УДК 004.056:621.391.82:519.722
DOI: 10.31673/2409-7292.2026.011799

Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В.

МОДЕЛЮВАННЯ ПРОЦЕСІВ ВИЯВЛЕННЯ ТЕХНІЧНИХ ЗАСОБІВ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ ІНФОРМАЦІЇ В УМОВАХ НАВМИСНОГО ВПЛИВУ ЗАВАД ЗА ДОПОМОГОЮ ВІДСТАНІ КУЛЬБАКА-ЛЕЙБЛЕРА

У статті розроблено математичну модель процесу виявлення технічних засобів несанкціонованого отримання інформації (ТЗНОІ) в умовах впливу навмисних завад, що мають складну структуру та негаусівську природу. Модель побудована на основі односторонньої леми Неймана-Пірсона для перевірки двох гіпотез та використовує відстань Кульбака-Лейблера як інформаційний критерій оцінки ефективності виявлення. Поставлено задачу класифікації сигналів на наявність ТЗНОІ та вплив завад, які можуть бути імпульсними, адаптивними або спеціально сформованими з використанням методів радіоелектронної протидії. Для моделювання процесу враховано стохастичні характеристики сигналів, їх кореляцію та непередбачувану змінність параметрів у часі. Представлено вектор ознак для аналізу сигналів у присутності кількох джерел завад, що дозволяє застосовувати методи машинного навчання для автоматизованого виявлення ТЗНОІ. Проведено експериментальні дослідження з дискретними та неперервними розподілами сигналів і завад, включаючи біноміальний, геометричний, пуассонівський та розподіл Лапласа, які демонструють залежність відстані Кульбака-Лейблера від потужності сигналу ТЗНОІ та характеру завад. Результати показують, що традиційні енергетичні статистики стають неінформативними у присутності стійких навмисних завад, тоді як статистика, що корелює сигнал ТЗНОІ та завади, дозволяє оцінювати інформаційну відокремлюваність гіпотез і забезпечує основу для адаптивних алгоритмів виявлення. Робота створює теоретичну базу для розвитку систем автоматизованого контролю технічного захисту інформації в умовах деструктивного радіоелектронного впливу та може бути використана для подальшого розвитку методів штучного інтелекту та машинного навчання у сфері захисту інформації.

Ключові слова: технічні засоби несанкціонованого отримання інформації, навмисні завади, стохастичний аналіз, відстань Кульбака-Лейблера, машинне навчання, інформаційна безпека, моделювання сигналів.

Вступ

Розвинення існуючих і створення нових методів і підходів щодо виявлення навмисних завад на технічні канали передачі інформації має тісний зв’язок з розвитком ТЗНОІ. Одним з головних факторів розвинення сучасних засобів несанкціонованого отримання інформації є розвиток таких цифрових засобів, що призводить до ускладнення їх виявлення. В умовах сучасних технологічних викликів особливої актуальності набуває проблема виявлення ТЗНОІ в реальному часі, зокрема за умов навмисного впливу завад, спрямованих на маскування їхнього функціонування [1] або зниження ефективності систем контролю технічного захисту інформації (ТЗІ). Зазвичай такі завади мають складну структуру, можуть бути імпульсними, адаптивними або спеціально сформованими з використанням методів радіоелектронної протидії. Існуючі методи технічного контролю мають обмежену ефективність за умов навмисного впливу завад, оскільки ґрунтуються переважно на детермінованих підходах, або використовуються методи теорії ймовірності з використанням відомих законів розподілу. Однак, дослідники не комбінують детермінований і стохастичний характер сигналів ТЗНОІ і складність просторово-часової структури завад. Тому постає необхідність у розробленні нових методів і алгоритмів виявлення ТЗНОІ з використанням сучасних підходів штучного інтелекту, машинного навчання та статистичного аналізу сигналів, які забезпечують адаптивність системи до мінливих умов радіоелектронного середовища.

Постановка проблеми

Збільшення функцій ТЗНОІ та способів їх приховування суттєво ускладнює забезпечення ТЗІ. Особливо складним є завдання їх виявлення в умовах навмисного впливу завад [2], які цілеспрямовано формуються для ускладнення роботи засобів контролю та зниження достовірності результатів пошуку. У зв’язку з цим виникає проблема створення та дослідження моделей процесів виявлення ТЗНОІ, які б враховували навмисний характер завад, їх параметричну невизначеність та вплив на інформативні ознаки виявлення. Розв’язання цієї

проблеми є актуальною так як дозволить підвищити достовірність результатів виявлення, обґрунтувати вимоги до технічних засобів захисту інформації та сформувати основу для розроблення ефективних алгоритмів протидії в умовах деструктивного інформаційного впливу.

Аналіз останніх досліджень і публікацій

Завдання виявлення інформативних і негативних сигналів, які забезпечують обробку інформації є однією з основних задач в сучасних засобах ТЗІ. В роботі [3] запропоновано мінімаксний критерій пошуку оптимальних нелінійних дискретних сигналів загального та спеціального призначення. Даний підхід базується на комбінаторних методах аналізу цифрових сигналів з детермінованою оцінкою інформативних параметрів. В роботі [4] запропоновано правила виявлення радіометричного сигналу на основі методу правдоподібності одної та двохбазової системи прийому. Однак в даній роботі не представлено метрику, яка б давала можливість встановити гіпотези наявності або відсутності сигналів.

В роботі [5] запропоновано використовувати характеристики фрактальної геометрії для виявлення закладних пристроїв. Однак, даний підхід базується на аналізі тільки одного параметру сигналу – амплітуді і не розглядаються дискретні (імпульсні) сигнали. В роботі [6] дається загальна характеристика технічним каналам витоку інформації і встановлюється, що найбільш ризиковим технічним каналом витоку інформації в ІКС є побічне електромагнітне випромінювання. В роботі [7] доводиться, що при абсолютній фазовій модуляції прийом сигналу можливий тільки при точно відомій початковій фазі, однак запропонований підхід дає можливість прийому сигналу з невизначеною початковою фазою і з невизначеною частотою несучого коливання. Однак даний підхід є детермінованим і не враховує випадковість завад. В роботі [8] пропонується *нетипове поєднання аналітичних методів* для задачі розпізнавання радіосигналів. На відміну від загальноприйнятих спектральних методів, автори роблять ставку на *диференціальні спектри і апроксимацію через систему спеціальних функцій*. Але не проведено оцінку роботи запропонованого підходу на реальних вимірювальних даних.

Мета і задачі дослідження

Метою є розроблення та дослідження математичної моделі процесу виявлення ТЗНОІ в умовах навмисного впливу негаусівських і нестаціонарних завад системами технічного захисту інформації. Основні задачі дослідження:

1. Сформулювати стохастичну модель сигналів ТЗНОІ з урахуванням гаусівських шумів і навмисних негаусівських завад зі складною просторово-часовою структурою;
2. Обґрунтувати доцільність використання відстані Кульбака-Лейблера як інформаційного критерію оцінки ефективності виявлення ТЗНОІ;
3. Дослідити поведінку відстані Кульбака-Лейблера для дискретних і неперервних законів розподілу сигналів і завад;
4. Провести експериментальну перевірку запропонованої моделі та проаналізувати залежність ефективності виявлення ТЗНОІ від потужності сигналу та характеристик завад.

Математичне формулювання постановки проблеми

Як відомо, вхідний сигнал $x(t)$ на пристрій, який забезпечує автоматизовану обробку інформації в робочому режимі, можна представити у вигляді рівності (1):

$$x(t) = s(t,\theta) + \eta(t), \tag{1}$$

де $s(t,\theta)$ – корисний сигнал з вектором власних параметрів; $\eta(t)$ – істотний випадковий шум, який має гаусовський розподіл.

Саме сигнал, який має представлення (1), є сигналом від ТЗНОІ. Нехай $z(t,\gamma)$ – сигнал, який є навмисною завадою на пристрій з вектором власних параметрів γ, який здійснює

обробку конфіденційної або таємної інформації. Ця завада має структурні або стохастичні характеристики [9]. Тоді, при наявності навмисних завад, рівність (1) прийме вид:

$$x(t) = s(t,\theta) + z(t,\gamma) + \eta(t). \tag{2}$$

Процес виявлення ТЗНОІ будемо розглядати як задачу прийняття рішення щодо наявності або відсутності сигналу корисного випромінювання $s(t,\theta)$ в умовах дії завад $z(t,\gamma)$ і шумів $\eta(t)$.

Іншими словами, процес виявлення ТЗНОІ уявляє собою стохастичний процес прийняття рішень в умовах невизначеності [10].

Математичне формулювання даної задачі полягає в перевірці двох гіпотез H_0 – корисний сигнал $s(t,\theta)$ спостерігається і H_1 – корисний сигнал не спостерігається. Таким чином маємо:

$$\begin{cases} H_0: \ x(t) = s(t,\theta) + z(t,\gamma) + \eta(t); \\ H_1: \ x(t) = z(t,\gamma) + \eta(t). \end{cases} \tag{3}$$

Система технічного контролю спостерігає реалізацію випадкового процесу (2): $x(t) \in R$, $t \in [0;T]$. Таким чином, задача виявлення ТЗНОІ полягає в визначенні однієї з гіпотез (3) на основі спостереження випадкового процесу (2).

Нехай $p(x(t)/H_i)$ – умовна ймовірність реалізації випадкового процесу $x(t)$ при прийнятті i-ї гіпотези, де $i = \overline{1,2}$. Згідно критерію відношення правдоподібності, перевірка гіпотез полягає в аналізі відношення правдоподібності $L_{H_1,H_2}(x(t))$, яке має наступний вид

$$L_{H_1,H_2}(x(t_k)) = \frac{p(x(t_k)/H_1)}{p(x(t_k)/H_0)}. \tag{4}$$

Якщо для заданого значення $x(t_k)$ рівність (4) приймає велике значення, то висновок схильний до того, що гіпотеза H_0 малоймовірна і її відхиляють; в протилежному випадку відхиляється гіпотеза H_1.

Для правильного визначення значень рівності (4), необхідно розглянути область наступного виду:

$$\left\{x(t_k): \ L_{H_1,H_2}(x(t_k)) > m\right\}; \ k = \overline{1,n},$$

де вибір значення $m > 0$ здійснюється таким чином, щоб виконувалась наступна вимога: розмір критерію дорівнює α (рівень значущості).

Тоді згідно лемі Неймана-Пірсона [11], головний критерій, за яким приймається гіпотеза H_1, визначається областю, яка визначається наступним чином:

$$\Xi = \left\{p(x(t_k)/H_1) > m \cdot p(x(t_k)/H_0)\right\}, \tag{5}$$

з критерієм значущості $\alpha = p(x(t_k)/\Xi)$. Тут α є функцією від m, тобто $\alpha = \alpha(m)$.

Однак, в реальних умовах розподіл $p(x(t)/H_i)$ невідомий, завади $z(t,\gamma)$ є негаусівськими і нестаціонарними, а параметри сигналу змінюються у часі. Таким чином, класичні моделі побудови законів розподілу не спрацьовують.

© Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера. Сучасний захист інформації, 1(65), 142–148.
https://doi.org/10.31673/2409-7292.2026.011799

Інформаційний критерій ефективності виявлення навмисних завад

В якості інформаційного критерія ефективності виявлення навмисних завад будемо використовувати відстань Кульбака-Лейблера [11], яка є мірою, що відрізняє один закон розподілу $p\left(x\left(t\right)/H_1\right)$ від іншого закону розподілу $p\left(x\left(t\right)/H_0\right)$. В цьому підході будемо вважати закон розподілу $p\left(x\left(t\right)/H_1\right)$ – істинним, а закон розподілу $p\left(x\left(t\right)/H_0\right)$ – наближеним. В такому контексті відстань Кульбака-Лейблера є оцінкою якості наближення. Цю відстань від розподілу $p\left(x\left(t\right)/H_1\right)$ до розподілу $p\left(x\left(t\right)/H_0\right)$ будемо позначати як $D_{KL}\left(H_1//H_0\right)$ і для дискретного набору даних $\left\{x\left(t_1\right),x\left(t_2\right),...,x\left(t_n\right)\right\}$ має наступне представлення:

$$D_{KL}\left(H_1//H_0\right)=\sum_{i=1}^{n}p\left(x\left(t_i\right)/H_1\right)\cdot\ln\frac{p\left(x\left(t_i\right)/H_1\right)}{p\left(x\left(t_i\right)/H_0\right)}. \tag{6}$$

У випадку, коли ми маємо неперервні закони розподілу $p\left(x\left(t\right)/H_1\right)$ і $p\left(x\left(t\right)/H_0\right)$ на проміжку часу $[t-\tau;\tau]$, то відстань Кульбака-Лейблера D_{KL} має наступне представлення

$$D_{KL}\left(H_1//H_0\right)=\int_{t-\tau}^{\tau}p\left(x\left(s\right)/H_1\right)\left(\ln\frac{p\left(x\left(s\right)/H_1\right)}{p\left(x\left(s\right)/H_0\right)}\right)dx(s). \tag{7}$$

Варто відмітити, що відстань Кульбака-Лейблера не симетрична, тобто в загальному випадку $D_{KL}\left(H_1//H_0\right)\neq D_{KL}\left(H_0//H_1\right)$ і з урахуванням (5) $D_{KL}\left(H_1//H_0\right)>0$. Якщо ж відстань Кульбака-Лейблера дорівнює нулю, то розподіли $p\left(x\left(t\right)/H_1\right)$ і $p\left(x\left(t\right)/H_0\right)$ співпадають.

На основі проведених експериментальних досліджень в табл. 1 представлено узагальнені результати інтерпретації метрики Кульбака-Лейблера для ТЗНОІ у випадку різних типів розподілів.

Таблиця 1

Інтерпретація метрики Кульбака-Лейблера для ТЗНОІ у випадку дискретних розподілів

№ з/п	Назва закону розподілу	Щільність істинного розподілу $p\left(x\left(t\right)/H_1\right)$ і його параметри	Щільність наближеного розподілу $p\left(x\left(t\right)/H_0\right)$ і його параметри	Відстань Кульбака-Лейблера згідно формули (6)	Інтерпретація щодо ТЗНОІ
1	Біноміаль-ний	$p\left(x\left(t\right)/H_1\right)=C_{10}^{k}\left(0,2\right)^{k}\times$ $\times\left(0,8\right)^{10-k}$	$\left\{0,1;0,15\right\}$	1,135	Активність наявності навмисних завад – гіпотеза H_1 суттєво відрізняється від наявності сигналу від ТЗНОІ – гіпотеза H_0.
2	Геомет-ричний	$p=0,4$ – ймовірність першої спостереження навмисних завад.	$\left\{0,2;0,35\right\}$	0,275	Активність наявності навмисних завад – гіпотеза H_1 мало відрізняється від наявності сигналу від ТЗНОІ – гіпотеза H_0. При таких даних настане час появи отримання інформації по ТЗНОІ.

© Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера. Сучасний захист інформації, 1(65), 142–148.
https://doi.org/10.31673/2409-7292.2026.011799

Продовження Таблиці 1

№ з/п	Назва закону розподілу	Щільність істинного розподілу $p(x(t)/H_1)$ і його параметри	Щільність наближеного розподілу $p(x(t)/H_0)$ і його параметри	Відстань Кульбака-Лейблера згідно формули (6)	Інтерпретація щодо ТЗНОІ
3	Закон розподілу Пуассона	$p(k)=\frac{5^k}{k!}e^{-5};\ k=\overline{0,2}$	$\{0,2;0,35\}$	0,768	Активність наявності навмисних завад – гіпотеза H_1 відрізняється від наявності сигналу від ТЗНОІ – гіпотеза H_0. При таких даних настане час появи отримання інформації від ТЗНОІ за рахунок навмисних завад.

В якості неперервних негаусівських завад розглянемо імпульсні електромагнітні завади, які мають розподіл Лапласа [12]:

$$f(z)=\exp\left(-|z(t)|\right), \tag{8}$$

аналогового засобу негласного отримання інформації передавання мовної інформації який має наступне представлення

$$s(t)=A\cos\left(2\pi f_c t+2,5\sin 2\pi f_m t\right), \tag{9}$$

з числовими значеннями параметрів: $A=10$ мкВ; $f_c=433,92$ МГц; $f_m=1,5$ кГц.

Експериментальна блок-схема проведених досліджень показана на рис. 1.

Рис. 1. Експериментальна блок-схема вимірювань

Сигнал, який має представлення (9) будемо вважати дійсним і введемо статистику, яка має наступне представлення:

$$S=\frac{10}{n}\sum_{i=1}^{n}x(t_i)\cdot\cos\left(867,4\pi t+2,5\sin 3\pi t\right). \tag{10}$$

З урахуванням (8) і (10) було проведено оцінювання розподілів $p(S/H_1)$ і $p(S/H_0)$ за формулою (7).

Наступним кроком є побудова графіку залежності відстані $D_{KL}(H_1//H_0)$ розподілів $p(S/H_1)$ і $p(S/H_0)$ і потужності P_s сигналу $s(t)$. Експериментальні дослідження показують,

© Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера. Сучасний захист інформації, 1(65), 142–148.
https://doi.org/10.31673/2409-7292.2026.011799

що потужність сигналу $s(t)$ ТЗНОІ змінюється в діапазоні від -15 дБ до 10 дБ. На рис. 2 представлено графік залежності $D_{KL}(H_1 // H_0)$ від P_s для $n=6$.

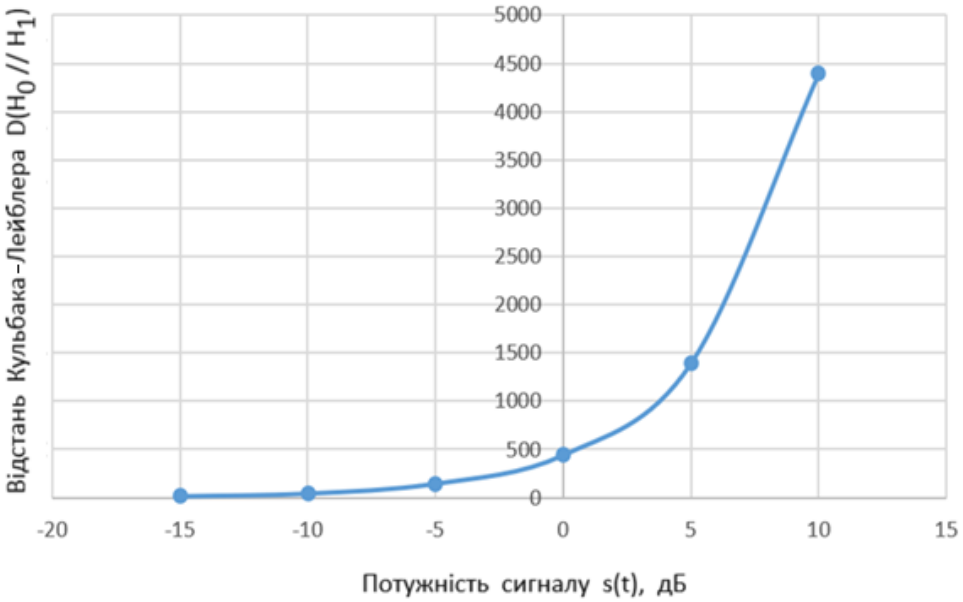

Рис. 2. Графік залежності відстані Кульбака-Лейблера від потужності сигналу ТЗНОЇ за розподілом Лапласа (7) завад

З рис. 1 видно, що відстань Кульбака-Лейблера зростає при умові відокремлення основного сигналу $s(t)$ від завади $z(t)$ і шуму $\eta(t)$. Крім того, для завади, яка розподілена за законом (8), статистика (10), яка корелює сигнали $x(t)$ і $s(t)$ якісно усереднює імпульсність, що призводить до зростання відстані Кульбака-Лейблера зі зростанням потужності сигналу $s(t)$.

Висновки

Для здійснення оцінки інформаційної відокремлюваності гіпотез H_0 – наявності сигналу ТЗНОІ при наявності навмисних завад і гіпотези H_1 – наявності тільки навмисних завад вперше було застосовано відстань Кульбака-Лейблера, яка дає можливість здійснювати класифікацію наявних навмисних завад і несучого сигналу ТЗНОІ.

Виділимо окремі пункти:

1. Сформульовано стохастичну математичну модель процесу виявлення ТЗНОІ, яка враховує одночасний вплив корисного сигналу ТЗНОІ, гаусівського шуму та навмисних негаусівських завад зі складною просторово-часовою структурою. Запропонована модель адекватно описує реальні умови функціонування систем технічного захисту інформації в умовах параметричної невизначеності та нестаціонарності завад;

2. У роботі вперше застосовано відстань Кульбака-Лейблера як інформаційний критерій для оцінки ефективності виявлення ТЗНОІ у присутності навмисних завад, що забезпечує кількісну оцінку відокремлюваності гіпотез «наявність сигналу ТЗНОІ» та «наявність тільки завад». Показано, що дана метрика забезпечує кількісну оцінку інформаційної відокремлюваності гіпотез «наявність сигналу ТЗНОІ» та «наявність лише навмисних завад» і є більш інформативною порівняно з традиційними енергетичними критеріями в умовах стійкого завадового впливу;

© Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера. Сучасний захист інформації, 1(65), 142–148.
https://doi.org/10.31673/2409-7292.2026.011799

3. Досліджено поведінку відстані Кульбака-Лейблера для дискретних і неперервних законів розподілу сигналів і завад, зокрема біноміального, геометричного, пуассонівського та розподілу Лапласа. Встановлено, що значення відстані Кульбака-Лейблера є чутливим до зміни параметрів сигналу ТЗНОІ та характеру завад, що дозволяє використовувати її як універсальний показник ефективності виявлення в умовах різних статистичних моделей;

4. Практичне значення моделі полягає в можливості прогнозування часу виявлення сигналів ТЗНОІ залежно від потужності сигналу та характеристик завад, що сприяє підвищенню достовірності результатів і ефективності протидії деструктивним впливам у критично важливих інформаційних системах.

Отримані результати формують методологічну базу для подальшого розвитку алгоритмів автоматизованого виявлення ТЗНОІ з використанням сучасних підходів штучного інтелекту, зокрема глибокого навчання, а також можуть бути інтегровані у системи контролю технічного захисту інформації в реальному часі.

Перелік посилань

1. Лаптєв О.А., Марченко В.В. (2025) Застосування завад для захисту інформації від витоку радіоканалом. Сучасний захист інформації. №1(61). 89-97. https://doi.org/10.31673/2409-7292.2025.013057.

2. Туровський О.Л., Правдивий А.М. (2024) Моделювання сигналів засобів негласного отримання інформації за допомогою сплайн-функцій. Сучасний захист інформації. №1(57). 22-27. https://doi.org/10. 31673/ 2409-7292.2024.010003.

3. Горбенко І.Д., Замула О.А., Хо Чи Лик (2020) Методи пошуку оптимальних за мінімаксним критерієм систем складних нелінійних дискретних сигналів. Радіотехніка. Вип. 200. 175-187. https://doi.org/ 10.30837/rt.2020.1.200.15.

4. Кудряшов В.Є., Макуха Б.А., Самоквіт В.І., Ялоза І.А. (2020) Правила виявлення радіометричного сигналу при багатоканальному прийомі. Радіотехніка. 2020. Вип. 201. 164-170. https://doi.org/10.30837/ rt.2020. 2.201.15.

5. Хоменко Т.А. (2021) Топологічна ідентифікація систем передачі даних в задачах захисту інформації на об’єктах інформаційної діяльності. Сучасний захист інформації. №1(45). 26-29. https://doi.org/10.31673/2409-7292.2021.012629.

6. Горліченко С.О. (2023) Особливості формування технічних каналів витоку інформації від сучасних ІКС. Ukrainian Scientific Journal of Information Security. Vol. 29. Issue 2, 80-87. https://doi.org/10.18372/2225-5036. 29. 17872.

7. Дакова Л.В., Даков С.Ю., Блаженний Н.В. (2023) Розробка алгоритмів оптимального прийому сигналів із фазорізнецевою модуляцією високої кратності. Ukrainian Scientific Journal of Information Security. Vol. 30. Issue 1. 46-50. https://doi.org/10.18372/2225-5036.30.18602.

8. Дробик О.В., Лаптєв О.А., Пархоменко І.І., Богуславська О.В., Пепа Ю.В., Пономаренко В.В. (2024) Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. Сучасний захист інформації. №2(58). 13-23. https://doi.org/10.31673/2409-7292.2024.020002.

9. Paul Orland (2023) Math for Programmers. Manning Shelter Island. 688. ISBN 978-1-61729-535-5.

10. Novikov O., Ilin M., Stopochkina I., Duduladenko V. (2025) Stealthy Cyberattacks on Control Systems Using an Adaptive Soft-Constrained Optimization Method. Theoretical and Applied Cybersecurity. Vol. 7 №1. 104-110. https://doi.org/10.20535/tacs.2664-29132025.1.333440.

11. Ankur A. Patel. Hands-On Unsupervised Learning Using Python (2020) Beijing・Boston Farnham Sebastopol Tokyo. O'Reilly Media. 425. ISBN 978-1-49203-564-0.

12. Іванченко С.О., Некоз В.С. (2024) Обґрунтування вирішальної схеми для оцінювання імовірності детектування електромагнітних сигналів з метою унеможливлення їх виявлення. Ukrainian Scientific Journal of Information Security. Vol. 30. Issue 2, 212-218. https://doi.org/10.18372/2225-5036.30.19209.

Надійшла до редакції (Received): 19.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

© Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера. Сучасний захист інформації, 1(65), 142–148.
https://doi.org/10.31673/2409-7292.2026.011799