ISSN 2076-1546
УДК 004.056 DOI: 10.46972/2076-1546.2024.27.01

О. Г. Корченко, О. М. Грищук

МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ

Проблема безпеки інформації, яка циркулює в каналах зв'язку, постійно актуалізується. Особливо гостро вона стоїть для VoIP-телефонії військового призначення або подвійного використання. Це пов'язано й зі зростанням цінності конфіденційної інформації, яка становить інтерес для кіберзлочинців, і з нарощенням технологічної складності кібератак за одночасного збільшення продуктивності технічних засобів несанкціонованого отримання інформації. Серед відомих механізмів забезпечення кібербезпеки мовної інформації, яка циркулює в каналах зв'язку, одне з ключових місць займають криптографічні методи її захисту. Найчастіше для організації безпечного VoIP-трафіку використовують протоколи безпеки SRTP, які реалізують симетричний криптографічний алгоритм шифрування AES. Водночас потенційна компрометація найкращого симетричного криптографічного алгоритму AES-256 потребує пошуку нових нетривіальних підходів до удосконалення механізмів забезпечення кібербезпеки. Одним із них є підхід, який ґрунтується на використанні моделі криптосистеми Фредгольма. Згадана криптографічна система належить до класу симетричних криптографічних систем, але до сьогодні, через відсутність науково обґрунтованих криптографічних алгоритмів, вона ще й досі не набула практичного впровадження. Для вирішення цієї суперечності в дослідженні з урахуванням принципу О. Керкгоффса розроблено метод криптографічного захисту мовної інформації на основі диференціальних перетворень академіка НАН України Г. Пухова. Запропонований метод дозволяє отримати шифр у вигляді диференціального спектра, який стійкий до відомих методів криптоаналізу. У статті розроблено алгоритм реалізації цього методу. Наведено результати шифрування та розшифрування мовної інформації. Збіжність результатів моделювання з іншими відомими методами підтверджує роботоздатність розробленого методу.

Ключові слова: *симетричний криптографічний алгоритм; диференціальні перетворення; ключ шифрування; диференціальний спектр; шифр; дискрета; гарантована криптостійкість; обернена задача; інтегральне рівняння Фредгольма першого роду.*

Постановка проблеми в загальному вигляді. VoIP-телефонія, порівняно з традиційними технологіями організації комунікацій між абонентами інформаційного обміну, має низку ключових переваг, зокрема її дешевизна та висока якість зв'язку [1] і надалі сприятимуть інтенсивному впровадженню в епоху діджиталізації технологій VoIP-телефонії в усі сфери діяльності суспільства. Разом із тим, незважаючи на застосовувані механізми забезпечення кібербезпеки VoIP-трафіку, наприклад,

шифрування з використанням таких безпечних протоколів, як IPSec, SSH та SRTP [2], які забезпечують конфіденційність [3], [4] засобів автентифікації, VPN-тунелювання тощо, мовна інформація й надалі стає об'єктом перехоплення технічних засобів несанкціонованого отримання інформації [5]–[7] та кібератак різних типів. Такими кібератаками з боку недобросовісних конкурентів можуть бути MITM, NAT Attack [8], [9]. Саме тому проблема забезпечення кібербезпеки VoIP-телефонії є та залишатиметься актуальною. Особливо гостро вона стоїть для VoIP-телефонії військового призначення та подвійного використання, а також інших критичних систем [10].

Аналіз останніх досліджень і публікацій. У публікації [6] достатньо ґрунтовно розкрито проблеми захисту мовної інформації за технологією VoIP-телефонії, зокрема зазначено, що криптографічному захисту підлягає сигнальний трафік, під яким розуміється мовна інформація, а також способи генерування (розподілу) ключів для протоколів її захисту.

Із [8] та [11] відомо, що серед протоколів захисту сигнального трафіку найбільшого поширення отримали SIP (стандарт IETF RFC 3261) та SIPS (стандарт RFC 3261). Разом із тим на практиці застосовують й інші протоколи під час роботи із сигнальним трафіком, наприклад такі [6], [12]: H.323 (стандарти ITU-T); MGCP і Megaco (стандарти ITU-T і IETF); MiNET (стандарти Mitel) тощо.

Зважаючи на стрімкий розвиток інформаційних технологій, зокрема й на основі квантових комп'ютерів, нині в галузі криптографії розробляють й інші, відмінні від проаналізованих вище класичних підходів, методи криптографічного захисту інформації [13].

На сучасному етапі розвитку науки й техніки під час шифрування та розшифрування в асиметричних та симетричних криптографічних системах використовують такі математичні методи: арифметика залишків; методи заміни та перестановки; метод шифрування за допомогою матриць; методи шифрування на основі теорії множин, еліптичних кривих тощо. Вони є математичним підґрунтям для розроблення відповідних безпечних протоколів. Так, для захисту мовної інформації в [14]–[17] запропоновано інноваційну технологію криптографічного захисту на диференціальних перетвореннях як новий засіб забезпечення кібербезпеки VoIP-трафіку. Основу цієї технології становить класична симетрична криптографічна система [18]–[20]. Водночас її відмінністю від відомих є застосування як криптографічного алгоритму інтегрального рівняння Фредгольма першого роду та операційного методу диференціальних перетворень академіка НАН України Г. Пухова [21]. Також відмінною є процедура генерування ключа шифрування на основі відповідного алгоритму [22], [23]. Однак ні в [13], ні в інших наукових публікаціях ґрунтовно не розкрито процедури шифрування та розшифрування для такого перспективного підходу. Також жоден із відомих методів не дає змоги шифрувати й розшифровувати мовну інформацію в симетричній криптографічній системі Фредгольма [19], [20], що стримує подальше розроблення новітніх методів шифрування та безпечних протоколів на їхній основі.

Формулювання завдання дослідження. Метою статті є розроблення методу криптографічного захисту мовної інформації на основі диференціальних перетворень.

Виклад основного матеріалу. Для практичної реалізації запропонованої в [13] методології в [24] наведено результати аналізу відомих математичних моделей мовної інформації, а в [25] обґрунтовано вибір такої моделі у вигляді гармонічного сигналу

$$z(t) = A_c \cos(2\pi f_c t + \varphi_c(t) + \varphi_c), \quad (1)$$

де $z(t)$ – математична модель мовної інформації, що підлягає шифруванню;

A_c – амплітуда сигналу, В;

f_c – несуча частота, Гц;

t – час передачі голосового повідомлення, с;

$\varphi_c(t)$ – фазова функція, рад/с;

φ_c – початкова фаза, рад.

Через зростаючі в комунікаційних системах потоки мовної інформації (1), яка має підлягати криптографічному захисту, основною вимогою, крім гарантованої теоретичної та практичної криптостійкості алгоритмів шифрування, залишається вимога до її шифрування в реальному масштабі часу. Відомі чисельні методи [26] (Ньютона – Котеса, Гаусса, Чебишева), що ґрунтуються на використанні квадратурних формул, суттєво обмежені в застосуванні в криптографічних системах, адже потребують значного обсягу обчислень. Тому для шифрування мовної інформації в реальному масштабі часу в симетричній криптографічній системі Фредгольма у [18]–[20] запропоновано застосувати точний операційний метод диференціальних перетворень академіка НАН України Г. Пухова [21]. Цей метод уже використовують у багатьох галузях науки й техніки. Наприклад, його було застосовано в електротехніці, спектроскопії та інших галузях, у яких фізичні процеси описуються у вигляді інтегральних та диференціальних рівнянь. Уперше в галузі кібербезпеки цей метод було використано для моделювання процесів кібернападу на державні інформаційні ресурси [27].

На відміну від відомих операційних методів інтегральних перетворень Лапласа та Фур'є, під час шифрування мовної інформації диференціальні перетворення ґрунтуються на переведенні оригіналів в область зображень за допомогою операції диференціювання [21]. У такому разі шифрування мовної інформації в області зображень для збереження точності вихідної математичної моделі мовної інформації без часового аргументу зводиться до виконання чотирьох арифметичних операцій в аналітичному або чисельному вигляді: множення, ділення, додавання та віднімання, – що практично реалізуються сучасними апаратними або програмними засобами криптографічного захисту. Крім того, ще однією перевагою методу диференціальних перетворень є значно простіша процедура розшифрування мовної інформації під час переходу з області зображень в область оригіналів.

Згідно з [21], [28] та [29] диференціальні перетворення передбачають подання вихідної математичної моделі степеневим рядом Тейлора із центром розкладання ряду в точці $t = 0$. Пряме і, відповідно, зворотне перетворення в загальному вигляді описують такими виразами [21]:

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \;\underline{\cdot}\; x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \qquad (2)$$

де $x(t)$ – оригінал, який є безперервною, що диференціюється нескінченну кількість разів, і обмеженою разом з усіма своїми похідними функцією дійсного аргументу *t*;

$X(k)$ і $\underline{x}(k)$ – рівноцінні позначення диференціального спектра за конкретних числових значень параметрів моделі.

Кількість дискрет диференціального спектра мовної інформації визначає точність розшифрування мовної інформації в області оригіналів і на практиці обмежується першими трьома-п'ятьма ненульовими дискретами.

Підвищення точності моделювання на основі диференціальних перетворень за потреби можна досягти двома шляхами. Перший – це збільшення кількості дискрет диференціального спектра досліджуваної моделі, але в цьому разі зростатиме аналітична складність моделі. І другий шлях – це застосування диференціальних перетворень нетейлорівського типу, але для цього потрібно мати апріорну інформацію про вигляд шуканої апроксимаційної функції.

Суть методу. Шифрування мовної інформації. Нехай у симетричній криптографічній системі захисту інформації [19], [20] шифруванню підлягає мовна інформація, яка від абонента *Alice* до абонента *Вов* передається протягом деякого фіксованого часу *T*, с. У загальному вигляді мовна інформація описується гармонічною математичною моделлю аналогового сигналу $z(t)$ (1) [25].

Шифрування мовної інформації $z(t)$ пропонуємо здійснювати на основі диференціальних перетворень (2) за криптографічним алгоритмом, що в загальному вигляді описується інтегральним рівнянням Фредгольма першого роду [17]:

$$\int_a^b K(\omega, t)\, z(t)\, dt = z(\omega),\ a \le \omega \le b,\ a \le t \le b. \qquad (3)$$

У виразі (3) прийнято такі позначення: $K(\omega, t)$ – секретний ключ шифрування (ядро інтегрального рівняння Фредгольма першого роду), що підлягає генеруванню; $z(\omega)$ – зашифровані дані (шифрограма), які відкритим каналом від відправника *Alice* передаються до одержувача *Bob.*

Головною перевагою шифрування за криптографічним алгоритмом (3) є гарантована теоретична та практична криптостійкість, яка випливає з некоректності за Ж. Адамаром [30], [31], адже без знання ключа шифрування задача дешифрування є практично не розв'язуваною [17]. Безпека шифру $z(\omega)$ залежить від складності розв'язання оберненої некоректної задачі розшифрування [17], [30], [32], яка описується інтегральним рівнянням Фредгольма першого роду (3). Зазначені положення підтверджують гіпотезу Н. Фергюсона [33], що слугує науковим підґрунтям для подальших досліджень.

На основі згенерованого згідно з (2) відповідним алгоритмом [23] ключа шифрування $K(\omega,t)\cdot \bar{K}(\omega,k)$ здійснюється шифрування мовної інформації $z(t)$. Для цього застосовується метод диференціальних перетворень (2) до (1) та (3). У результаті отримуємо диференціальний спектр $Z^k(\omega)$, що є зашифрованою мовною інформацією $z(\omega)$ в області зображень.

Розшифрування мовної інформації. Нехай розшифруванню підлягає шифрограма, що описується диференціальним спектром вигляду $Z^k(\omega)$, яку отримав одержувач *Bob* відкритим каналом зв'язку. Одержувачу також відомий секретний ключ шифрування $K(\omega,k)$, переданий йому через закритий канал. Розшифрування шифрограми на стороні одержувача пропонуємо здійснювати на основі диференціальних перетворень (2) за криптографічним алгоритмом, що в загальному вигляді описується методом регуляризації академіка М. Тихонова [31] та Д. Філліпса [32]:

$$z(\omega)=\lim_{\alpha\to 0} z_{\alpha}(\omega), \tag{4}$$

де $z_a(\omega)$ – розшифрована мовна інформація з точністю до параметра регуляризації a, при цьому $a>0,\ a\to 0$.

У результаті застосування методу регуляризації (4) та зворотного диференціального перетворення (2) розшифруванню підлягає мовна інформація, яка передавалася (1). На цьому метод завершує свою роботу.

Блок-схему методу криптографічного захисту мовної інформації на основі диференціальних перетворень наведено на рис. 1.

Алгоритм методу має певні кроки (див. рис. 1).

У ході шифрування мовної інформації алгоритм методу складається з восьми кроків.

Крок 1. Генерування мовної інформації $z(t)=A_c\cos(\omega_c t)$, де $\omega_c=2\pi f_c$ – циклічна частота, рад/с; $\varphi_c(t)=0$ рад/с; $\varphi_c=0$ рад.

Крок 2. Формування моделі диференціального спектра мовної інформації $Z(k)$ на основі диференціальних перетворень (2): $Z(k)=A_c\dfrac{(\omega_c H)^k}{k!}\cos\dfrac{\pi k}{2}$.

Крок 3. Розрахунок нульової дискрети для k:= 0: $Z(0)=A_c$.

Крок 4. Розрахунок першої дискрети для k:= 1: $Z(1)=A_c\dfrac{(\omega_c H)}{1!}\cos\dfrac{\pi}{2}=0$.

Крок 5. Розрахунок n-ї дискрети для k:= n: $Z(n)=A_c\dfrac{(\omega_c H)^n}{n!}\cos\dfrac{\pi n}{2}$.

Крок 6. Побудова диференціального спектра мовної інформації:

$$S(k)=\sum_{k=0}^{k=n}Z(k)=Z(0)+Z(1)+\ldots+Z(n)=A_c-A_c\frac{(\omega_c H)^2}{2}+\ldots+A_c\frac{(\omega_c H)^n}{n!}\cos\frac{\pi n}{2}.$$

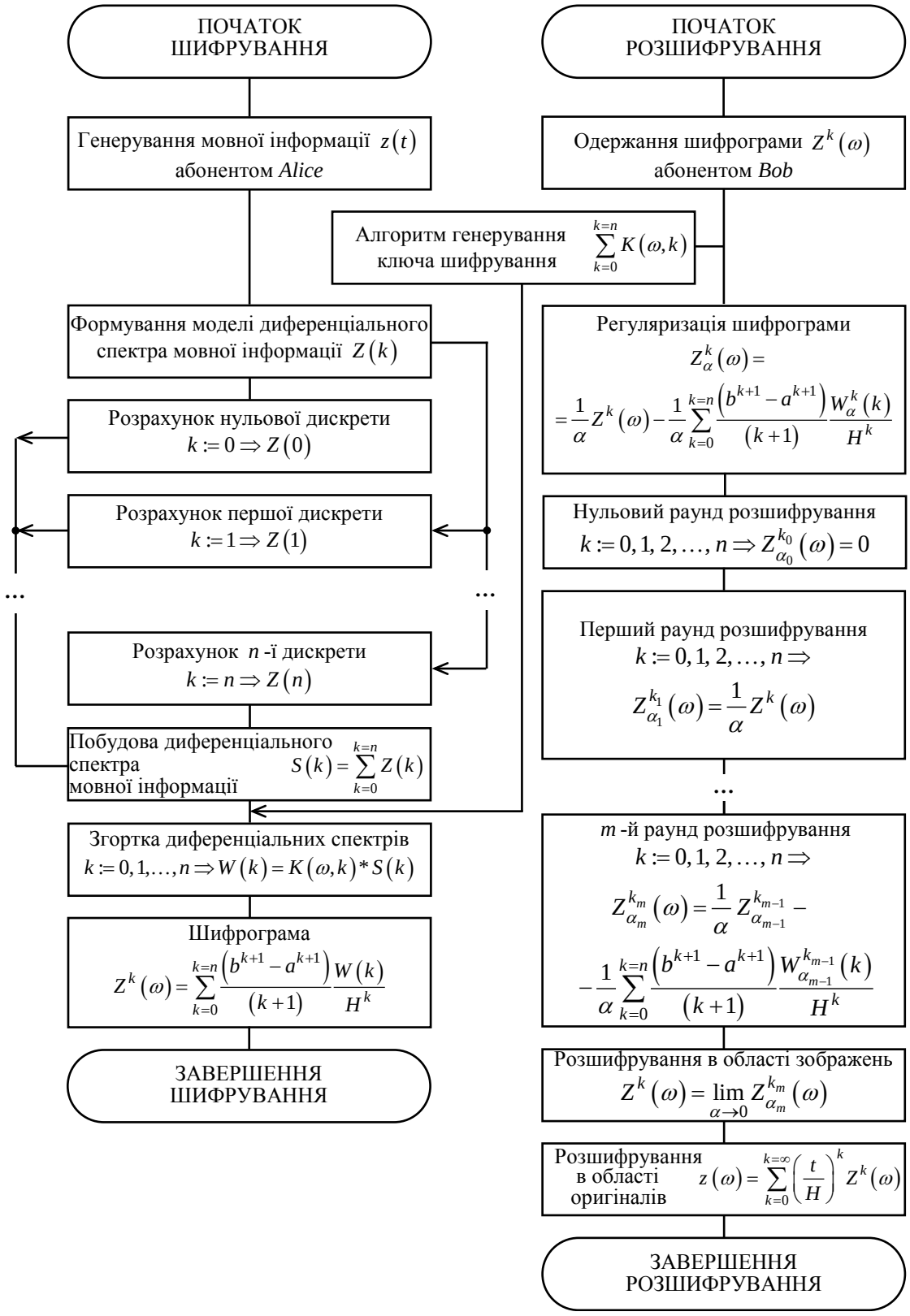

Рис. 1. Алгоритм методу шифрування мовної інформації на основі диференціальних перетворень

Крок 7. Розрахунок згортки диференціальних спектрів для k:= 0, 1,…, n:

$$W(k) = K(\omega,k) * S(k) = \sum_{l=0}^{l=k} (\omega,k-l)S(l),$$

де $K(\omega,k)$ – ключ шифрування в області зображень [23].

Крок 8. Отримання шифрограми для *k*:= 0, 1,…, *n*: $Z^k(\omega) = \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W(k)}{H^k}$.

Під час розшифрування мовної інформації алгоритм методу складається із семи кроків.

Крок 1. На приймальній стороні одержується шифрограма такого вигляду: $Z^k(\omega) = \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W(k)}{H^k}$.

Крок 2. Здійснюється регуляризація шифрограми:

$$Z_a^k(\omega) = \frac{1}{a} Z^k(\omega) - \frac{1}{a} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_a^k(k)}{H^k},$$

де *a* – параметр регуляризації, $a > 0,\ a \to 0$.

Крок 3. Проводиться нульовий раунд розшифрування для k_0 при *k*:= 0, 1, 2,…, *n*: $Z_{a_0}^{k_0}(\omega) = 0$.

Крок 4. Проводиться перший раунд розшифрування для k_1 при *k*:= 0, 1, 2,…, *n*: $Z_{a_1}^{k_1}(\omega) = \frac{1}{a} Z^k(\omega)$.

Крок 5. Проводиться *m*-й раунд розшифрування для k_m при *k*:= 0, 1, 2,…, *n*:

$$Z_{a_m}^{k_m}(\omega) = \frac{1}{a} Z_{a_{m-1}}^{k_{m-1}}(\omega) - \frac{1}{a} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_{a_{m-1}}^{k_{m-1}}(k)}{H^k}.$$

Крок 6. Здійснюється розшифрування мовної інформації в області зображень k_m при *k*:= 0, 1, 2,…, *n*:

$$Z^k(\omega) = \lim_{\alpha \to 0} Z_{\alpha_m}^{k_m}(\omega).$$

Крок 7. Розшифрування мовної інформації в області оригіналів:

$$z(\omega) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H}\right)^k Z^k(\omega) = A_c \cos(\omega_c t).$$

Перевірку достовірності розробленого методу здійснимо шляхом порівняння з відомими рішеннями, наприклад, викладеними в [34] та [35].

Шифрування мовної інформації

Крок 1. Генерування мовної інформації.

Нехай шифруванню підлягає мовна інформація, яка описується гармонічною моделлю загального вигляду $z(t)=cos(t)$, де A_c =1 В, ω_c =1 рад/с; $\varphi_c(t)=0$ рад/с; $\varphi_c=0$ рад [34] та [35].

Крок 2. Формування моделі диференціального спектра мовної інформації $Z(k)$ [25] на основі диференціальних перетворень (2):

$$Z(k)=\frac{H^k}{k!}cos\frac{\pi k}{2}. \tag{5}$$

Крок 3. Розрахунок нульової дискрети для *k*:= 0:

$$Z(0)=1. \tag{6}$$

Крок 4. Розрахунок першої дискрети для *k*:= 1:

$$Z(1)=0. \tag{7}$$

Крок 5. Розрахунок *n*-ї дискрети мовної інформації для *k*:= 2, 3,…, *n*, де *n* = 8, маємо:

$$\left[\begin{array}{ll}
для\ k:=2 & Z(2)=-\frac{1}{2}H^2;\\
для\ k:=3 & Z(3)=0;\\
для\ k:=4 & Z(4)=\frac{1}{24}H^4;\\
для\ k:=5 & Z(5)=0;\\
для\ k:=6 & Z(6)=-\frac{1}{720}H^6;\\
для\ k:=7 & Z(7)=0;\\
для\ k:=8 & Z(8)=\frac{1}{40320}H^8.
\end{array}\right. \tag{8}$$

Крок 6. Побудова диференціального спектра мовної інформації (5) з урахуванням (6)–(8):

$$S(k)=\sum_{k=0}^{k=8}Z(k)=1-\frac{1}{2}H^2+\frac{1}{24}H^4-\frac{1}{720}H^6+\frac{1}{40320}H^8. \tag{9}$$

Крок 7. Розрахунок згортки диференціальних спектрів $W(k)$ (9). При цьому диференціальний спектр ключа шифрування $K(\omega,k)$ для *k*:= 0, 1,…, *n* для обраного прикладу згідно з [35] в області оригіналів описується виразом $K(\omega,t)=cos(\omega-t)$.

Відповідно до алгоритму генерування ключа шифрування на основі диференціальних перетворень [22], [23], дискрети диференціального спектра для *k*:= 0, 1,…, *n*, де *n* = 8, дорівнюватимуть

$$\begin{cases} \text{для } k := 0 \quad K(\omega,0) = \cos(\omega); \\ \text{для } k := 1 \quad K(\omega,1) = \sin(\omega) H; \\ \text{для } k := 2 \quad K(\omega,2) = -\frac{1}{2}\cos(\omega) H^2; \\ \text{для } k := 3 \quad K(\omega,3) = -\frac{1}{6}\sin(\omega) H^3; \\ \text{для } k := 4 \quad K(\omega,4) = \frac{1}{24}\cos(\omega) H^4; \\ \text{для } k := 5 \quad K(\omega,5) = \frac{1}{120}\sin(\omega) H^5; \\ \text{для } k := 6 \quad K(\omega,6) = -\frac{1}{720}\cos(\omega) H^6; \\ \text{для } k := 7 \quad K(\omega,7) = -\frac{1}{5040}\sin(\omega) H^7; \\ \text{для } k := 8 \quad K(\omega,8) = \frac{1}{40320}\cos(\omega) H^8. \end{cases} \tag{10}$$

З урахуванням дискрет диференціального спектра ключа шифрування (10) та дискрет мовної інформації (9) згортка їхніх диференціальних спектрів $W(k)$ визначатиметься як

$$W(k) = \sum_{l=0}^{l=k} K(\omega, k-l) S(l) = K(\omega,8) S(0) + K(x,7) S(1) + \\ + K(\omega,6) S(2) + \ldots K(\omega,0) S(8) = \frac{1}{315}\cos(\omega) H^8. \tag{11}$$

Крок 8. Отримання шифрограми для *k*:= 0, 1,…, 8:

$$Z^{k_8}(\omega) = \sum_{k=0}^{k=8} \frac{\pi^{k+1}}{H^k} \frac{W(k)}{(k+1)} = \frac{\pi^9}{2835}\cos(\omega). \tag{12}$$

Розшифрування мовної інформації

Крок 1. На приймальній стороні одержано шифрограму у вигляді (19).

Крок 2. Регуляризація шифрограми:

$$Z_\alpha^k(\omega) = \frac{1}{\alpha} Z^k(\omega) - \frac{1}{\alpha} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_\alpha^k(k)}{H^k}. \tag{13}$$

Крок 3. Нульовий раунд розшифрування для k_0 при *k*:= 0, 1, 2,…, 8:

$$Z_{a_0}^{k_0}(\omega) = 0. \tag{14}$$

Крок 4. Перший раунд розшифрування для k_1 при *k*:= 0, 1, 2,…, 8:

$$Z_{a_1}^{k_1}(\omega)=\frac{1}{a}Z^{k}(\omega)=\frac{\pi^9}{2835a}cos(\omega). \tag{15}$$

Крок 5.m-й раунд розшифрування для k_m при *k*:= 0, 1, 2,…, 8:

$$Z_{\alpha_8}^{k_8}(\omega)=\frac{\pi^9}{2835\,\alpha}\cos(\omega)-\frac{1}{\alpha}\sum_{k=0}^{k=8}\frac{\pi^{k+1}}{k!}\frac{W_{\alpha_1}^{k_1}(k)}{(k+1)}=\frac{\pi^9}{2835\,\alpha}\cos(\omega)-\frac{\pi^9}{2835\,\alpha^2}\times$$
$$\times\left(\pi-\frac{1}{3!}\pi^3+\frac{1}{5!}\pi^5-\frac{1}{7!}\pi^7+\frac{1}{9!}\pi^9\right), \tag{16}$$

де $b=\pi$, $a=0$ [35].

Крок 6. Здійснюється розшифрування мовної інформації в області зображень при *k*:= 0, 1, 2,…, 8.

З урахуванням (16) розшифрована мовна інформація в області зображень із точністю до параметра регуляризації *a* визначається за таким виразом:

$$Z_{a}^{k}(\omega)=\frac{\pi^9}{2835a}cos(\omega)ъ(k), \tag{17}$$

де $\pi-\frac{1}{3!}\pi^3+\frac{1}{5!}\pi^5-\frac{1}{7!}\pi^7+\frac{1}{9!}\pi^9\approx sin(\pi)=0$;

$ъ(k)$ – теда, $ъ(k)=\begin{cases}1,\ k=0;\\ 0,\ k\geq 1.\end{cases}$

У разі обрання параметра регуляризації *a* рівним 10,46, маємо *a* = 10,46, тоді для окремого прикладу (17) в області зображень отримаємо

$$Z_{a_8}^{k_8}(\omega)\approx cos(\omega)ъ(k). \tag{18}$$

Крок 7. Розшифрування мовної інформації в області оригіналів при *k*:= 0, 1, 2,…, 8:

$$z(\omega)=\frac{H^k}{k!}\left[\frac{d^kZ_{a_8}^{k_8}(\omega)}{dt^k}\right]_{t=0}=cos(\omega). \tag{19}$$

Висновки. Розроблений у статті метод криптографічного захисту мовної інформації на основі диференціальних перетворень дає змогу в реальному масштабі часу шифрувати та розшифровувати мовну інформацію, подану моделями гармонічних сигналів. Гарантована теоретична криптостійкість визначається кількістю дискрет диференціального спектра ключа шифрування. Практична криптостійкість є величиною обернено пропорційною до параметра регуляризації. Вона забезпечується практичною

нерозв'язуваністю задачі розшифрування на основі оберненої некоректної задачі на базі інтегрального рівняння Фредгольма першого роду. Збіжність результатів шифрування й розшифрування на основі розробленого методу й інших відомих рішень підтвердили його роботоздатність. Напрямом подальших досліджень є розроблення протоколу шифрування мовної інформації на основі запропонованого методу.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Claxson N. Securing VoIP: Encrypting Today's Digital Telephony Systems // Network Security. 2018. № 11. P. 11–13.
2. Bilash D. A., Tkachov V. M. Security Mechanisms of VoIP-telephony // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : матеріали 11-ї Міжнар. наук.-техн. конф. Т. 2. Баку : ВА ЗС АР; Харків : НТУ «ХПІ», 2021. С. 78.
3. How to Know if VoIP is the Right Solution for Your Business // Weave Communications. 2020. URL: https://www.getweave.com/en-ca/how-to-know-if-voip-is-the-right-solution-for-your-business (last accessed: 21.08.2024).
4. Kumar V., Roy Om Prakash. Security and Challenges in Voice over Internet Protocols: A Survey // IOP Conf. Series: Materials Science and Engineering. 2021. 012020. https://doi.org/10.1088/1757-899x/1020/1/012020
5. Chan Y. Y., Al-Marzouqi S. M. Practical Implementations for Securing VoIP Enabled Mobile Devices // Network and System Security : Third International Conference. Australia, Gold Coast, QLD, Oct. 19–21, 2009. P. 409–415. https://doi.org/10.1109/nss.2009.24
6. Popescu E.-E. VoIP Security Threats // International Journal of Information Security and Cybercrime. 2024. Vol. 13, Iss. 1. P. 66–70. https://doi.org/10.19107/ijisc.2024.01.06
7. Sadiwala R. Analysis of Security Threats of VoIP Systems // SHODH SANGAM – A RKDF University Journal of Science and Engineering. No. 2581–5806, Vol. 01, Iss. 02. P. 34–46.
8. Kumar V., Roy Om Prakash. Reliability and Security Analysis of VoIP Communication Systems // Rising Threats in Expert Applications Solutions. Advances in Intelligent Systems and Computing. 2020. Vol. 1187. P. 687–694. https://doi.org/10.1007/978-981-15-6014-9_84
9. Arafat M. Y., Ahmed F., Sobhan M. A. SIP Security in IP Telephony // International conference. Elastix World. Mexico, October, 2013. P. 1–11.
10. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури : монографія / С. П. Євсеєв, О. Ю. Заковоротний, О. В. Мілов та ін. Харків : Вид-во «Новий Світ-2000», 2024. 300 с.
11. Alvaonos D., Limniotis K., Stavrou S. On the Cryptographic Features of a VoIP Service // Cryptography. 2018. № 2, Vol. 1. P. 1–12. https://doi.org/10.3390/cryptography2010003
12. Мажаренко В. В. Дослідження особливостей впровадження сервісів IP-телефонії в інтернет-ресурси : магістерська дис. 171 – Електроніка. Київ : КПІ ім. Ігоря Сікорського, 2020. 110 с.
13. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г. К. Бронштак, И. А. Громыко, С. И. Доценко, Е. Л. Перчик // Прикладная электроника. 2014. Т. 13, № 3. С. 337–349.
14. Грищук О. М., Жилін А. В. Новітня технологія криптографічного захисту мовної інформації // Актуальні питання застосування спеціальних інформаційно-комунікаційних

систем : тези доп. VII наук.-практ. конф. (Київ, 12 червня 2024). Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2024. С. 376.
15. Грищук О. М. Сучасні інформаційні технології криптографічного захисту інформації у секторі безпеки і оборони // Графічні технології моделювання об'єктів, процесів та явищ : тези доп. Міжнар. наук.-практ. конф. (Одеса, 23–24 квітня 2020). Одеса : Військова академія, 2020. С. 87.
16. Грищук О. М. Інновації в криптографії // Воєнні інновації в сучасних війнах : зб. тез Міжнар. академіч. форуму. Київ : ЦНДІ ЗС України, 2024. С. 192.
17. Грищук О. М. Симетрична криптосистема на диференціальних перетвореннях як новий засіб забезпечення кібербезпеки VoIP-трафіку // Всеукр. наук.-практ. інтернет-конф. ["Стратегії кіберстійкості: управління та безперервність бізнесу"] (25 лютого 2021). Київ : ДУТ, 2021. С. 51–52.
18. Грищук О. М. Математичний опис криптосистеми Фредгольма // Міжнар. наук.-практ. конф. ["Інформаційна безпека та інформаційні технології"] (24–25 квітня 2019). Харків : ХНЕУ ім. Семена Кузнеця, 2019. С. 4.
19. Грищук О. М., Грищук Р. В. Узагальнена модель криптосистеми Фредгольма // Кібербезпека: освіта, наука, техніка. 2019. № 1 (4). С. 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423
20. Hryshchuk O. Mathematical Model of a Symmetrical Cryptographic System for the Protection of Speech Information Based on Differential Transformations // Кібербезпека: освіта, наука, техніка. 2024. № 1 (25). С. 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409
21. Пухов Г. Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография. Київ : Наук. думка, 1986. 158 с.
22. Грищук О. М. Особливості вибору ключа шифрування для криптосистеми Фредгольма // Комп'ютерна інженерія і кібербезпека: досягнення та інновації : тези доп. II Всеукр. наук.-практ. конф. (25–27 листопада 2020). Кропивницький, 2020. С. 109–110.
23. Hryshchuk O. Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations / International security and practical conference ["Information security and information technologies"]. (September, 13–19, 2021). Kharkiv; Odesa, 2021. P. 229–233.
24. Корченко О. Г., Грищук О. М. Порівняльний аналіз математичних моделей мовної інформації // Безпека інформації. 2022. № 2 (28). С. 48–56. https://doi.org/10.18372/2225-5036.28.16949
25. Грищук О. М. Диференціальний спектр мовної інформації // Захист інформації. 2022. № 3 (24). С. 120–128. https://doi.org/10.18372/2410-7840.24.17189
26. Крилик Л. В., Богач І. В., Лісовенко А. І. Чисельне інтегрування функцій. Вінниця : ВНТУ, 2019. 74 с.
27. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія. Житомир : Рута, 2010. 280 с.
28. Пухов Г. Е. Дифференциальные преобразования функций и уравнений : монография. Київ : Наукова думка, 1980. 420 с.
29. Пухов Г. Е. Дифференциальные спектры и модели : монография. Київ : Наукова думка, 1990. 184 с.

30. Тихонов А. М., Арсенин В. Я. Методы решения некорректных задач. Москва, 1979. 285 с.
31. Охріменко М. Г., Жуковська О. А., Купка О. О. Методи розв'язування некоректно поставлених задач. Київ : Центр учбової літератури, 2022. 166 с.
32. Phillips D. L. A Technique for the Numerical Solution of Certain Integral Equations of the First Kind // J. Ass. Comput. 1962. P. 84–97. https://doi.org/10.1145/321105.321114
33. Ferguson N., Schroeppel R., Whiting D. A Simple Algebraic Representation of Rijndael // Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2001. P. 103–111. https://doi.org/10.1007/3-540-45537-X_8
34. Wazwaz A. M. The Regularization Method for Fredholm Integral Equations of the First Kind // Computer Methods in Applied Mechanics and Engineering. 2011. № 61. P. 2981–2986. https://doi.org/10.1016/j.camwa.2011.03.083
35. Wazwaz A. M. The Regularization-Homotopy Method for the Linear and Non-Linear Fredholm Integral Equations of the First Kind // Communications In Numerical Analysis. 2011. Vol. 2011. P. 1–11. https://doi.org/10.5899/2011/cna-00105

Стаття надійшла до редакції 05.11.2024.

REFERENCES

1. Claxson, N. (2018). Securing VoIP: Encrypting Today's Digital Telephony Systems. *Network Security, 11,* 11–13.
2. Bilash, D. A., & Tkachov, V. M. (2021). Security Mechanisms of VoIP-telephony. In *Suchasni napriamy rozvytku informatsiino-komunikatsiinykh tekhnolohii ta zasobiv upravlinnia: materialy 11-i Mizhnar. nauk.-tekhn. konf. [Modern Directions of Development of Information and Communication Technologies and Management Tools: Materials of the 11th International Scientific and Technical Conference]*. Vol. 2. (p. 78). Baku; Kharkiv [in Ukrainian].
3. How to Know if VoIP is the Right Solution for Your Business (2020). *Weave Communications.* Retrieved from https://www.getweave.com/en-ca/how-to-know-if-voip-is-the-right-solution-for-your-business
4. Kumar, V., & Roy Om Prakash. (2021). Security and Challenges in Voice over Internet Protocols: A Survey. In *IOP Conf. Series: Materials Science and Engineering*, 012020. https://doi.org/10.1088/1757-899x/1020/1/012020
5. Chan, Y. Y., & Al-Marzouqi, S. M. (2009). Practical Implementations for Securing VoIP Enabled Mobile Devices. In *Network and System Security: Third International Conference*. Australia, Gold Coast, QLD, Oct. 19–21, 2009. (pp. 409–415). https://doi.org/10.1109/nss.2009.24
6. Popescu, E.-E. (2024). VoIP Security Threats. *International Journal of Information Security and Cybercrime, 13,* Iss. 1, 66–70. https://doi.org/10.19107/ijisc.2024.01.06
7. Sadiwala, R. (n. d.). Analysis of Security Threats of VoIP Systems. *SHODH SANGAM – A RKDF University Journal of Science and Engineering. No. 2581–5806,* Vol. 01, Iss. 02, 34–46.
8. Kumar, V., & Roy Om Prakash. (2020). Reliability and Security Analysis of VoIP Communication Systems. *Rising Threats in Expert Applications Solutions. Advances in Intelligent Systems and Computing, 1187,* 687–694. https://doi.org/10.1007/978-981-15-6014-9_84
9. Arafat, M. Y., Ahmed, F., & Sobhan, M. A. (2013). SIP Security in IP Telephony. In

International conference. Elastix World. Mexico, October, 2013. (pp. 1–11).
10. Yevseiev, S. P., Zakovorotnyi, O. Yu., & Milov, O. V. et al. (2024). *Metodolohiia syntezu modelei intelektualnykh system upravlinnia ta bezpeky ob'iektiv krytychnoi infrastruktury : monohrafiia [Methodology for the Synthesis of Models of Intelligent Control and Security Systems for Critical Infrastructure Facilities: Monograph]*. Kharkiv [in Ukrainian].
11. Alvaonos, D., Limniotis, K., & Stavrou, S. (2018). On the Cryptographic Features of a VoIP Service. *Cryptography, № 2*, Vol. 1, 1–12. https://doi.org/10.3390/cryptography2010003
12. Mazharenko, V. V. (2020). *Doslidzhennia osoblyvostei vprovadzhennia servisiv IP-telefonii v internet-resursy : mahisterska dys. 171 – Elektronika [Research on the Features of Implementing IP Telephony Services in Internet Resources: Master's thesis. 171 – Electronics]*. Kyiv [in Ukrainian].
13. Bronshpak, G. K., Gromyko, I. A., Dotsenko, S. I., & Perchik, E. L. (2014). Kriptografiia novogo pokoleniia: Integral'nye uravneniia kak al'ternativa algebraicheskoi metodologii [New Generation Cryptography: Integral Equations as an Alternative to Algebraic Methodology]. *Prikladnaia elektronika [Applied Electronics], Vol. 13,* № 3, 337–349 [in Russian].
14. Hryshchuk, O. M., & Zhylin, A. V. (2024). Novitnia tekhnolohiia kryptohrafichnoho zakhystu movnoi informatsii [The Latest Technology of Cryptographic Protection of Speech Information]. In *Aktualni pytannia zastosuvannia spetsialnykh informatsiino-komunikatsiinykh system : tezy dop. VII nauk.-prakt. konf. [Current Issues of the Application of Special Information and Communication Systems: Theses of the VII Scientific-Practical Conference]*. Kyiv, June 12, 2024. (p. 376). Kyiv [in Ukrainian].
15. Hryshchuk, O. M. (2020). Suchasni informatsiini tekhnolohii kryptohrafichnoho zakhystu informatsii u sektori bezpeky i oborony [Modern Information Technologies of Cryptographic Protection of Information in the Security and Defense Sector]. In *Hrafichni tekhnolohii modeliuvannia ob'iektiv, protsesiv ta yavyshch : tezy dop. Mizhnar. nauk.-prakt. konf. [Graphical Technologies for Modeling Objects, Processes and Phenomena: Theses of the International Scientific-Practical Conference]*. Odesa, April 23–24, 2020. (p. 87). Odesa: Military Academy [in Ukrainian].
16. Hryshchuk, O. M. (2024). Innovatsii v kryptohrafii [Innovations in Cryptography]. In *Voienni innovatsii v suchasnykh viinakh: zb. tez Mizhnar. akademich. forumu. [Military Innovations in Modern Wars: Collection of Theses of the International Academic Forum]*. (p. 192). Kyiv [in Ukrainian].
17. Hryshchuk, O. M. (2021). Symetrychna kryptosystema na dyferentsialnykh peretvorenniakh yak novyi zasib zabezpechennia kiberbezpeky VoIP-trafiku [Symmetric Cryptosystem on Differential Transformations as a New Means of Ensuring Cybersecurity of VoIP Traffic]. In *Vseukr. nauk.-prakt. internet-konf. ("Stratehii kiberstiikosti: upravlinnia ta bezperervnist biznesu") [All-Ukrainian Scientific and Practical Internet Conference ("Cyber Resilience Strategies: Management and Business Continuity")]*. Kyiv, February 25, 2021. (pp. 51–52). Kyiv: SUT [in Ukrainian].
18. Hryshchuk, O. M. (2019). Matematychnyi opys kryptosystemy Fredholma [Mathematical Description of the Fredholm Cryptosystem]. In *Mizhnar. nauk.-prakt. konf. ("Informatsiina bezpeka ta informatsiini tekhnolohii") [International scientific and practical conference ("Information Security and Information Technologies")]*. Kharkiv, April 24–25, 2019. (p. 4). Kharkiv: KhNEU [in Ukrainian].

19. Hryshchuk, O. M., & Hryshchuk, R. V. (2019). Uzahalnena model kryptosystemy Fredholma [Generalized Model of Fredholm Cryptosystem]. *Kiberbezpeka: osvita, nauka, tekhnika [Cybersecurity: Education, Science, Technology]*, *1* (4), 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423 [in Ukrainian].
20. Hryshchuk, O. (2024). Mathematical Model of a Symmetrical Cryptographic System for the Protection of Speech Information Based on Differential Transformations. *Kiberbezpeka: osvita, nauka, tekhnika [Cybersecurity: Education, Science, Technology]*, *1* (25), 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409
21. Pukhov, G. E. (1986). *Differentsial'nye preobrazovaniia i matematicheskoe modelirovanie fizicheskikh protsessov : monografiia [Differential Transformations and Mathematical Modeling of Physical Processes: Monograph]*. Kyiv [in Russian].
22. Hryshchuk, O. M. (2020). Osoblyvosti vyboru kliucha shyfruvannia dlia kryptosystemy Fredholma [Features of Choosing an Encryption Key for the Fredholm Cryptosystem]. In *Komp'iuterna inzheneriia i kiberbezpeka: dosiahnennia ta innovatsii : tezy dop. II Vseukr. nauk.-prakt. konf. [Computer Engineering and Cybersecurity: Achievements and Innovations: Theses of the II All-Ukrainian Scientific and Practical Conference]*. Kropyvnytskyi, November 25–27, 2020. (pp. 109–110). Kropyvnytskyi [in Ukrainian].
23. Hryshchuk, O. (2021). Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations. In *International security and practical conference ("Information security and information technologies").* Kharkiv, Odesa, September 13–19, 2021. (pp. 229–233).
24. Korchenko, O. H., & Hryshchuk, O. M. (2022). Porivnialnyi analiz matematychnykh modelei movnoi informatsii [Comparative Analysis of Mathematical Models of Speech Information]. *Bezpeka informatsii [Information Security]*, *2* (28), 48–56. https://doi.org/10.18372/2225-5036.28.16949 [in Ukrainian].
25. Hryshchuk, O. M. (2022). Dyferentsialnyi spektr movnoi informatsii [Differential Spectrum of Speech Information]. *Zakhyst informatsii [Information Security]*, *3* (24), 120–128. https://doi.org/10.18372/2410-7840.24.17189 [in Ukrainian].
26. Krylyk, L. V., Bohach, I. V., & Lisovenko, A. I. (2019). *Chyselne intehruvannia funktsii [Numerical Integration of Functions]*. Vinnytsia [in Ukrainian].
27. Hryshchuk, R. V. (2010). *Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren : monohrafiia [Theoretical Foundations of Modeling Information Attack Processes Using Methods of Differential Game Theories and Differential Transformations: Monograph]*. Zhytomyr [in Ukrainian].
28. Pukhov, G. E. (1980). *Differentsial'nye preobrazovaniia funktsii i uravnenii : monografiia [Differential Transformations of Functions and Equations: Monograph]*. Kyiv [in Russian].
29. Pukhov, G. E. (1990). *Differentsial'nye spektry i modeli : monografiia [Differential Spectra and Models: Monograph]*. Kyiv [in Russian].
30. Tikhonov, A. M., & Arsenin, V. Ia. (1979). *Metody resheniia nekorrektnykh zadach [Methods for Solving Ill-posed Problems]*. Moscow [in Russian].
31. Okhrimenko, M. H., Zhukovska, O. A., & Kupka, O. O. (2022). *Metody rozv'iazuvannia nekorektno postavlenykh zadach [Methods of Solving Incorrectly Posed Problems]*. Kyiv [in Ukrainian].

32. Phillips, D. L. (1962). A Technique for the Numerical Solution of Certain Integral Equations of the First Kind. *J. Ass. Comput*., 84–97. https://doi.org/10.1145/321105.321114
33. Ferguson, N., Schroeppel, R., Whiting, D. (2001). A Simple Algebraic Representation of Rijndael. *Selected Areas in Cryptography,* 103–111. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45537-X_8
34. Wazwaz, A. M. (2011). The Regularization Method for Fredholm Integral Equations of the First Kind. *Computer Methods in Applied Mechanics and Engineering, 61,* 2981–2986. https://doi.org/10.1016/j.camwa.2011.03.083
35. Wazwaz, A. M. (2011). The Regularization-Homotopy Method for the Linear and Non-Linear Fredholm Integral Equations of the First Kind. *Communications In Numerical Analysis, Vol. 2011,* 1–11. https://doi.org/10.5899/2011/cna-00105

O. G. Korchenko, O. M. Hryshchuk

SPEECH INFORMATION CRYPTOGRAPHIC PROTECTION METHOD BASED ON DIFFERENTIAL TRANSFORMATIONS

The problem of information security that circulates in communication channels is constantly being updated. It is especially acute for military VoIP telephony or dual use. This relates to the growth of the value of confidential information, which is of interest to cybercriminals, and with the increase in the technological complexity of cyberattacks at the same time as the productivity of technical means of obtaining unauthorized information increases. Cryptographic methods of information protection occupy one of the key places among the well-known mechanisms for ensuring the cyber security of speech information circulating in communication channels. SRTP security protocols, which implement the symmetric cryptographic encryption algorithm AES, are most often used to organize secure VoIP traffic. At the same time, the potential compromise of the best symmetric cryptographic algorithm AES-256 requires the search for new non-trivial approaches to improving cyber security mechanisms. One of these approaches developed in the article is an approach based on the use of the Fredholm cryptosystem model. The mentioned cryptographic system belongs to the class of symmetric cryptographic systems, but to date, due to the lack of scientifically based cryptographic algorithms, it has not yet gained practical implementation. To resolve this contradiction, the article, based on the principle of O. Kerckhoffs, developed a method of cryptographic protection of speech information based on differential transformations developed by Academician of the National Academy of Sciences of Ukraine H. Pukhov. The developed method makes it possible to obtain a cipher in the form of a differential spectrum, which is resistant to known methods of cryptanalysis. The article developed an algorithm for implementing the method. The results of encryption and decryption of speech information are given. The convergence of simulation results with other known methods confirms the workability of the developed method.

Keywords: *symmetric cryptographic algorithm; differential transformations; encryption key; differential spectrum; cipher; discrete; guaranteed cryptographic strength; inverse problem; Fredholm integral equation of the first kind.*