Volodymyr NAKONECHNYI, DSc (Engin.), Prof.
ORCID ID: 0000-0002-0247-5400
e-mail: volodym.nakonechnyi@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Volodymyr SAIKO, DSc (Engin.), Prof.
ORCID ID: 0000-0002-3059-6787
e-mail: v.saiko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola MORDVYNTSEV, DSc (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7674-3164
e-mail: lukolyy@gmail.com
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine

Vladyslav LUTSENKO, PhD Student
ORCID ID: 0000-0002-2377-1858
e-mail: vlkiller175@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ADVANTAGES AND RISKS OF USING CHATGPT

B a c k g r o u n d . *This article presents ChatGPT - a new chatbot, one of the latest products in the field of artificial intelligence, created by OpenAI, which developed this technology together with Elon Musk. The article provides recommendations for connecting to a chatbot. The main advantages of artificial intelligence are defined, and examples of its application are given.*

Current educational processes should develop a cross-disciplinary and practice-oriented approach in the student.

R e s u l t s . *It is shown that among the main advantages of ChatGPT is the ability to generate texts on a given topic, to answer almost all user questions, and to express oneself even in Ukrainian. Specific examples of chatbot questions related, in particular, to information protection, risk management, etc., are given. Demonstrated responses from his side. Focused on the dangers of using a new chatbot. It is shown that possible plagiarism, compatibility issues, malicious use, privacy issues, copyright infringement issues, and problems of using ChatGPT in the educational system occupy a special place among the identified dangers. It is emphasized that the education system is currently experiencing a significant crisis and that the process of obtaining knowledge is adequate to the challenges of today, it is necessary to radically revise the approach to what the current teacher and the educational process itself should be. It is noted that Ukraine needs a fundamental transformation of the very essence of the education system. Now the main task of the teacher is to give the student himself the opportunity to take the initiative in learning, to effectively use the information received, to combine it and to apply the received result in solving his task. A successful student must learn to solve complex tasks that are at the junction of various subjects and disciplines.*

C o n c l u s i o n s . *So, ChatGPT is a powerful tool, but today it has some drawbacks that should be considered if you plan to use it.*

K e y w o r d s : *chatbot, neural networks, application, encryption, copyright, privacy, artificial intelligence.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.056
DOI: https://doi.org/10.17721/ISTS.2024.7.62-68

Сергій ТОЛЮПА, д-р техн. наук, проф.
ORCID ID: 0000-0003-1715-0761
e-mail: serhii.toliupa@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Сергій ЛАПТЄВ, асп.
ORCID ID: 0000-0002-7291-1829
e-mail: salaptiev@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ РАДІОСИГНАЛІВ ЗА ДОПОМОГОЮ ТОПОЛОГІЧНОЇ ІДЕНТИФІКАЦІЇ ЗАГРОЗ

Вступ. *Людство ввійшло в епоху інформаційної цінності, в якій інформація стає ресурсом, важливішим за інші ресурси. Тому доступ до інформації, особливо до конфіденційної, зокрема і до інформації, яка містить основні конкурентні переваги, є першочерговим завданням конкурентної розвідки. Отримання такої інформації, найчастіше, пов'язане з порушенням закону та застосуванням спеціальних технічних засобів. Нині є можливість розв'язувати складні проблеми щодо витікання інформації швидшими темпами, але спеціалісти технічної розвідки можуть використовувати нові способи проникнення у вашу систему, щоб викрасти важливу інформацію та завдати непоправної шкоди.*

Методи. *Досліджено методи виявлення небезпечних радіосигналів, які можуть бути сигналами від радіозакладних пристроїв. Запропоновано вдосконалений метод виявлення радіосигналів, вказане вдосконалення засновано на використанні топологічної ідентифікації загроз. Метод засновано на тому, що об'єкт інформаційної діяльності треба розбити на фрактали, тобто області самоподібності. Області самоподібності визначаються фізичними властивостями радіосигналів. Крім фрактальної розмірності, з метою значного підвищення ймовірності виявлення небезпечних радіосигналів, як ідентифікацію радіосигналів вводять відповідні фрактальні міри. Фрактальні міри додатково дозволяють визначати зони, в яких виявляються небезпечні радіосигнали. Задаючи відповідні еталонні значення відповідних параметрів радіосигналів можна визначати фрактальні розмірності через показник Герста і залежно від отриманого значення розмірності можна ідентифікувати небезпечні радіосигнали, сигнали радіозакладних пристроїв або інших пристроїв знімання інформації, які встановлені на об'єкті з конфіденційною інформацією. Використання запропонованого методу дозолить збільшити ефективність виявлення сигналів радіозакладних пристроїв та у випадку виявлення таких сигналів блокувати канал витікання інформації.*

Результати. *Згідно з дослідженнями аналітиків 76 % міжнародних компаній та державних установ стикались із промисловою розвідкою. За допомогою технічних засобів видобувається 80–90 % необхідної інформації. У зв'язку із цим, зберігання у таємниці комерційно важливої інформації, дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Для отримання доступу до комерційної інформації зловмисник застосовує технічні засоби. Одним із видів технічних засобів є радіозакладний пристрій. Для передавання інформації створюється канал передавання отриманої інформації. Тому дуже важливим є питання виявлення та блокування каналів витікання інформації.*

Висновки. *Доведено, що використовуючи методи фрактальної геометрії, можна об'єкт інформаційної діяльності розбити на фрактали, на області самоподібності. Критеріями, за якими визначають ці області, є фізичні принципи роботи закладних пристроїв. Задаючи відповідні еталонні значення відповідних параметрів, можна визначати фрактальні розмірності через показник Герста.*

Ключові слова: *радіосигнал, радіозакладний пристрій, витікання інформації, фрактальна розмірність.*

Вступ

Людство увійшло в епоху інформаційної цінності, в якій інформація стає ресурсом, важливішим за інші ресурси. Тому доступ до інформації, особливо до конфіденційної інформації, зокрема і до інформації, яка містить основні конкурентні переваги, є першочерговим завданням конкурентної розвідки. Отримання такої

інформації, найчастіше, пов'язане з порушенням закону та застосуванням спеціальних технічних засобів. Нині є можливість розв'язувати складні проблеми з витікання інформації більш швидкими темпами, але спеціалісти технічної розвідки можуть використовувати нові способи проникнення у вашу систему, щоб викрасти важливу інформацію та завдати непоправної шкоди. Якість інформації, що використовується, дозволяє отримувати відповідний економічний або моральний ефект. Згідно з дослідженнями аналітиків 76 % міжнародних компаній і державних установ стикались із промисловою розвідкою. За допомогою технічних засобів видобувається 80–90 % необхідної інформації. У зв'язку із цим, зберігання у таємниці комерційно важливої інформації, дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Відповідно до мети, яку ставить для себе конкурентна розвідка, використовують різні канали витікання інформації. Існує багато різних типів моделей, які дають можливість виявляти окремі різні канали витікання інформації.

Тому розроблення й удосконалення моделей та методів ідентифікації каналів витікання конфіденційної інформації на об'єкті інформаційної діяльності нині є дуже актуальними.

Метою цієї статті є підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів.

Огляд літератури. Питанням захисту конфіденційної інформації, розробленню та вдосконаленню моделей виявлення каналів витікання інформації та сигналів радіозакладних пристроїв присвячено значну кількість публікацій.

У роботі (Козачок, 2017) розглянуто різні методи біометричної статичної та динамічної ідентифікації, що дозволяє підвищити ступінь захисту інформації. Ці методи базуються на фізіологічних особливостях людини. На основі цих фізіологічних особливостей можна будувати різні математичні моделі ідентифікації. Вказані моделі можна використовувати у процесі створення різних технологій захисту інформації з обмеженим доступом. Але цей принцип не дозволяє повною мірою захистити конфіденційну інформацію.

Дослідженнями, висвітленими у працях (Sobchuk, Samoilenko, & Samoilenko, 1999) визначено велику кількість параметрів для ідентифікації кібератак на інформаційні системи. Ідентифікація кібератак дає можливість підвищити рівень захисту інформації. Проте кібератаки ідентифікуються не повною мірою та визначені лише для вузького класу об'єктів, до того ж, постійно розвиваються. Тому ідентифікація не розв'язує проблему повністю.

В роботах В. Собчука, О. Капустяна, О. Барабаша, О. Машкова розкрито особливості ідентифікації в корпоративних інформаційно-телекомунікаційних системах. Досліджено сучасні засоби ідентифікації. Проте методи ідентифікації не розглянуто з погляду можливих інформаційних атак. Не запропоновано математичної моделі, за допомогою якої можна створювати технологію виявлення загроз.

Учені О. Барабаш, Н. Лукова-Чуйко, І. Саланда запропоновали технологічне рішення для ідентифікації об'єктів інформаційної діяльності у створені технічних систем охорони. Однак це рішення притаманне не кожній системі, більшість із них залишаються поза розробленим методом.

Дослідження таких учених, як Н. В. Лукова-Чуйко, С. В. Толюпа, С. О. Лаптєв, О. А. Лаптєв, описують метод фрактальної розмірності. Проте його запропоновано лише для ідентифікації для оптичних систем. Це значно скорочує кількість галузей, у яких можна використовувати фрактальний аналіз. Тому розвиток теорії фракталів потребує подальшого поширення на різні галузі й об'єкти інформаційної діяльності.

У науковій літературі є багато методик, методів і моделей, які дають можливість виявляти канали витікання інформації, канали якими відбувається витікання конфіденційної інформації, але загальної або універсальної моделі, або загального методу виявлення каналів витікання інформації, нині не існує.

З огляду на викладене вище, наукове завдання з підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних пристроїв щодо вдосконалення методу виявлення небезпечних радіосигналів на об'єктах інформаційної діяльності є актуальним (Козачок, 2017, с. 42–48).

Методи

У роботі досліджено методи виявлення небезпечних радіосигналів, які можуть бути сигналами від радіозакладних пристроїв. Запропоновано вдосконалений метод виявлення радіосигналів, Вказане вдосконалення засновано на використанні топологічної ідентифікації загроз. Метод засновано на тому, що об'єкт інформаційної діяльності треба розбити на фрактали, тобто області самоподібності. Такі області самоподібності визначаються фізичними властивостями радіосигналів. Крім фрактальної розмірності, з метою значного підвищення ймовірності виявлення небезпечних радіосигналів, як ідентифі-

кацію радіосигналів вводять відповідні фрактальні міри. Фрактальні міри додатково дозволяють визначати зони, в яких виявляються небезпечні радіосигнали. Задаючи відповідні еталонні значення відповідних параметрів радіосигналів, можна визначати фрактальні розмірності через показник Герста і залежно від отриманого значення розмірності можна ідентифікувати небезпечні радіосигнали, сигнали радіозакладних пристроїв або інших пристроїв знімання інформації, які встановлені на об'єкті з конфіденційною інформацією. Використання запропонованого методу дозолить підвищити ефективність виявлення сигналів радіозакладних пристроїв та у випадку виявлення таких сигналів блокувати канал витікання інформації.

Результати

Під час робіт із пошуку та блокування радіозакладних пристроїв на об'єктах інформаційної діяльності, виникає необхідність розбиття приміщення на пошукові зони. Можна розділити загальне приміщення за існуючим розподілом. У кожній пошукової зоні з якоюсь імовірністю може розміщуватися радіозакладний пристрій. Практично це і є початком використання сучасного топологічного аналізу. Такий аналіз можна застосовувати в реалізації різних топологічних ефектів, пов'язаних з аналізом аудіоінформації та аналізу зображень. У процесі дослідження об'єктів у багатьох випадках виникає завдання з'ясувати, яким чином пошукові зони позв'язані. Необхідно зрозуміти, чи можна з однієї пошукової зони (геометричного образу) отримати матеріал для іншої. Тобто вже переходимо у фрактальну теорію – в окремий розділ математики. Частиною фрактальної теорії і є саме топологія системи (Sobchuk, Samoilenko, & Samoilenko, 1999, с. 926–933).

Оскільки фрактал – це множина точок у просторі, то це може бути якась геометрична фігура, що має властивість самоподібності. Тоді дослідження розмірності D вказаного об'єкта можна використовувати у пошуку закладних пристроїв у інших зонах на об'єкті. Підтверджує цю теорію те, що радіосигнали мають ознаки фрактальної структури. Використовуватимемо таке припущення або позначення: якщо фрактальна розмірність області розповсюдження сигналу $D=1$, то це означатиме, що сигнал неперервно розповсюджується без перешкод; якщо $D=2$, то поляризований сигнал поширюється у плоскій області; у разі $D=3$, сигнал розповсюджується у тривимірному просторі. Іншими словами, запропонована фрактальна розмірність дає загальну характеристику розповсюдження сигналу. Однак за наявності завад, область розповсюдження сигналу не можна розглядати як неперервну, тому що в цьому випадку виникають особливі зони, в яких сигнал не поширюється за іншими законами. Тоді в цих випадках фрактальна розмірність уже набуватиме дробове значення. Отже, фрактальну розмірність цієї області залежно від області розповсюдження сигналу, можна в загальному випадку записати виразом (1) (Sobchuk, 2018, p. 233–239):

$$D = k - H, \quad k = \overline{1,3}. \tag{1}$$

Тут H – показник Герста.

Показник Герста невідомий, пояснимо визначення цього показника. Спочатку необхідно розтлумачити поняття – обраний поріг, перевищення якого свідчить про наявність значного радіосигналу в пошукової зоні. Як поріг для радіосигналу бажано використовувати файл зразка. Файл зразка – це файл, який отримали під час сканування радіодіапазону поблизу об'єкта обстеження. Тоді математичний опис виглядатиме так: $\{\Delta_i, i=1,..,n\}$ – послідовність рівнів перевищення порогів радіосигналів від файлу зразка. На рис. 1 зображено, яким способом визначається перевищення порога файлу зразка (Sobchuk et al., 2019, p. 79–95). Дельта на рисунку показує перевищення порога радіосигналу зразка.

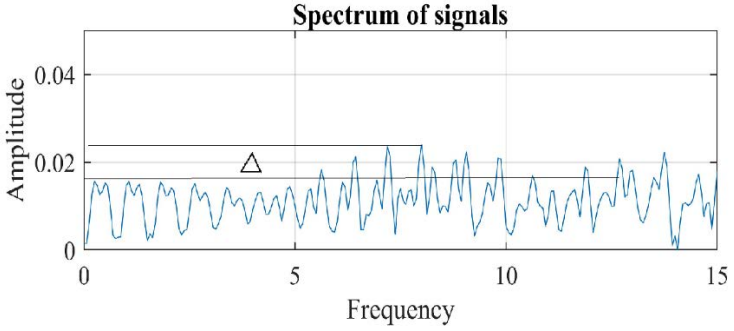

Рис. 1. Визначення перевищення порога заданої порогової амплітуди сигналів

Для виявлення радіозакладного пристрою задають порогову амплітуду A_n і в заданому діапазоні частот від f_1 до f_2 т за допомогою сканувального приймача або спектр-аналізатора визначають i-ту амплітуду сигналу – того сигналу, що наявний у пошуковій зоні.

Загалом маємо

$$\Delta_i = A_i - A_n. \quad (2)$$

Нехай R – розмах між максимальним і мінімальним значеннями цих порогів.

Тоді

$$R = \max \Delta_i - \min \Delta_i. \quad (3)$$

Середнє значення порога Δ визначимо як середнє арифметичне всіх даних, тобто матимемо вираз

$$\Delta = \frac{1}{n}\sum_{i=1}^{n}\Delta_i, \quad (4)$$

а середнє квадратичне відхилення визначатиметься виразом

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\Delta_i^2 - \Delta^2}. \quad (5)$$

З огляду на вирази (3)–(5) і маючи показник Герста, який буде визначатись виразом (6), маємо

$$H = \frac{\ln\left(\frac{R}{\sigma}\right)}{\ln\left(\frac{n}{2}\right)}. \quad (6)$$

Зробивши підстановку, а саме вираз (6) у (2) отримаємо три можливі значення фрактальної розмірності, які описуватимуться виразом (7):

$$D_1 = 1 - H,\ D_2 = 2 - H,\ D_3 = 3 - H. \quad (7)$$

Дослідженнями під час пошукових робіт установлено: якщо фрактальна розмірність має значення $D_1 > 0,6$, то з великою імовірністю можна стверджувати, що на об'єкті, де проводять роботи з пошуку та блокування радіозакладних пристроїв, якраз і розміщено такий пристрій.

Якщо ж фрактальна розмірність набуває значення $1 < D_2 < 1,35$, то на об'єкті відбувається несанкціоноване знімання інформації за допомогою СВЧ-накачки, без використання радіозакладних пристроїв. Проте такий канал витікання інформації дуже важко виявити у зв'язку з тим, що він працює тільки у разі направлення на закладний пристрій спрямованим випромінюванням.

Якщо фрактальна розмірність набуває значення $D_3 > 2$, то на об'єкті міститься цифровий засіб прихованого знімання інформації.

Отже, запропоновано модель і метод, які дозволяють підвищити ефективність виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів.

Варто враховувати, що критерій, за яким знаходять області пошуку, визначається фізичними принципами роботи закладних пристроїв. Тому не слід не звертати увагу на досвід фахівця. Саме досвід фахівця доповнює всі фізично-математичні методи пошуку і дозволяє зрозуміти, в якій частині об'єкта може знаходитись той чи інший тип засобу прихованого отримання інформації. Тому ймовірність виявлення каналів і пристроїв знімання інформації також дуже суттєво залежить від досвіду фахівця (Mashkov et al., 2019, p. 344–357).

Практичне застосування розробленої моделі. З метою практичного використання та підтвердження адекватності розробленої моделі проведено натурне моделювання. Як пошуковий апаратно-програмний комплекс небезпечних радіосигналів у натурному моделюванні застосовували програмно-апаратний комплекс DigScan, який дозволяє програмувати порогове значення радіосигналів. Установлювали різні порогові значення, але в цій роботі за порогове взяли значення амплітуди порога 50 дБ. Частотний діапазон обрали від 50 Гц до 3 МГц, але для моделювання можна було використати і менший діапазон частот. Мета радіомоніторингу полягала в тому, що ми намагалися лише отримати відхилення від установленого нами порогового значення. Тобто у натурному моделюванні нас цікавило лише відхилення від установленого порогового значення (Barabash et al., 2018).

У реальній роботі у процесі пошуку та блокування засобів прихованого отримання інформації, порогове значення встановлюється для кожного конкретного об'єкта. Порогове значення обиралось після попереднього сканування радіодіапазону біля об'єкта. Порогове значення у методичних матеріалах має назву файл зразка. Слід враховувати, що порогове значення діапазону сканування різне і залежить від частотного завантаження місцевості, де розташовано об'єкт.

В результаті натурного моделювання отримали результати, які дозволили вичислити відхилення від порогових значень у заданому частотному діапазоні. Результати сканування у заданому радіапазоні та відхилення амплітуди наведено у таблиці.

ISSN 2707-1758

Таблиця

Результати сканування

i – порядковий номер амплітуди сигналу	Δ_i, дБ
1	–6,0
2	–6,5
3	–4,0
4	1,0
5	0,5
6	–2,0
7	–5,0
8	2,0
9	–4,0
10	–4,5
11	–8,0
12	–10,0
13	–5,0
14	–1,5
15	–3,5
16	–5,0
17	3,0
18	1,0
19	2,0
20	–1,5
21	–1,0
22	–4,5
23	–5,0
24	–6,0
25	–5,5

Використовуючи дані таблиці, визначили, що $\Delta_{\min} = -10$, $\Delta_{\max} = 3$ і згідно з виразом (3) $R = 13$. У подальшому застосували вираз (4) й отримали, що $\Delta = -2{,}84$, середнє квадратичне відхилення рівня згідно з виразом (4) σ = 3,3 дБ. Надалі обчислюємо показник Герста, який згідно з виразом (6) знаходять так:

$$H = \frac{\ln(3{,}94)}{\ln(12{,}5)} = 0{,}54.$$

Маємо такі результати фрактальної розмірності відповідно: $D_1 = 0{,}46$, $D_2 = 1{,}46$, $D_3 = 2{,}46$. За результатами натурного моделювання та математичних обчислень значень фрактальних розмірностей доходимо висновку, що найбільшій області розповсюдження небезпечного сигналу відповідає фрактальна розмірність D_3, а це у свою чергу дає можливість стверджувати, що на об'єкті пошуку сигнал поширюється у тривимірному просторі. Це доводить, що з великою імовірністю можна стверджувати про наявність небезпечних сигналів цифрового діапазону. Тобто є велика ймовірність, що на об'єкті пошуку працює цифровий засіб прихованого знімання інформації. Результати моделювання підтвердили адекватність методу та довели дієвість методу пошуку небезпечних сигналів на об'єкті.

Висновки

В результаті проведених досліджень запропоновано вдосконалений метод виявлення небезпечних сигналів. Запропонований метод надає можливість підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів. Удосконалення полягає у застосуванні у методі топологічної ідентифікації загроз.

Доведено, що використовуючи методи фрактальної геометрії можна об'єкт інформаційної діяльності розбити на фрактали, на області самоподібності. Критерії, за якими знаходять ці області, визначаються фізичними принципами роботи закладних пристроїв. Задаючи відповідні еталонні значення відповідних параметрів можна визначати фрактальні розмірності через показник Герста. За показником Герста, залежно від отриманого значення розмірності можна ідентифікувати вид закладного пристрою, який установлено на об'єкті. Додатково з метою значного підвищення ефективності виявлення закладних пристроїв, варто для покращення виявлення небезпечних сигналів вводити відповідні фрактальні міри. Це надає можливість не тільки виявляти небезпечні сигнали, а ще й визначати місце розташування засобу знімання інформації на об'єкті.

Внесок авторів: Сергій Толюпа – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Сергій Лаптєв – збір емпіричних даних та їх валідація; емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Козачок, В. (2017). Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах. *Сучасний захист інформації*, 2(30), 42–48.

Barabash, O., Lukova-Chuiko, N., Sobchuk, V., & Musienko, A. (2018). Application of petri networks for support of functional stability of information systems. *IEEE 1st International Conference on System Analysis and Intelligent Computing*, SAIC 2018 – Proceedings, 2018. Shatylova dacha str., 4, of. 702, Kharkiv. https: // doi.org/10.1109/SAIC.2018.8516747.

Mashkov, O., Sobchuk, V., Barabash, O., Dakhno, N., Shevchenko, H., & Maisak, T. (2019). Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. *Mathematical Modeling and Computing*, 6(2), 344–357.

Sobchuk, V. (2018). Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. *Statistics Optimal Information Computer*, 6, 233–239.

Sobchuk, V., Barabash, O., Kopiika, O., Zamrii, I., & Musienko, A. (2019). *Modern Mathematics and Mechanics: Fundamentals, Problems and Challenges. Fraktal & Differential Properties of the Inversor of Digits of Q_s-Representation of Real Number*. Springer.

Sobchuk, V., Samoilenko, A., & Samoilenko, V. (1999). On periodic solutions of the equation of a nonlinear oscillator with pulse influence. *Ukrainian Mathematical Journal*, Springer New York, 926–933.

REFERENCES

Barabash, O., Lukova-Chuiko, N., Sobchuk, V., & Musienko, A. (2018). Application of petri networks for support of functional stability of information systems. *IEEE 1st International Conference on System Analysis and Intelligent Computing*, SAIC 2018 – Proceedings, 2018, https: // doi.org/10.1109/ SAIC.2018.8516747.

Kozachok, V. (2017). Peculiarities of identification and authorization in modern corporate information and telecommunication systems. *Modern information protection*, 2(30), 42–48 [in Ukrainian].

Mashkov, O., Sobchuk, V., Barabash, O., Dakhno, N., Shevchenko, H., & Maisak, T. (2019). Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. *Mathematical Modeling and Computing*, vol. 6(2), 344–357.

Sobchuk, V. (2018). Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. *Statistics Optimal Information Computer*, 6, 233–239.

Sobchuk, V., Barabash, O., Kopiika, O., Zamrii, I., & Musienko, A. (2019). *Modern Mathematics and Mechanics: Fundamentals, Problems and Challenges. Fraktal & Differential Properties of the Inversor of Digits of Q_s-Representation of Real Number*. Springer.

Sobchuk, V., Samoilenko, A., & Samoilenko, V. (1999). On periodic solutions of the equation of a nonlinear oscillator with pulse influence. *Ukrainian Mathematical Journal*, Springer New York, 926–933.

Отримано редакцією журналу / Received: 13.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24

Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 0000-0003-1715-0761
e-mail: serhii.toliupa@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Serhii LAPTIEV, PhD Student
ORCID ID: 0000-0002-7291-1829
e-mail: salaptiev@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

IMPROVEMENT OF THE METHOD OF DETECTION OF RADIO SIGNALS WITH THE HELP OF TOPOLOGICAL IDENTIFICATION OF THREATS

B a c k g r o u n d . *Humanity has entered the era of information value. An era in which information becomes a more important resource than other resources. Therefore, access to information, especially to conference information, especially to information that contains the main competitive advantages, is the primary task of competitive intelligence. Obtaining such information is most often associated with breaking the law and using special technical means. Complex data breaches can now be resolved at a faster pace, but tech intelligence professionals can use new ways to penetrate your system to steal valuable information and cause irreparable damage.*

M e t h o d s . *The work examines the methods of detecting dangerous radio signals, which can be signals from radio jamming devices. An improved method of detecting radio signals is proposed, the improvement is based on the use of topological identification of threats. The method is based on the fact that the object of information activity must be divided into fractals, that is, areas of self-similarity. Areas of self-similarity are determined by the physical properties of radio signals. In addition to the fractal dimension, in order to significantly increase the probability of detecting dangerous radio signals, introduce the appropriate fractal measures as the identification of radio signals. Fractal measures additionally allow you to determine the zones in which dangerous radio signals are detected. By setting the appropriate reference values of the relevant parameters of radio signals, it is possible to determine the fractal dimensions through the Hurst index and, depending on the obtained dimension value, it is possible to identify dangerous radio signals, signals of radio interceptor devices or other information capture devices that are installed at the facility with conference information. The use of the proposed method allows to increase the efficiency of detection of signals of radio interceptor devices and, in case of detection of such signals, to block the channel of information leakage.*

R e s u l t s . *According to research by analysts, 76% of international companies and government institutions have encountered industrial intelligence. With the help of technical means, 80-90% of the necessary information is extracted. In this regard, keeping commercially important information secret allows us to successfully compete in the market for production and sales of goods and services. The attacker uses technical means to gain access to commercial information. One of the types of technical means is a radio device. For the transmission of information, a transmission channel of the received information is created. Therefore, the issue of identifying and blocking information leakage channels is very important.*

C o n c l u s i o n s . *It is proved that using the methods of fractal geometry, it is possible to divide the object of information activity into fractals, into areas of self-similarity. The criteria by which these areas are determined are determined by the physical principles of embedded devices. By setting the corresponding reference values of the corresponding parameters, it is possible to determine the fractal dimensions through the Hurst index.*

K e y w o r d s : *radio signal, radio deposit device, information flow, fractal dimension.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.