ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

КРИПТОЛОГІЯ/ CRYPTOLOGY

DOI: 10.18372/2225-5036.30.19242

ФОРМАЛІЗОВАНА ПОСТАНОВКА НАУКОВОГО ЗАВДАННЯ З РОЗРОБЛЕННЯ СИМЕТРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Ольга Грищук

Національний університет оборони України

ГРИЩУК Ольга Михайлівна
Рік та місце народження: 1984 рік, м. Житомир, Україна.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: старший науковий співробітник науково-дослідної лабораторії управління інформаційною безпекою науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій Інституту стратегічних комунікацій Національного університету оборони України з 2024 р.
Наукові інтереси: кібербезпека, інформаційна безпека.
Публікації: 8 наукових статей, тези 11 доповідей.
E-mail: hry.olha@gmail.com.
Orcid ID: 0000-0001-6957-4748.

Анотація. *За останні роки кількість викликів та загроз сучасним інформаційним технологіям постійно зростає. Безпекова ситуація ускладнюється тим, що в умовах збройного конфлікту кіберзагрози набувають ознак гібридності. Гібридність кіберзагроз проявляється у впливі однієї загрози на одну послугу безпеки в усіх безпекових складових одночасно. Наприклад, якщо в інформаційній технології циркулює мовна інформація, то вплив на таку властивість як конфіденційність одночасно відбувається для таких безпекових складових як інформаційна безпека, безпека інформації та кібербезпека. Тому в нинішніх умовах дуже важливо удосконалювати існуючі або розробляти нові механізми забезпечення безпеки мовної інформації. Існуючі підходи до захисту мовної інформації ґрунтуються в основному на використанні криптографічних алгоритмів, які реалізовано в симетричних або асиметричних криптографічних системах. Зважаючи на відносно більшу швидкодію симетричних криптографічних систем, порівняно з асиметричними, вони й надалі залишаються в пріоритеті під час захисту мовної інформації. Разом з тим, вони також підвладні сучасним методам криптоаналізу. Саме тому дуже важливо розробити нетиповий та нетривіальний криптоалгоритм, який реалізуватиме відповідну симетричну криптографічну систему захисту мовної інформації. Виходячи з зазначеного у статті наведено формалізовану постановку наукового завдання з розроблення симетричної криптографічної системи захисту мовної інформації. Її особливостями мають стати: по-перше, використання в якості криптографічного алгоритму інтегрального рівняння Фредгольма першого роду; по-друге, використання в якості ключа шифрування його ядра; по-третє, в якості інформації, що підлягає шифруванню має бути мовна інформація у вигляді аналогового сигналу; по-четверте, використання в процесі шифрування та розшифрування мовної інформації диференціальних перетворень академіка НАН України Г. Пухова; по-п'яте, використанні методу регуляризації А. Тихонова для розшифрування шифротексту з вихідної мовної інформації у вигляді диференціального спектру. Висунуто вимоги до розроблюваної симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень. Такі вимоги стосуються гарантованої теоретичної та практичної криптостійкості. Для їх виконання визначено сутність і зміст наукового завдання, що вирішується у статті. Наведено його формалізовану постановку.*

Ключові слова: *мовна інформація, симетрична криптографічна система, наукове завдання, диференціальні перетворення, регуляризація, ключ шифрування, інтегральне рівняння Фредгольма першого роду.*

Постановка проблеми

Високотехнологічний характер збройної боротьби призвів до стрімкого розвитку інформаційно-комунікаційних систем різного цільового призначення. Наприклад, в Збройних Силах України такими системами є автоматизовані системи (АСУ) АСУ "Дельта", АСУ "ОРЕАНДА-ПС", АСУ "Дзвін-АС", АСУ "Гермес-С2" [1] та ін. В збройних силах російської федерації – АСУ "Акация", "Созвездие-М2", "Андромеда-Д", "Кассиопея-Д", білорусі – АСУ "Альянс" [1] тощо. Вбачається, що у найближчому майбутньому кількість багатоцільових інформаційно-комунікаційних систем тільки збільшуватиметься. Для захисту мовної інформації в інформаційно-комунікаційних систе-

мах [2] останнім часом дуже часто застосовуються спеціальні шифратори в які вже інтегровані відповідні модулі перетворення інформації, наприклад шифратор СКАТ-Е від української компанії ТРИТЕЛ [3].

У [3] показано, що шифрування мовної інформації в модулі СКАТ-Е реалізується на основі криптографічного алгоритму ДСТУ ГОСТ 28147:2009. Не зважаючи на легку апаратну реалізацію даного криптографічного алгоритму [4] існуючі недоліки, зокрема такий як відносно низька швидкодія на сучасних системах [5], ставлять під загрозу отримання зловмисником несанкціонованого доступу до мовної інформації.

Враховуючи, що в світі активізувалося розроблення квантових комп'ютерів, то не виключається, що ключі шифрування застосовуваного в Україні криптоалгоритму ДСТУ ГОСТ 28147:2009 також будуть зламані. Зокрема, французькими і американськими вченими в 2020 р. зламний ключ асиметричного шифрування RSA-240 довжиною 795 біт. Не виключається, що буде зламано ключ симетричного шифрування AES (ас)-256. Тому з причини суттєвого збільшення кількості кіберінцидентів [6], пов'язаних з компрометацією засобів VoIP-телефонії [7, 8], бізнес і Збройні Сили України все частіше потребують використання засобів безпечного шифрування [9].

Таким чином, як показано вище, проблема забезпечення безпеки мовної інформації й надалі залишається актуальною. Її розв'язання потребує вирішення ряду частинних наукових завдань, одним з яких є розроблення симетричної криптографічної системи на основі диференціальних перетворень.

Аналіз останніх досліджень та публікацій

Аналіз останніх досліджень і публікацій [10-19] показав, що починаючи з 1976 р. після появи відомої роботи New Directions in Cryptography американських криптографів У. Діффі та М. Геллмана [20], в світі у цілому та в Україні зокрема інтенсифікувався процес винайдення нових підходів до криптографічного захисту мовної інформації. Найбільш інтенсивно сьогодні розвиваються когнітивна криптографія [11], криптографія на основі хаосу [12–14], конструктивна криптографія [15], квантова криптографія [16–19], постквантова криптографія [10] тощо.

Підсумовуючи переваги та недоліки перспективних підходів до криптографічного захисту мовної інформації слід відмітити, що більшість з них вкладається в класичну парадигму асиметричних або симетричних криптографічних систем. Як слідство забезпечення криптостійкості алгоритмів захисту мовної інформації ґрунтується на складності вирішення задач факторизації, дискретного логарифмування тощо (для асиметричних криптосистем) або комбінаторної складності (для симетричних криптосистем). Як показали результати аналізу перспективності застосування нового підходу в криптографії, так званої інтегральної криптографії [21], існуюча математична складність вирішення задачі криптоаналізу може бути покладена в основу забезпечення криптостійкості перспективних алгоритмів шифрування для захисту мовної інформації. Зокрема це стосується й симетричних криптографічних систем захисту мовної інформації нового покоління.

Мета та постановка завдання

Метою дослідження **є** постановка у формалізованому вигляді задачі з розроблення та дослідження симетричної криптографічної системи захисту мовної інформації.

Виклад основного матеріалу дослідження

На сьогодні відомо два основні підходи до постановки наукових завдань. Перший – це вербальний підхід, який більш властивий дослідженням гуманітарного спрямування [21]. Другий – це формалізований підхід до постановки наукових завдань. Він більш властивий точним наукам [22-26]. Його базовою перевагою є можливість чіткої й коректної у математичному сесі постановки наукового завдання, яке може бути вирішене математичними методами й перевірене на збіжність з відомими результатами.

Одним із таких наукових завдань яке підлягає розв'язанню в рамках поставленої в статті мети є завдання з розроблення та дослідження симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень, яка повинна мати гарантовану теоретичну та практичну криптостійкість, що повинна забезпечуватися практичною нерозв'язаністю оберненої некоректної задачі, покладеної в основу створеного криптоалгоритму [2, 27].

У широкому сенсі графічне подання розв'язуваного наукового завдання розкрито у вигляді схеми (рис. 1). Виходячи з аналізу сутності та змісту поставленого наукового завдання (див. рис. 1) воно може бути подано у наступному формалізованому вигляді.

Нехай захисту підлягатиме мовна 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:

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

Припущення. Ключ шифрування K зберігається в секреті обома учасниками обміну мовною інформацією.

В якості моделі мовної інформації I можуть використовуватися гармонічні математичні моделі, які описуються функціональними залежностями, у яких параметри мовної інформації змінюються в часі. Під гарантованою теоретичною та практичною криптостійкістю в статті розуміється стійкість шифру до криптоаналізу, яка забезпечується за рахунок застосування для шифрування мовної інформації криптоалгоритмів на основі інтегральних рівнянь Фредгольма першого роду [27]:

$$u(x) = \int_0^x K(x, s)\, z(s)\, ds, \qquad (2)$$

де $u(x)$ – шифрограма; $z(s)$ – мовна інформація, яка підлягає шифруванню; $K(x, s)$ – секретний ключ шифрування (розшифрування); $z(x)$ – розшифрована мовна інформація.

Рис. 1. Сутність і зміст наукового завдання

З урахуванням зазначеного основною перевагою подання алгоритмів шифрування мовної інформації інтегральними рівняннями Фредгольма першого роду є гарантована теоретична та практична криптостійкість шифрограм до відомих типів криптографічних атак. Другою вагомою перевагою є їх висока адекватність, оскільки рівняння (2) містить усі необхідні й достатні параметри мовної інформації як вокалізованих, так і невокалізованих складових мовного сигналу.

Обмеження. При розробленні криптографічної системи захисту мовної інформації повинен використовуватися один ключ K, тобто криптографічна система повинна бути віднесена до класу симетричних криптографічних систем. Гарантована теоретична та практична криптостійкість обмежена класом обернених некоректних задач. Для розшифрування зашифрованої мовної інформації I повинні використовуватися методи регуляризації некоректних задач.

За прийнятих припущень та обмежень виходячи з (1) та (2) математична постановка наукового завдання може бути подана системою вигляду:

$$\begin{cases} S \Rightarrow u(x); \\ E \Rightarrow \int\limits_0^x K(x,s)\, z(s)\, ds; \\ K \Rightarrow K(x,s); \\ I \Rightarrow z(x), \end{cases} \qquad (3)$$

де $u(x)$ – шифрограма; $z(s)$ – мовна інформація I, яка підлягає шифруванню; $K(x,s)$ – секретний ключ K, який використовується сторонами інформаційного обміну для шифрування та розшифрування відповідно; $z(x)$ – розшифрована мовна інформація I.

Переслідуючи поставлену в статті мету щодо розроблення та дослідження симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень, яка має гарантовану теоретичну та практичну криптостійкість, що повинна забезпечуватися практичною нерозв'язаністю оберненої некоректної задачі покладеної в основу створеного криптоалгоритму, передбачається розв'язання ряду частинних задач, а саме:

- проведення аналізу відомих підходів до забезпечення криптографічного захисту мовної інформації та обґрунтувати за його результатами вибору напряму дослідження;

-подальший розвиток математичної моделі симетричної криптографічної системи захисту мовної інформації;

- розроблення алгоритму генерації та вибору ключа шифрування (розшифрування) мовної інформації на основі диференціальних перетворень;

- розроблення методу шифрування (розшифрування) мовної інформації на основі диференціальних перетворень;

- верифікація симетричної криптографічної системи на основі диференціальних перетворень та розроблення практичних рекомендацій із захисту мовної інформації на основі диференціальних перетворень.

Структурно-логічну схему вирішення поставлених задач з визначеним ступенем функціональної декомпозиції можна подати у вигляді рис. 2.

На рисунку (рис. 2) показано, що при послідовному вирішенні чотирьох взаємопов'язаних частинних наукових задач розробленню підлягають три наукові положення, ступінь наукової новизни яких має бути визначений за одержаними результатами.

Висновки. У статті формалізовано наукове завдання, яке полягає у розробленні та дослідженні симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень,

яка повинна мати гарантовану теоретичну та практичну криптостійкість, що забезпечується практичною нерозв'язаністю оберненої некоректної задачі, покладеної в основу створеного криптоалгоритму.

Його вирішення є підґрунтям для практичної реалізації в подальшому розробленої симетричної криптографічної системи.

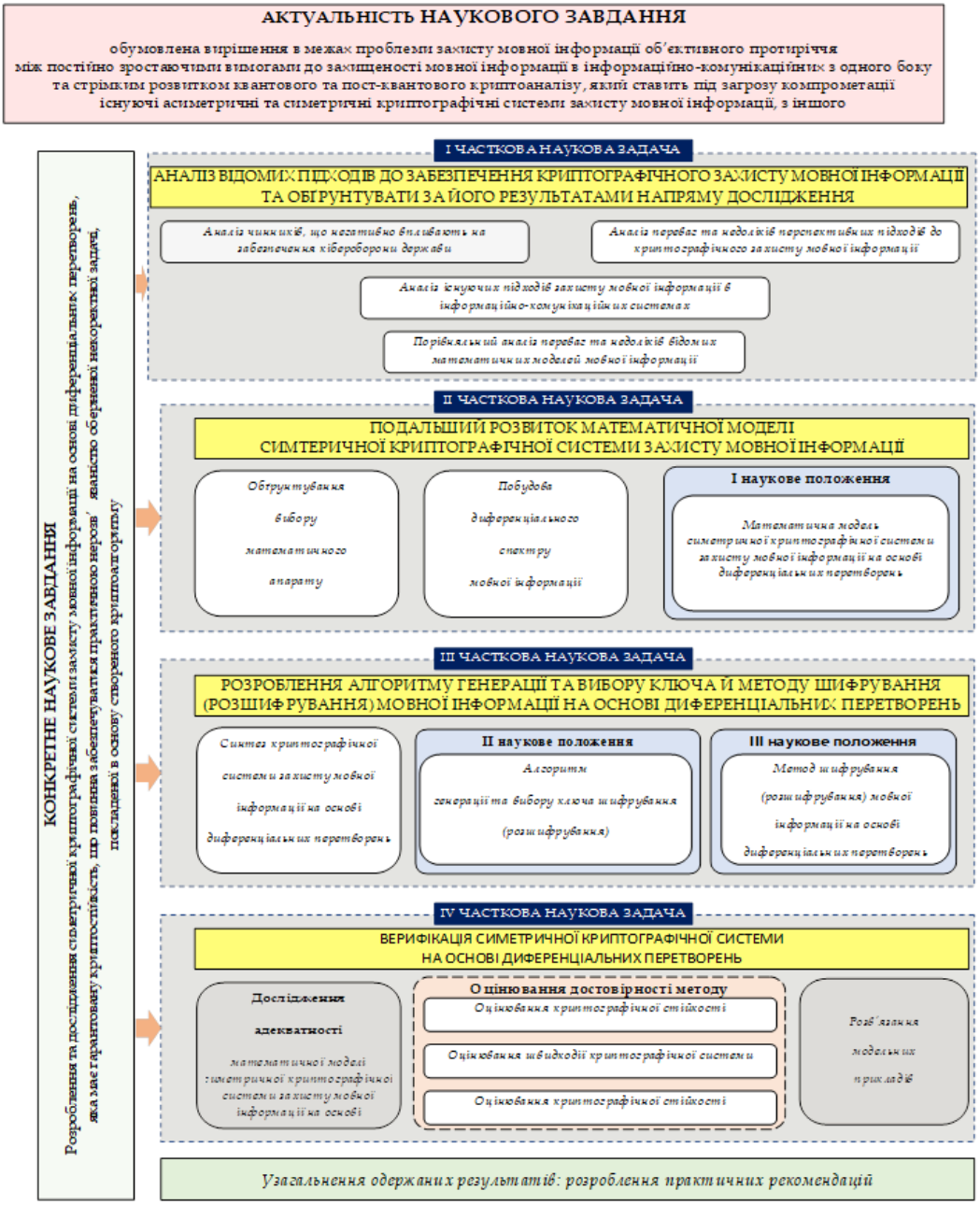

Рис. 2. Структурно-логічна схема вирішення наукового завдання

Список літератури

[1]. Кобзар О. В. Топологія побудови операційної системи реального часу автоматизованої системи управління Військово-Морськими Силами Збройних Сил України / О. В. Кобзар, М. В. Мусієнко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. № 20. 2022. С. 28-41.

[2]. Hryshchuk O. Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations / O. Hryshchuk // III International Scientific And Practical Conference ["Information Security And Information Technologies"], (Odesa, 13-19 Sept. 2021 y.). – CEUR Workshop Proceedings, 2021. pp. 1–5.

[3]. СКАТ-Е: шифратор з інтегрованим модулем перетворення мовної інформації [Електронний ресурс] // Трител. 2016. Режим доступу до ресурсу: https://cutt.ly/CUKepeA.

[4]. Олійников Р. В. Методи аналізу і синтезу перспективних симетричних криптографічних перетворень. Дис. д-ра техн. наук: 05.13.05, Харк. нац. ун-т радіоелектрон. Х., 2014. 420 с.

[5]. Єфіменко А. А. Порівняльний аналіз алгоритму симетричного блокового перетворення "Калина" (ДСТУ 7624:2014) з іншими міжнародними стандар-

тами шифрування даних / А. А. Єфіменко, Є. М. Байлюк, О. А. Покотило // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2018. Вип. 15. С. 156-162.

[6]. Грищук Р. В. Основи кібернетичної безпеки: монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

[7]. Mentsiev A. VoIP security threats / A. Mentsiev, A. Dzhangarov // Инженерный вестник Дона. 2019. № 1. С. 1-7.

[8]. Roy O. P. A Survey on Voice over Internet Protocol (VoIP) Reliability Research / O. P. Roy, V. Kumar // IOP Conf. Series: Materials Science and Engineering. 2020. № 1020. С. 1-9.

[9]. Claxson N. Securing VoIP: encrypting today's digital telephony systems / N. Claxson // Network Security. 2018. № 11. С. 11-13.

[10]. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнєцов, О. В. Потій та ін.// Радиотехника. 2016. Вип. 186. С. 32-52.

[11]. Ogiela M. R. On Using Cognitive Models in Cryptography / M. R. Ogiela, L. Ogiela // IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). Crans-Montana, 2016. pp. 1055-1058.

[12]. Kocarev L. Chaos-based Cryptography Theory, Algorithms and Applications / L. Kocarev, S. Lian. Springer Science & Business Media, 2011. 390 p.

[13]. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р. Л. Політанський ; Міністерство освіти і науки України, Національний університет "Львівська політехніка". Львів ; Дрогобич: Коло, 2015. 184 с.

[14]. Pekerti A. Secure End-to-End Voice Communication: A Comprehensive Review of Steganography, Modem-Based Cryptography, and Chaotic Cryptography Techniques / A. Pekerti, A. Sasongko, A. Indrayanto // IEEE Access. 2024. Vol. 12 pp. 75146-75168.

[15]. Maurer U. Constructive Cryptography – A New Paradigm for Security Definitions and Proofs / U. Maurer // Springer-Verlag Berlin Heidelberg. 2012. pp. 33-56.

[16]. Quantum Cryptography [Електронний ресурс] / R. J. Hughes, D. M. Alde, P. Dyer та ін. // Los Alamos National Laboratory. 1994. Режим доступу до ресурсу: https://arxiv.org/pdf/quant-ph/9504002.pdf].

[17]. Думачев В. Н. Модели и алгоритмы квантовой информации : монография / В. Н. Думачев. – Воронеж : ВИМВД, 2009. 231 с.

[18]. Калюжний І. Г. Квантова криптографія: принципи, проблеми та перспективи / І. Г. Калюжний // Інформаційні системи, механіка та керування. 2015. Вип. 13. С. 29-37. Режим доступу: http://nbuv.gov.ua/UJRN/Ismk_2015_13_5.

[19]. Richard J. Quantum Cryptography / J. Richard, D. Hughes, M. Alde and etc. [Електронний ресурс] // University of California, LA National Laboratory. 1995. Режим доступу до ресурсу: https:// arxiv. org/pdf/quant-ph/9504002/.

[20]. Diffie W. New Directions in Cryptography / W. Diffie, M. E. Hellman. // IEEE Transactions on Information Theory. 1976. pp. 644-654.

[21]. Броншпак Г. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г. Броншпак, И. Громыко, С. Доценко и др. // Прикладная электроника. № 3. 2014. С. 337-349.

[22]. Ходаківський Є. І. Методологія наукових досліджень в парадигмі синергетики: монографія / Є.І. Ходаківський, В.К. Данилко, Ю.С. Цал-Цалко. За заг. ред. д-ра екон. наук Є.І. Ходаківського. Житомир: Житомирський державний технологічний університет, 2009. 340 с.

[23]. Грищук Р. В. Постановка задачі розробки методики скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р. В. Грищук, В. М. Мамарєв // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля, 2011. – № 1 (5). С. 74-78.

[24]. Грищук Р. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак / Р. В. Грищук, В. В. Охрімчук // Безпека інформації 2015. Том 21. № 3. С. 276-282.

[25]. Грищук Р. В. Формалізована постановка наукового завдання для підвищення ефективності виявлення загроз за даними з мережі Інтернет / Р. В. Грищук, О. В. Лагодний // Сучасна спеціальна техніка. 2018. № 1 (52). С. 23-48.

[26]. Hryshchuk R. The Synergetic Approach for Providing Bank Information Security: The Problem Formulation / Ruslan Hryshchuk, Sergii Yevseiev // Безпека інформації. 2016. Том 22. № 1 С. 64-74.

[27]. Грищук Р. Узагальнена модель криптосистеми Фредгольма / Р. Грищук, О. Грищук // Кібербезпека: освіта, наука, техніка. № 4 (4). 2019. С. 14-23.

УДК 004.056

Hryshchuk O. Formalized scientific problem statement for the development of a symmetric cryptographic system for protecting voice information

Abstract. *In recent years, the number of challenges and threats to modern information technologies has been steadily increasing. The security situation is further complicated by the fact that, in the context of armed conflict, cyber threats acquire a hybrid nature. The hybridity of cyber threats manifests in the impact of one threat on a single security service across all security components simultaneously. For instance, when voice information circulates within an information technology system, the impact on a property such as confidentiality simultaneously affects various security components, including information security, data security, and cybersecurity. Therefore, in the current conditions, it is crucial to enhance existing mechanisms or develop new ones to ensure the security of voice information. Existing approaches to protecting voice information are primarily based on the use of cryptographic algorithms implemented in symmetric or asymmetric cryptographic systems. Given the relatively higher speed of symmetric cryptographic systems compared to asymmetric ones, they continue to be preferred for protecting voice information. However, they are also susceptible to modern cryptanalytic methods. Therefore, it is crucial to find an unconventional and non-trivial cryptographic algorithm that will implement an effective symmetric cryptographic system for protecting voice information. Based on the above, the article presents the formalized scientific problem statement for the development of a*

symmetric cryptographic system for protecting voice information. Its features are expected to be: first, the use of the Fredholm integral equation of the first kind as the cryptographic algorithm; second, the use of its kernel as the encryption key; third, the information to be encrypted should be voice information in the form of an analogue signal; fourth, the use of differential transformations by Academician H. Pukhov of the National Academy of Sciences of Ukraine in the encryption and decryption process; fifth, the application of A. Tikhonov's regularization method for decrypting ciphertext from the original voice information in the form of a differential spectrum.Requirements for the development of a symmetric cryptographic system for protecting voice information based on differential transformations are proposed. These requirements relate to guaranteed theoretical and practical cryptographic strength. To meet these requirements, the essence and content of the scientific task being solved in the article have been defined. Its formalized statement is presented.

Keywords: *voice information, symmetric cryptographic system, scientific problem, differential transformations, regularization, encryption key, Fredholm integral equation of the first kind.*

Грищук Ольга Михайлівна, аспірантка, старший науковий співробітник науково-дослідної лабораторії управління інформаційною безпекою науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій Інституту стратегічних комунікацій Національного університету оборони України.

Olha Hryshchuk, postgraduate student, senior researcher of the National Defence University of Ukraine.

Отримано *8 червня 2024 року,* затверджено редколегією *26 червня 2024 року*