УкрНДНЦ», 2015. – 68 с. – Набув чинності 01.01.2017. – На заміну: ДСТУ ISO/IEC 29115:2013.

19. Грищук, О. М. (2025). *Симетрична криптографічна система на основі інтегральних перетворень* (Дисертація доктора філософії, Державний університет інформаційно-комунікаційних технологій). Державний університет інформаційно-комунікаційних технологій. https://duikt.edu.ua/uploads/p_2807_74835522.pdf.
20. Beyne, T. (2025). Cryptanalysis of a nonlinear filter-based stream cipher. *IACR Cryptology ePrint Archive*, 2025/197. https://eprint.iacr.org/2025/197.
21. Biham, E., & Dunkelman, O. (2007). Differential cryptanalysis in stream ciphers. *IACR Cryptology ePrint Archive*, 2007/218. https://eprint.iacr.org/2007/218.
22. Canteaut, A. (2025). Linear cryptanalysis for stream ciphers. In S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 1–7). Cham: Springer. https://doi.org/10.1007/978-3-030-71522-9_356.
23. Esmaeili Salehani, Y. (2013). *Side channel attacks on symmetric key primitives* (Master's thesis, Queen's University). Library and Archives Canada. https://central.bac-lac.gc.ca/.item?id=TC-QMG-7765&op=pdf&app=Library&oclc_number=896966803.
24. Devlin, I. (2007). *Stream ciphers for secure display* [Doctoral dissertation, Durham University]. Retrieved from Durham E-Theses.
25. Ito, K., & Jin, B. (2014). *Inverse problems: Tikhonov theory and algorithms* (Vol. 22). World Scientific Publishing Company.
26. Pukhov, G. E. (1978). Computational structure for solving differential equations by Taylor transformations. *Cybernetics and Systems Analysis*, 14, 383–390. https://doi.org/10.1007/BF01074670.
27. Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). John Wiley & Sons.
28. Arora, S., & Barak, B. (2009). *Computational complexity: A modern approach.* Cambridge University Press. Retrieved from https://theory.cs.princeton.edu/complexity/book.pdf.
29. Горбенко, Ю. І., Корченко, О. Г., & Коваль, В. В. (2011). Сутність та оцінка стійкості криптографічних перетворень в кільцях зрізаних поліномів. *Захист інформації,* (4), 45–52.
30. Bauer, F., & Kindermann, S. (2009). Recent results on the quasi-optimality principle. *Journal of Inverse and Ill-Posed Problems*, 17(1), 5–18.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Ruslan V. Hryshchuk
Laureate of the Borys Paton National Prize of Ukraine,
Honoured Scientist and Engineer of Ukraine
Doctor of Technical Sciences, Professor, Colonel
Deputy Commandant of the Odesa Military Academy, Military Academy (Odesa), Odesa, Ukraine
ORCID ID: 0000-0001-9985-8477
Prof.hry@gmail.com

Olha M. Hryshchuk
PhD, Lieutenant Colonel
Postgraduate Student in National Defence University of Ukraine,
National Defence University of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-6957-4748
Hry.olha@gmail.com

EVALUATING CRYPTOGRAPHIC RESILIENCE IN THE FREDHOLM CRYPTOSYSTEM: METHODOLOGY AND RESULTS ANALYSIS

Abstract. The rapid advancement of quantum cryptanalysis technologies poses a growing threat to the security of existing asymmetric and symmetric cryptosystems. This challenge has accelerated the global and Ukrainian development of post-quantum cryptography, including the creation of new algorithms and innovative cryptosystems based on unconventional mathematical principles. One such system is the Fredholm cryptosystem, which is both conceptually novel and largely unexplored from a cybersecurity standpoint. Unlike conventional cryptographic solutions grounded in discrete mathematics, the Fredholm system operates on the basis of integral calculus. Due to the absence of theoretical and practical evaluations of its cryptographic strength, the system's implementation remains limited. To address this gap, the present study introduces a methodology for assessing the cryptographic resilience of the Fredholm cryptosystem. The proposed framework focuses on its weakest component—the encryption key's resistance to brute-force attacks. The primary theoretical metric is the number of operations required to exhaustively search the key space. Using combinatorial analysis, the study proves a lemma demonstrating that resilience depends solely on the number of discrete elements in the key's differential spectrum, rather than their permutation order. Time required to compromise the key is considered as an additional metric. For practical resilience, the study employs the norm of the solution to the inverse ill-posed decryption problem, which determines the regularization parameter affecting both stability and accuracy. The probability of successful key recovery is also introduced as a supplementary criterion. The results show that the Fredholm cryptosystem's practical resilience increases with the number of operations needed to identify the discrete differential spectrum of the encryption key. Based on the findings, the paper outlines the system's strengths and limitations and offers recommendations for its application in critical information and communication infrastructures.

Keywords: differential transformations; cyberattack; cybersecurity; cryptosystem; cryptographic resilience; encryption key; regularization parameter

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bronshpak, H., Hromyko, I., Dotsenko, S., et al. (2014). Next-generation cryptography: Integral equations as an alternative to algebraic methodology. *Applied Electronics*, 3, 337–349.
2. Hryshchuk, R. V., & Hryshchuk, O. M. (2019). Generalized model of the Fredholm cryptosystem. *Cybersecurity: Education, Science, Technique*, 4(4), 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423.
3. Hryshchuk, O. (2024). Mathematical model of a symmetrical cryptographic system for the protection of speech information based on differential transformations. *Cybersecurity: Education, Science, Technique*, 1(25), 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409.

4. Hryshchuk, O. M. (2024). Encryption key generation algorithm in a symmetric cryptographic system for speech information protection based on differential transformations. *Modern Information Protection*, 4(60), 6–15. https://doi.org/10.31673/2409-7292.2024.040001.
5. Korchenko, O. H., & Hryshchuk, O. M. (2024). Method of cryptographic protection of speech information based on differential transformations. Problems of Development, Testing, *Application and Operation of Complex Information Systems: Scientific Papers Collection*, 27(I), 4–19. https://doi.org/10.46972/2076-1546.2024.27.01.
6. Suknov, M., Hromyko, I., & Perchyk, Y. (2020). Method of cryptological data transformations. *Cybersecurity and Computer Science*, 2(18), 33–40. https://doi.org/10.26565/2519-2310-2020-2-04
7. Marinakis, G. (2022). Evaluating the security of cryptographic systems. *Scientific Press International Limited*. https://surl.li/bkhsrj.
8. Gorbenko, I. D., Kuznetsov, O. O., Gorbenko, Y. I., Vdovenko, S. V., Tymchenko, V. V., & Lutsenko, M. V. (2021). Studies on statistical analysis and performance evaluation for some stream ciphers. *International Journal of Computing*, 20(1). https://www.computingonline.net/computing/article/view/1277.
9. State Enterprise "UkrNDNC". (2016). DSTU ISO/IEC 19790:2015. *Information technology – Security techniques – Security requirements for cryptographic modules* (ISO/IEC 19790:2012, IDT). Kyiv, Ukraine.
10. State Enterprise "UkrNDNC". (2016). DSTU ISO/IEC 24759:2015. *Information technology – Security techniques – Test requirements for cryptographic modules* (ISO/IEC 24759:2012, IDT). Kyiv, Ukraine.
11. State Enterprise "UkrNDNC". (2023). DSTU ISO/IEC 15408-1:2023. *Information technology – Cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model* (ISO/IEC 15408-1:2022, IDT). Kyiv, Ukraine.
12. State Enterprise "UkrNDNC". (2016). DSTU ISO/IEC 18045:2015. *Information technology – Security techniques – Methodology for IT security evaluation* (ISO/IEC 18045:2008, IDT). Kyiv, Ukraine.
13. State Enterprise "UkrNDNC". (2016). DSTU ISO/IEC 11770-1:2015. *Information technology – Security techniques – Key management – Part 1: General* (ISO/IEC 11770-1:2010, IDT). Kyiv, Ukraine.
14. State Enterprise "UkrNDNC". (2015). DSTU ISO/IEC 11770-2:2014. *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques* (ISO/IEC 11770-2:2008, IDT). Kyiv, Ukraine.
15. State Enterprise "UkrNDNC". (2015). DSTU ISO/IEC 11770-3:2014. *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques* (ISO/IEC 11770-3:2008, IDT). Kyiv, Ukraine.
16. State Enterprise "UkrNDNC". (2015). DSTU ISO/IEC 11770-4:2014. *Information technology – Security techniques – Key management – Part 4: Mechanisms based on unstable secrets* (ISO/IEC 11770-4:2007, IDT). Kyiv, Ukraine.
17. State Enterprise "UkrNDNC". (2015). DSTU ISO/IEC 11770-5:2014. *Information technology – Security techniques – Key management – Part 5: Group key management* (ISO/IEC 11770-5:2011, IDT). Kyiv, Ukraine.
18. State Enterprise "UkrNDNC". (2015). DSTU ISO/IEC 29115:2014. *Information technology – Security techniques – Entity authentication assurance framework* (ISO/IEC 29115:2013, IDT). Kyiv, Ukraine.
19. Hryshchuk, O. M. (2025). *Symmetric cryptographic system based on integral transformations* (PhD dissertation, State University of Information and Communication Technologies). https://duikt.edu.ua/uploads/p_2807_74835522.pdf.
20. Beyne, T. (2025). Cryptanalysis of a nonlinear filter-based stream cipher. *IACR Cryptology ePrint Archive*, 2025/197. https://eprint.iacr.org/2025/197
21. Biham, E., & Dunkelman, O. (2007). Differential cryptanalysis in stream ciphers. *IACR Cryptology ePrint Archive*, 2007/218. https://eprint.iacr.org/2007/218.
22. Canteaut, A. (2025). Linear cryptanalysis for stream ciphers. In S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 1–7). Springer. https://doi.org/10.1007/978-3-030-71522-9_356.
23. Esmaeili Salehani, Y. (2013). *Side channel attacks on symmetric key primitives* (Master's thesis, Queen's University). Library and Archives Canada. https://central.bac-lac.gc.ca/.item?id=TC-QMG-7765&op=pdf&app=Library&oclc_number=896966803.
24. Devlin, I. (2007). *Stream ciphers for secure display* (Doctoral dissertation, Durham University). Durham E-Theses.
25. Ito, K., & Jin, B. (2014). Inverse problems: Tikhonov theory and algorithms (Vol. 22). *World Scientific Publishing Company*.

26. Pukhov, G. E. (1978). Computational structure for solving differential equations by Taylor transformations. Cybernetics and Systems Analysis, 14, 383–390. https://doi.org/10.1007/BF01074670
27. Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.).* John Wiley & Sons.
28. Arora, S., & Barak, B. (2009). Computational complexity: A modern approach. *Cambridge University Press.* https://theory.cs.princeton.edu/complexity/book.pdf.
29. Horbenko, Y. I., Korchenko, O. H., & Koval, V. V. (2011). Essence and evaluation of the resilience of cryptographic transformations in rings of truncated polynomials. *Information Protection,* (4), 45–52.
30. Bauer, F., & Kindermann, S. (2009). Recent results on the quasi-optimality principle. *Journal of Inverse and Ill-Posed Problems,* 17(1), 5–18.