УДК 004.056
DOI: 10.31673/2409-7292.2021.012629

Хоменко Т.А.

ТОПОЛОГІЧНА ІДЕНТИФІКАЦІЯ СИСТЕМ ПЕРЕДАЧІ ДАНИХ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В роботі розглянуто проблему, пов'язану з виявленням загроз, пов'язаних з витоком інформації по існуючим каналам, які мають різний фізичний принцип на об'єктах інформаційної діяльності. Запропоновано математичну модель, яка базується на теорії фрактального аналізу і яка ідентифікує канал, по якому відбувається несанкціонований виток інформації на об'єкті інформаційної діяльності. На основі експериментальних даних, які були отримані, використовуючи різні канали несанкціонованого зняття інформації на об'єкті інформаційної діяльності, представлена шкала, в якій визначаються інтервали належності розміру фрактальної розмірності, що дає можливість виявити канал, по якому здійснюється намір витоку інформації на об'єкті інформаційної діяльності.

Ключові слова: ідентифікація, сигнал, щільність розподілу, фрактальна розмірність, канал витоку інформації.

Вступ

Серед багатьох завдань, пов'язаних з функціонуванням підприємств різних форм власності і особливо підприємств критичної інфраструктури, основною є захист інформації. Першим і основним початком даного процесу є об'єкт інформаційної діяльності. На цих об'єктах зберігається документація, яка містить комерційну таємницю, здійснюються перемови, які повинні зберігатись в умовах таємниці, набирається пароль клавіатурою персонального комп'ютера для заходу в інтернет-банкінг, та інше. Відповідно до мети, яку ставить для себе шукач конфіденційної інформації з даного об'єкту, використовується відповідний канал витоку інформації. Існує багато моделей, які дають можливість виявляти окремі канали, по яким відбувається виток конфіденційної інформації. Однак, універсальної моделі, за допомогою якої можна було б виявити канал витоку інформації, на теперішній час не існує. Побудові математичної моделі, за допомогою якої можна було б ідентифікувати канал витоку конфіденційної інформації на об'єкті інформаційної діяльності присвячена дана робота.

Постановка проблеми. Основними задачами захисту інформації на об'єктах інформаційної діяльності є ідентифікація загроз від витоку інформації за рахунок різних каналів. При технології захисту інформації з обмеженим доступом важливим є виявлення каналів за допомогою яких здійснюється несанкціоноване зняття інформації. Для цього застосовуються різні методи і моделі ідентифікації. На теперішній час існує багато різних методів ідентифікації, але зі швидким розвитком технологій зняття інформації, вони мають свої недоліки. Тому подальше розв'язування задач для ідентифікації загроз, пов'язаних з витоком інформації на об'єктах інформаційної діяльності є актуальною на теперішній час.

Аналіз публікацій. В роботі [1] розглянуті різні методи біометричної ідентифікації за їх характеристиками і які поділяються на дві групи, а саме статичні і динамічні. Ці методи базуються на фізіологічних особливостях людини. На основі цих особливостей можна будувати різні математичні моделі ідентифікації, які можна застосовувати при створені різних технологій захисту інформації з обмеженим доступом. В роботі [2] визначено кортеж параметрів для ідентифікації кібератак на інформаційні системи, що дає можливість підвищити рівень захисту інформації, але вони визначені лише для вузького класу об'єктів, для яких це необхідно. В роботі [3] розкриті особливості ідентифікації в корпоративних інформаційно-телекомунікаційних системах. Розглянуті сучасні засоби ідентифікації. Однак не запропоновано математичної моделі, за допомогою якої можна створювати технологію виявлення загроз. В роботі [4] запропоновано технологічне рішення для ідентифікації об'єктів інформаційної діяльності при створені технічних систем охорони. Однак, дане рішення притаманне не для кожної системи. В роботі [5] використовується метод фрактальної розмірності для ідентифікації лише для оптичних систем.

Мета статті. Метою даної статті є розробка математичної моделі виявлення наявність загроз на об'єкт інформаційної діяльності на основі теорії фракталів.

Викладення основного матеріалу. При дослідженні об'єктів інформаційної діяльності на наявність закладних пристроїв, виникає необхідність розбиття приміщення на зони, в яких з великою ймовірністю зосереджено пристрій негласного зняття інформації. Сучасний топологічний аналіз використовується в реалізації різних топологічних ефектах, пов'язаних з аналізом аудіо інформації, аналізу зображень [4].При досліджені геометричних об'єктів в багатьох випадках виникає завдання з'ясувати, яким чином геометричні образи зв'язані. Іншими словами необхідно зрозуміти, чи можна з одного геометричного образу отримати інший. Розділом математики, яка вивчає ці питання є фрактальна теорія, частина якою є топологія системи.

Так як фрактал – це геометрична фігура, яка має властивість самодібності, то дослідження розмірності D даного об'єкта можна використовувати при пошуку закладних пристроїв на об'єкті інформаційної діяльності. Це пов'язано з тим, що сигнали і поля мають ознаки фрактальної структури. Якщо фрактальна розмірність області розповсюдженя сигналу, $D=1$, то це означає, що сигнал неперервно розповсюджується по дроту без перешкод. Якщо $D=2$, то розповсюджується поляризований сигнал в плоскій області і при $D=3$ сигнал розповсюджується в трьохвимірном просторі. Іншими словами, фрактальна розмірність дає точну характеристику розпосюдження сигналу.

Однак, при наявності перешкод, область розповсюдження сигналу не можна розглядати як неперевну і в цьому випадку виникають особливі зони, в яких сигнал не розповсюджується. В цих випадках фрактальна розмірність вже приймає дробове значення. Отже, в залежності від області розповсюдження сигналу, фрактальну розмірність цієї області можна в загальному випадку записати наступним чином

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

де H - показник Херста. Визначення показника Херста здійснюється наступним чином.
Нехай $\{\Delta_i, i = \overline{1,n}\}$ - послідовність рівнів порогів перевищення сигналів від файла примірника (попередньо знятий файл радіосигналу), які визначаються в приміщенні, яке досліджується на наявність закладних пристроїв. На рисунку 1 представлено схематично, яким чином визначається поріг перевищення.

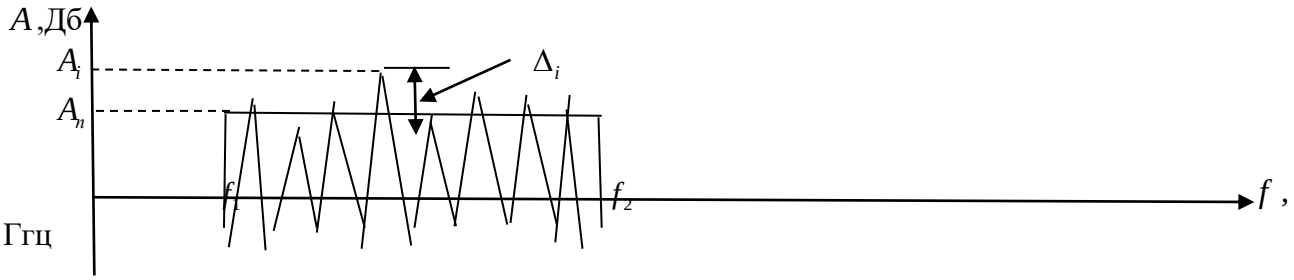

Рис. 1. Визначення порогів перевищення заданої порогової амплітуди.

З рисунку 1 видно, що для виявлення наявності закладного пристрою задається порогова амплітуда A_n і в заданому діапазоні частот від f_1 до f_2 за допомогою скануючого приладу визначається i-та амплітуда сигналу , який є в наявності на ОІД. Тоді,

$$\Delta_i = A_i - A_n$$

Нехай R - розмах між максимальним і мінімальним значенням цих порогів. Тоді

$$R = \max \Delta_i - \min \Delta_i , \tag{2}$$

При цьому, середнє значення порогу Δ визначаємо, як середнє арифметичне всіх значень порогів, тобто

$$\Delta = \frac{1}{n} \sum_{i=1}^{n} \Delta_i , \tag{3}$$

а середнє квадратичне відхилення має вид

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^{n} \Delta_i^2 - \Delta^2} . \tag{4}$$

Тоді, з урахуванням (2)-(4) показник Херста буде визначатись наступним чином

$$H = \frac{\ln\left(\frac{R}{\sigma}\right)}{\ln\left(\frac{n}{2}\right)}. \tag{5}$$

Підставивши (5) в (1) будемо мати три можливих значення фрактальної розмірності, а саме

$$D_1 = 1 - H , \; D_2 = 2 - H , \; D_3 = 3 - H . \tag{6}$$

При проведенні досліджень на ОІД, було встановлено, що якщо фрактальна розмірність має значення $D_1 > 0.6$, то з великою ймовірністю можна стверджувати, що на ОІД, що досліджується в наявності присутня мережевий закладний пристрій. Якщо ж фрактальна розмірність приймає значення $1 < D_2 < 1.35$, то на ОІД відбувається СВЧ накачка і закладний пристрій передає направлений сигнал. І якщо фрактальна розмірність приймає значення $D_3 > 2$, то на ОІД заховано цифровий засіб негласного отримання інформації.

При застосуванні приладу DigScan і при пороговій амплітуді 50 Дб було проведено натурний експеримент на ОІД і отриманні значення перевищення порогу рівнів сигналів представлені в таблиці 1.

Використовуючи дані таблиці 1 знаходимо, що $\Delta_{\min} = -10$, $\Delta_{\max} = 3$ і згідно (2) $R = 13$ Використовуючи формулу (3) маємо, що $\Delta = -2{,}84$, тоді середнє квадратичне відхилення рівня порогу перевищення згідно формули (4) $\sigma = 3{,}3$ Дб. Тоді, показник Херста згідно (5) обчислюється наступним чином

$$H = \frac{\ln(3.94)}{\ln(12.5)} = 0.54 .$$

Тоді, фрактальні розмірності відповідно дорівнюють $D_1 = 0.46$, $D_2 = 1.46$, $D_3 = 2.46$. Отримані значення фрактальних розмірностей показують, що найбільшій області розповсюдження небезпечного сигналу відповідає фрактальна розмірність D_3, що в свою чергу дає можливість стверджувати, що на ОІД, сигнал розповсюджується в трьохвимірному

просторі, що доводить те, що з великою ймовірністю можна стверджувати наявність цифрового засобу негласного отримання інформації на об'єкті інформаційної діяльності.

Таблиця 1.

i	Δ_i в (Дб)	i	Δ_i в (Дб)
1	-6	14	-1.5
2	-6.5	15	-3,5
3	-4	16	-5
4	1	17	3
5	0,5	18	1
6	-2	19	2
7	-5	20	-1,5
8	2	21	-1
9	-4	22	-4,5
10	-4,5	23	-5
11	-8	24	-6
12	-10	25	-5,5
13	-5		

Висновок. Використовуючи характеристики фрактальної геометрії можна довільний об'єкт інформаційної діяльності розбити на фрактали – області самоподібності. Критерій, за яким визначаються ці області визначається фізичними принципами роботи закладних пристроїв. Це залежить від інтуїції фахівця, який розуміє, в якій частині об'єкта може знаходитись той чи інший тип засобу негласного отримання інформації. Також це можна застосовувати і до оптичних засобів – скритих відеокамер. Задаючи відповідні еталонні значення відповідних параметрів можна визначати фрактальні розмірності через показник Херста і в залежності від отриманого значення розмірності можна ідентифікувати вид закладного пристрою, який заховано на ОІД. Однак, варто відмітити, що крім фрактольної розмірності варто в якості ідентифікації вводити відповідні фрактальні міри, за допомогою яких можна визначати зони покриття небезпечними сигналами. Але це є об'єктом подальших досліджень.

Перелік посилань

1. П. Бідюк «Сучасні методи біометричної ідентифікації» / Петро Бідюк, Володимир Бондарчук. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні 1(18) вип., сс. 137-146, 2009.

2. А. Гізун «Основні параметри для ідентифікації порушника інформаційної безпеки» / Андрій Гізун, Владислава Волянська, Вікторія Риндюк, Сергій Гнатюк. Захист інформації. Том 15, №1, Січень-березень, сс. 66-74, 2013.

3. В.А. Козачок, «Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах», Сучасний захист інформації, №2(30), сс. 42-48, 2017.

4. Ю.С. Курской, «Топологическая идентификация оптических систем», Радиотехника, Вип. 196, сс. 51-54, 2019.

5. Соломонова С.Г. «Технологічне рішення для ідентифікації об'єктів інформаційної діяльності у технічній системі охорони», Сучасний захист інформації, №1(41), сс. 49-53, 2020.

6. В.В. Пічкур Теорія динамічних систем. Навчальний посібник. / В.В. Пічкур, О.В. Капустян, В.В. Собчук. – Луцьк: Вежа-Друк, 2020. – 348 с.

Надійшла: 04.02.2021 Рецензент: д.т.н., с.н.с. Лаптєв О.А.