УДК 004.056.53:004.89:621.391.82 https://doi.org/10.15407/pp2026.02.067

Г.В. Шуклін, О.В. Барабаш, А.Б. Гребенніков, І.Д. Данилов, Ю.В. Пепа

АНАЛІЗ СТІЙКОСТІ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВИЯВЛЕННЯ ЗАСОБІВ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ ІНФОРМАЦІЇ В УМОВАХ НАВМИСНИХ ЗАВАД

У роботі запропоновано новий науковий підхід до визначення умов стійкості процесів виявлення технічних засобів несанкціонованого отримання інформації (ТЗНОІ) в умовах впливу навмисних завад. Показано, що стійкість інтелектуальної системи виявлення навмисних завад залежить від часу затримки, який враховується системою диференціальних рівнянь із запізненням, які описують інертність каналів моніторингу, затримки обробки сигналів та адаптивну динаміку параметрів, що характеризують наявність навмисних завад. Для аналізу стійкості системи застосовано овал Рихлінського як інструмент дослідження спектральних властивостей характеристичного квазіполінома систем диференціальних рівнянь із запізненням. Отримано нову умову стійкості процесів виявлення (СПВ) за наявності змінних затримок та активної протидії з боку порушника. Проведено аналітичний та кількісний аналіз динаміки системи, що демонструє ділянки стійкого та нестійкого функціонування інтелектуального модуля виявлення.
Ключові слова: захист інформації, навмисні завади, диференціальні рівняння із запізненням, овал Рихлінського, стійкість, інтелектуальний моніторинг, технічні канали витоку інформації

G.V. Shuklin, O.V. Barabash, A.B. Grebennikov, I.D. Danylov, Yu.V. Pepa

ANALYSIS OF THE RESILIENCE OF AN INTELLIGENT SYSTEM FOR DETECTING MEANS OF UNAUTHORIZED INFORMATION ACCESS IN THE FACE OF DELIBERATE INTERFERENCE

This paper proposes a new scientific approach to determining the stability conditions for processes aimed at detecting technical means of unauthorized information acquisition (TMAIA) under the influence of deliberate jamming. It is shown that the stability of an intelligent system for detecting intentional jamming depends on the delay time, which is accounted for by a system of delay differential equations describing the inertia of monitoring channels, signal processing delays, and the adaptive dynamics of parameters characterizing the presence of intentional jamming. To analyses the stability of the system, the Rychlinski oval is used as a tool for investigating the spectral properties of the characteristic quasi-polynomial of systems of differential equations with delay. A new stability condition for detection processes (SPV) is obtained in the presence of variable delays and active countermeasures by the attacker. An analytical and numerical analysis of the system's dynamics has been carried out, demonstrating the regions of stable and unstable operation of the intelligent detection module.
Keywords: information security, deliberate interference, differential equations with delay, Rychlinski's oval, stability, intelligent monitoring, technical information leakage channels

Вступ

Сучасні системи захисту інформації функціонують в умовах складної електромагнітної та інформаційної обстановки, що характеризується активним застосуванням засобів радіоелектронного придушення, генерацією маскувальних шумів, динамічними змінами параметрів каналів витоку та прихованим функціонуванням стійкості процесів виявлення (СПВ). Особливу небезпеку становлять технічні засоби несанкціонованого отримання інформації, здатні здійснювати приховану передачу даних, адаптуватися до умов середовища, змінювати параметри корисного сигналу.

Класичні моделі виявлення базуються переважно на статичних імовірнісних підходах і не враховують інертність процесів аналізу, тимчасові затримки обробки, накопичувальний ефект перешкод та нелінійну адаптацію порушника.

У зв'язку з цим виникає необхідність розробки динамічних моделей, що враховують запізнення та стійкість процесів виявлення.

Аналіз останніх досліджень

Проблематика виявлення ТЗНОІ в умовах навмисного деструктивного впливу є міждисциплінарною, оскільки поєднує питання технічного захисту інформації, радіомоніторингу, радіоелектронної протидії, статистичного аналізу сигналів, машинного навчання та теорії стійкості динамічних систем із запізненням. Сучасні дослідження в цій сфері свідчать, що класичні статичні підходи до виявлення каналів витоку інформації вже не повною мірою відповідають умовам функціонування сучасних об'єктів інформаційної діяльності, де порушник здатний адаптувати параметри сигналу, створювати імітаційні завади, змінювати спектральні характеристики випромінювання та впливати на роботу інтелектуальних засобів моніторингу.

У роботі [1] розглянуто моделювання процесів виявлення ТЗНОІ в умовах навмисного впливу завад. Автори акцентують увагу на тому, що процес виявлення ТЗНОІ повинен аналізуватися не лише з позиції ймовірності правильного виявлення, а й з урахуванням динаміки зміни ознак сигналу, впливу завад, часових затримок обробки та адаптивної поведінки порушника. В [2, 3] розглянуто адаптивні методи протидії активним шумовим завадам та методи протидії у радіонавігаційних конфліктах. У цих дослідженнях показано, що навмисні завади можуть мати не лише шумовий, а й адаптивний або імітаційний характер. Вони здатні змінювати частотні, часові та енергетичні параметри залежно від поведінки системи виявлення. Це особливо важливо для задач виявлення ТЗНОІ, оскільки порушник може не просто маскувати сигнал, а формувати такі завадові впливи, які спричиняють хибні спрацьовування або знижують достовірність ухвалення рішень інтелектуальним детектором. Автори в [4] досліджують ефективність функціонування систем передачі інформації з хаотичними сигналами та OFDM-модуляцією в умовах впливу навмисних завад. Значущість цього джерела полягає в тому, що автори розглядають вплив завад на складні сигнальні структури, які мають нелінійні та спектрально розподілені властивості. Для задач виявлення ТЗНОІ це має принципове значення, оскільки побічні електромагнітні випромінювання, приховані радіоканали або маскувальні сигнали можуть мати складну спектральну структуру, що ускладнює їх ідентифікацію класичними методами спектрального аналізу.

Окремий напрям досліджень пов'язаний із технічними каналами витоку інформації. Так у роботі [5] проаналізовано технічний канал витоку інформації через побічні електромагнітні пере- випромінювання допоміжних технічних засобів і систем. Це дослідження важливе для формування фізичної основи моделі виявлення, оскільки наявність ТЗНОІ або каналів витоку часто проявляється через амплітудні, частотні, просторові та часові ознаки електромагнітного випромінювання. Саме такі ознаки можуть бути використані як вхідні параметри для інтелектуального детектора. У роботі [6] запропоновано алгоритми вимірювання частоти кадрової розгортки моніторів для частотно-вибіркового придушення каналів витоку інформації. Це джерело демонструє практичний підхід до виявлення та придушення конкретного типу технічного каналу витоку. Його доцільно використати для обґрунтування того, що ефективне виявлення ТЗНОІ потребує не лише реєстрації факту випромінювання, а й аналізу його частотно-часових характеристик, які можуть бути змінені або замасковані під дією навмисних завад. Дослідження [7] присвячене аналізу та моделюванню джерел радіоелектронної боротьби з урахуванням просторово-частотного орієнтування. Значення цієї роботи полягає в тому, що вона враховує не лише спектральні, а й просторові характеристики джерел завад. Для інтелектуальної системи виявлення ТЗНОІ це є важливим, оскільки локалізація джерела сигналу або завади може бути одним із ключових критеріїв ухвалення рішення. Просторово-частотне моделювання дозволяє підвищити достовірність розмежування корисного сигналу, побічного випромінювання та навмисної завади. У роботі [8] розглянуто нейромережеву модель оцінювання рівня захищеності

складнозашумленої мовної інформації. Це дослідження є важливим з позиції використання інтелектуальних методів аналізу сигналів в умовах високого рівня шумів. Нейромережеві підходи дають можливість виявляти приховані закономірності в даних, які важко формалізувати класичними аналітичними методами. У контексті даної статті це підтверджує доцільність використання інтелектуального детектора, який поєднує спектральні, статистичні, кореляційні та ймовірнісні ознаки.

Серед іноземних досліджень важливе місце займає робота [9], в якій запропоновано методи виявлення jamming-атак у мережах IEEE 802.11 на основі машинного навчання. Автори показують, що ML-методи можуть ефективно розрізняти нормальний режим роботи мережі та режим навмисного радіоелектронного придушення. Це є важливим для обґрунтування інтелектуального компонента системи виявлення, оскільки воно демонструє практичну ефективність машинного навчання у задачах ідентифікації навмисних завад. У праці [10] досліджено фізичну автентифікацію супутникових передавачів із використанням глибинного навчання. Автори використовують ознаки фізичного рівня сигналу для ідентифікації джерел випромінювання. Отже, застосування глибинного навчання до фізичного рівня сигналу є перспективним напрямом для підвищення стійкості систем виявлення. У роботі [11] розглянуто захист когнітивних радіомереж від інтелектуального постановника завад, який адаптує свою поведінку залежно від реакції системи. Це дослідження є особливо важливим для даної статті, оскільки в ній також розглядається не звичайний випадковий шум, а саме інтелектуальна завада, яка аналізує роботу детектора та намагається знизити його ефективність. Такий підхід дозволяє розглядати протидію як динамічний процес взаємодії системи захисту та порушника. Дослідження [12] присвячене виявленню атак фальсифікації даних спектрального зондування у мобільних когнітивних радіомережах із використанням методів штучного інтелекту. Показано, що загроза може бути пов'язана не лише з фізичним придушенням сигналу, а й з навмисним викривленням даних, на основі яких система ухвалює рішення. У контексті виявлення ТЗНОІ це означає, що інтелектуальний детектор повинен бути стійким не тільки до шумових завад, а й до фальсифікації або імітації ознак витоку інформації.

У роботі [13] систематизовано методології та виклики використання машинного навчання для гарантування безпеки спільного використання спектра. Автори аналізують атаки на спектральне зондування, включаючи імітацію легітимного користувача та фальсифікацію результатів вимірювання. Зазначимо важливість захисту систем моніторингу від адаптивних і маскувальних впливів, які можуть порушувати достовірність виявлення. В [14] досліджено ефективність frequency hopping як методу протидії jamming-атакам у мережах IEEE 802.11. Це джерело є важливим для розуміння традиційних методів зниження впливу навмисних завад. Разом з тим, воно показує, що навіть ефективні методи частотної перебудови мають обмеження в умовах адаптивного порушника. Це підтверджує необхідність створення більш складних інтелектуальних систем виявлення та протидії, які враховують динаміку завадового впливу.

Математичну основу дослідження стійкості систем із часовими затримками розкрито у працях [15, 16]. В [15] запропоновано покращені критерії стійкості для нейронних мереж із запізненням на основі функціоналів Ляпунова–Красовського, а в роботі [16] досліджено стійкість мережевих систем керування з урахуванням затримок передавання та втрат пакетів. Це положення є близьким до задачі аналізу інтелектуального детектора, в якому затримки обробки, інерційність каналів моніторингу та несвоєчасне оновлення параметрів можуть призводити до втрати стійкості процесу виявлення.

Таким чином, аналіз наукових джерел показує, що на сьогодні достатньо ґрунтовно досліджено окремі аспекти проблеми: технічні канали витоку інформації, методи радіоелектронної протидії, виявлення jamming-атак, застосування машинного навчання до аналізу сигналів, а також математичні критерії стійкості систем із

запізненням. Водночас недостатньо досліджено питання комплексного поєднання цих напрямів у межах єдиної математичної моделі стійкості інтелектуальної системи виявлення ТЗНОІ в умовах навмисних адаптивних завад. Саме це визначає наукову доцільність розробки моделі на основі систем диференціальних рівнянь із запізненням та застосування геометричних критеріїв аналізу стійкості, зокрема овалу Рихлінського.

Мета статті

Метою даної статті є розробка та наукове обґрунтування математичної моделі стійкості процесів виявлення технічних засобів несанкціонованого отримання інформації (ТЗНОІ) в умовах навмисного деструктивного впливу з використанням систем диференціальних рівнянь із запізненням та апарату овалу Рихлінського для аналізу стійкості інтелектуальної системи ухвалення рішень щодо виявлення витоку інформації технічними каналами.

Постановка проблеми

Нехай система захисту здійснює моніторинг об'єкта інформаційної діяльності. Необхідно визначити:

1. Стійкість процесу виявлення;
2. Вплив затримок;
3. Вплив адаптивних перешкод;
4. Умови втрати виявлення.

Введемо наступні позначення:

$x_1(t)$ – інтегральна міра ознак, за якими система виявлення навмисних завад спроможна ідентифікувати наявність технічного каналу витоку інформації;

$x_2(t)$ – змінна, яка характеризує інтенсивність навмисного деструктивного впливу на систему виявлення;

$x_3(t)$ – інтегральна оцінка інтелектуального детектора, структурну схему якого представлено на рис. 1, і яка характеризує внутрішній стан інтелектуальної системи ухвалення рішень.

У табл. 1 представлено перелік ознак для технічних каналів витоку інформації.

Таблиця 1.

Ознаки витоку інформації по технічним каналам

Вид технічного каналу	Ознаки наявності витоку
1. Радіотехнічний канал	А) Амплітуда паразитного випромінювання Б) Стійкі спектральні піки В) Особливості модуляції Г) Гармонічні складові
2. Акустичні і віброакустичні канали	А) Кореляція вібрацій Б) Особливі частоти В) Часові шаблони
3. Побічне електромагнітне випромінювання	А) Рівень побічного електромагнітного випромінювання Б) Просторова локалізація джерела В) Синхронізація з обчислювальними процесами
4. Мережеві приховані канали	А) Аномалії трафіку Б) Нетипова періодичність В) Приховані часові кореляції

У запропонованій моделі розглядаються саме інтелектуальні перешкоди. На відміну від звичайного шуму, який є або стаціонарним, або випадковим і який не адаптується, інтелектуальна перешкода аналізує поведінку системи захисту, змінює свій спектр для імітації корисного сигналу, створює складні кореляції і намагається викликати хибні тривоги.

В табл. 2 представлено види інтелектуальних перешкод, які розглядаються в моделюванні процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад.

Таблиця 2.

Основні види інтелектуальних перешкод

Види інтелектуальних завад	Характеристики завад
1. Активні електромагнітні	А) Широкосмугове зашумлення Б) Імпульсні завади В) Адаптивна зміна частоти
2. Імітаційні	А) Генерація хибних спектральних ознак Б) Копіювання структури сигналу ТЗНОІ
3. Когнітивні	А) Аналіз роботи детектора Б) Динамічна адаптація В) Формування маскуючих послідовностей за допомогою нейронних мереж

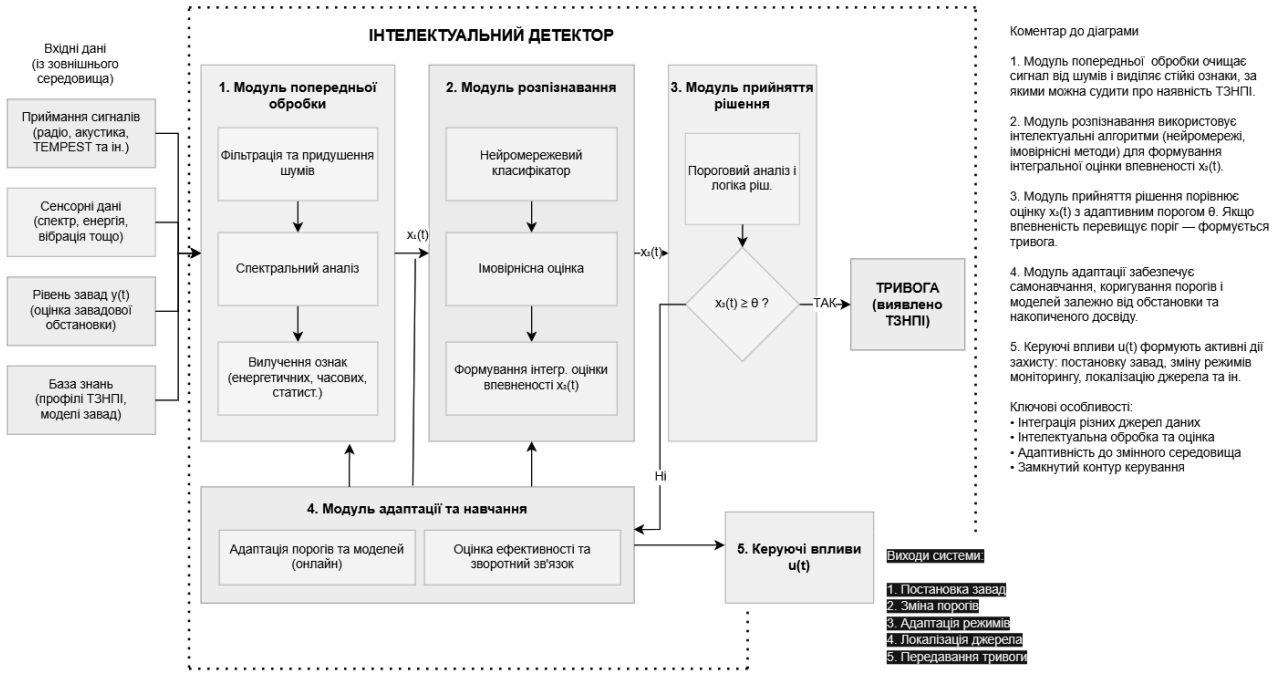

Рис. 1. Структурна схема інтелектуального декодера виявлення ТЗНОІ

За допомогою цієї оцінки рішення не є бінарним, тобто «виявлено/не виявлено». Ця оцінка характеризує впевненість системи в правильності ухвалення рішення в реальному режимі часу. Ця оцінка включає в себе спектральні ознаки, часові аномалії, статистичні відхилення, класифікатори, створені за допомогою нейронних мереж, імовірнісні оцінки і кореляційні показники.

τ – затримка обробки (час запізнення). Ця величина є одним з небезпечних факторів, позаяк в реальних системах миттєвого аналізу не існує.

Основна задача полягає в створені взаємозв'язку динамічних змінних $x_1(t)$, $x_2(t)$, $x_3(t)$ з урахуванням часу запізнення τ за допомогою якої інтелектуальний детектор прийняття рішення виявляє ТЗНОІ.

Викладення основного матеріалу

Математична модель, яка зазначена в меті даної статті, формується системою трьох диференціальних рівнянь з запізненням.

Перше диференціальне рівняння описує динаміку корисного сигналу і має наступний вид

$$\frac{dx_1(t)}{dt} = a \cdot x_1(t) - c \cdot x_2(t) \cdot x_1(t) - b \cdot x_1(t-\tau) + u(t) \ , \tag{1}$$

де a – коефіцієнт підсилення ознак; b – коефіцієнт деградації внаслідок часу затримки τ;
c – коефіцієнт придушення навмисних завад.

Друге диференційне рівняння описує динаміку інтелектуальної (навмисної) завади і має вид:

$$\frac{dx_2(t)}{dt} = d \cdot x_2(t) + g \cdot x_3(t-\tau) + f \cdot \sin(\omega \cdot t) \ , \tag{2}$$

де d – коефіцієнт затухання; g – коефіцієнт адаптації завад; $f \cdot \sin(\omega \cdot t)$ – штучний шумовий вплив.

Третє рівняння моделює інтелектуальний модуль виявлення завад і має наступний вид

$$\frac{dx_3(t)}{dt} = -n \cdot x_2(t) + k \cdot x_3(t) + m \cdot x_1(t-\tau) + l \cdot \sigma(x_1(t)) \ , \tag{3}$$

де n – параметр придушення завадою, який характеризує ступінь руйнівного впливу завад на інтелектуальний детектор.

Перший доданок рівняння (3) визначає деградацію оцінку виявлення ТЗНОІ під впливом завад. Інакше кажучи, цей параметр визначає, наскільки система захисту вразлива до такої завади;

k – параметр затухання інтелектуальної оцінки, який характеризує швидкість втрати накопиченої впевненості інтелектуального детектора. Другий доданок правої частини рівняння (3) визначає істотне затухання внутрішнього стану системи. Інакше кажучи, інтелектуальна система не повинна нескінченно «пам'ятати» старі ознаки. Якщо підозрілі сигнали зникли, то впевненість має поступово зменшуватися, інакше інтелектуальний детектор почне генерувати помилкові сигнали тривоги, стане інертним і втратить здатність до адаптації;

m – параметр чутливості до істинних ознак ТЗНОІ, який визначає наскільки сильно інтелектуальний модуль реагує на ознаки ТЗНОІ. Третій доданок правої частини рівняння (3) описує посилення істотних ознак ТЗНОІ. Інакше кажучи, цей параметр є параметром «уваги» системи до виявленого сигналу. Чим більше значення цього параметра, тим сильніший вплив ознак ТЗНОІ, швидше зростає впевненість інтелектуального детектора і вища ймовірність виявлення ТЗНОІ;

l – параметр інтелектуального нелінійного підсилення, який керує інтелектуальним накопиченням впевненості інтелектуального детектора у виявленні істинних ознак ТЗНОІ:

$$\sigma(x_1(t)) = \frac{1}{1 + e^{-x_1(t)}} \ . \tag{4}$$

Сигмоїда (4) моделює нейронну активність інтелектуального детектора, а також імовірність ухвалення рішень і м'який поріг. У разі малого значення параметра l система диференціальних рівнянь, яка складається з рівнянь (1) – (3), майже лінійна, що свідчить про слабку інтелектуальність детектора і неякісне виявлення прихованих ТЗНОІ. У випадку достатньо великого значення параметра l, система має високий рівень інтелектуальності, що призводить до різкого виявлення аномалій і високої чутливості. Однак водночас є і недоліки, адже виникають нелінійні коливання змінної $x_1(t)$, хаотичні режими і складності стійкості інтелектуальної системи ухвалення рішень.

Розв'язок системи диференціальних рівнянь (1) – (3) має достатньо складне представлення, однак, якщо цю систему лінеаризувати, то можна дослідити стійкість цієї системи навколо її стаціонарної точки $\left(x_1^*, x_2^*, x_3^*\right)$. В інтерпретації математичного визначення стійкості системи виявлення ТЗНОІ введемо наступне означення.

Означення 1. Система диференціальних рівнянь (1) – (3), яка моделює процеси виявлення ТЗНОІ називається стійкою, якщо для довільного $\varepsilon > 0$ і для довільного $t > t - \tau$ виконується система нерівностей

$$\begin{cases} x_1(t) < x_1^* \\ x_2(t) < x_2^* \\ x_3(t) < x_3^* \end{cases}. \quad (5)$$

Після лінеаризації системи (1) – (3) вона матиме наступний вигляд:

$$\frac{dX(t)}{dt} = AX(t) + BX(t-\tau), \quad (6)$$

де $X(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{pmatrix}$, $A = \begin{pmatrix} a & -c \cdot x_1^* & 0 \\ 0 & d & 0 \\ 0 & -n & k \end{pmatrix}$, $B = \begin{pmatrix} -b & 0 & 0 \\ 0 & 0 & g \\ m & 0 & 0 \end{pmatrix}$.

Для системи (5) характеристичне рівняння має наступний вигляд:

$$\det\left(\lambda I - A - B \cdot e^{-\lambda \cdot \tau}\right) = 0 \ , \quad (7)$$

де I – одинична матриця розміром 3х3.

Здійснивши відповідні перетворення, рівняння (6) являє собою наступний квазіполіном:

$$\lambda^3 + v_2\lambda^2 + v_1\lambda + v_0 + \left(b\lambda^2 - b(d+k)\lambda + dbk\right) \cdot e^{-\lambda \cdot \tau} + g \cdot \left(bn + mcx_1^*\right) \cdot e^{-2\lambda\tau} = 0 \ , \quad (8)$$

де $v_2 = -d - k - a$, $v_1 = d \cdot k + a \cdot d + a \cdot k + n \cdot g$, $v_0 = -a \cdot (d \cdot k) + n \cdot g$.

Рівняння (7) є трансцендентним і тому теорема Ляпунова, доведена для систем диференціальних рівнянь (5), у яких відсутній другий доданок правої частини рівняння (5), не є справедливою. Однак Український математик Рихлінський В.А. [1] зумів довести теорему щодо умов стійкості систем диференціальних рівнянь виду (5), яка отримала назву овал Рихлінського.

Суть теореми Рихлінського полягає у визначенні кола (околу) належності кожного спектра матриці

$$Q = A + B \cdot e^{-\lambda \cdot \tau} \ , \quad (9)$$

де кожному її власному числу відповідає область в комплексній площині за наступної умови

$$\begin{cases} |\lambda - a| \le -c \cdot x_1^* + d + k - n \\ |\lambda - d| \le a - c \cdot x_1^* - n + k \\ |\lambda - k| \le a - c \cdot x_1^* + d - n \end{cases}. \quad (10)$$

Система (9), яка визначає область, що носить назву овал Рихлінського, враховує взаємний вплив умов системи і дозволяє точніше оцінювати локальне розташування коренів рівняння (7) в комплексній площині. При цьому, область стійкості (10) повинна задовольняти умови, визначені наступною системою:

$$\begin{cases} |\lambda - a| \cdot |\lambda - d| \le d + k - c \cdot x_1^* - n \\ |\lambda - a| \cdot |\lambda - k| \le -c \cdot x_1^* + d + k - n \\ |\lambda - d| \cdot |\lambda - a| \le a - c \cdot x_1^* - n + k \\ |\lambda - d| \cdot |\lambda - k| \le a - c \cdot x_1^* + d - n \end{cases}. \quad (11)$$

Якщо позначити через $\mathrm{Re}(\lambda)$ дійсні частини власних чисел рівняння (6) і якщо для всіх λ, які належать овалам (10), виконується умова

$$\mathrm{Re}(\lambda) < 0, \quad (12)$$

то система є стійкою.

Продемонструємо вище викладене на конкретному прикладі. Нехай матриця A має наступний вигляд:

$$A = \begin{pmatrix} 1{,}4 & -0{,}35 & 0 \\ 0 & 1{,}1 & 0 \\ 0 & 0{,}3 & 1{,}6 \end{pmatrix}.$$

Після проведених розрахунків за представленням (7) і (10) було отримано наступні значення спектра матриці (9) з побудовою овалу Рихлінського, які представлені на рис. 2:

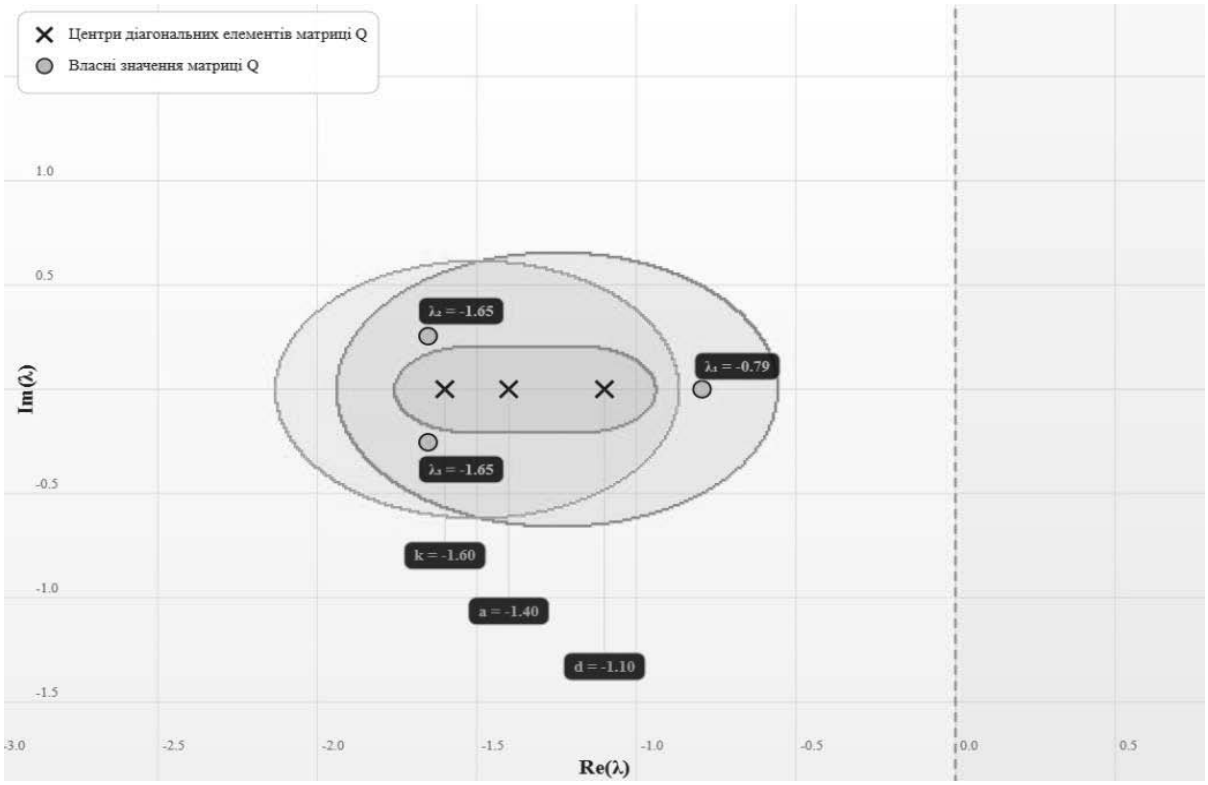

Рис. 2. Овали Рихлінського для лінеарізованої системи (6)

Овали Рихлінського показують, що стійкість диференціальних систем з запізненням визначається не тільки належністю дійсних частин розв'язків характеристичного рівняння (7), а і належністю їх певній області в цій комплексній півплощині. Практично це означає: інтелектуальний детектор здатний стабільно виявляти ТЗНОІ навіть за наявності помірних адаптивних перешкод.

Висновки

У даній роботі розроблено математичну модель процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу перешкод. Застосування систем диференціальних рівнянь із запізненням дозволило описати динаміку корисних ознак, адаптацію навмисних завад, описати структурну схему інтелектуального детектора виявлення ТЗНОІ ухвалення рішень. Уперше було застосовано геометричні представлення овалу Рихлінського, що уможливило забезпечення аналізу стійкості складної нелінійної системи. Отримані результати показують, що критичними факторами деградації виявлення ТЗНОІ є часові затримки, адаптивність перешкод, зростання нелінійності інтелектуального аналізу. Запропонований підхід може стати основою для створення інтелектуальних систем активної протидії ТЗНОІ нового покоління.

Література

1. Khusainov D.Ya., Ivanov A.F., Shuklin G,V.(2005). On a representation of solution of linear delay systems. Differential Equations. 2005. Volume 41. P. 1054-1058 https://link.springer.com/article/10.1007/s10625-005-0249-4
2. Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пепа Ю.В. (2026) Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад. Сучасний захист інформації. №1(65). 142–148 https://doi.org/10.31673/2409-7292.2026.011799
3. Крючкова Л., Ворохоб Н. (2025) Адаптивні методи протидії активним шумовим завадам. Кібербезпека: освіта, наука, техніка. Т. 2. № 30. 455–472. https://doi.org/10.28925/2663-4023.2025.30.987
4. Крючкова Л., Шандрук М. (2025) Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка. № 4(28). 766–780. https://doi.org/10.28925/2663-4023.2025.28.863
5. Васюта К., Збежховська У., Слободянюк В. (2022) Аналіз ефективності функціонування систем передачі інформації з хаотичними сигналами з OFDM-модуляцією в умовах впливу навмисних завад. Information Technology and Security. Vol. 10. Issue 2(19). 216–229. https://doi.org/10.20535/2411-1031.2022.10.2.270439
6. Заболотний В.І., Олейніков А.М., Заболотний Д.М., Кустов А.К. Технічний канал витоку інформації побічними електромагнітними перевипромінюваннями допоміжних технічних засобів і систем. Радіотехніка. 2024. № 218. DOI: 10.30837/rt.2024.3.218.04.
7. Євграфов Д.В., Яремчук Ю.Є. (2022). Алгоритми вимірювання частоти кадрової розгортки моніторів для частотно-вибіркового придушення каналів витоку інформації. Вісник Вінницького політехнічного інституту. 2022. № 4. С. 83–90. https://doi.org/10.31649/1997-9266-2022-163-4-83-90
8. Бибик Р., Опірський І. (2025). Дослідження методів аналізу та моделювання джерел РЕБ з урахуванням просторово-частотного орієнтування. Кібербезпека: освіта, наука, техніка. 2025. Том 2. №30. С.20 – 34 . https://doi.org/10.28925/2663-4023.2025.30.950.
9. Нужний С. (2025) Нейромережева модель оцінювання рівня захищеності складнозашумленої мовної інформації на основі структурної схеми RII. Кібербезпека: освіта, наука, техніка. 2025. №2(30). С. 645-661. https://doi.org/10.28925/2663-4023.2025.30.970
10. Puñal O., Aktas I., Schnelke C.-J., Abidin G., Wehrle K., Gross J. Machine Learning-Based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation. IEEE WoWMoM, 2014. DOI: 10.1109/WoWMoM.2014.6918964.
11. Oligeri G., Sciancalepore S., Raponi S., Di Pietro R. PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning. IEEE Transactions on Information Forensics and Security. 2023. Vol. 18. P. 274–289. DOI: 10.1109/TIFS.2022.3219287.
12. Ibrahim K., Alnajim A.M., Naveed Malik A., Waseem A., Alyahya S., Islam M., Khan S. Entice to Trap: Enhanced Protection against a Rate-Aware Intelligent Jammer in Cognitive Radio Networks. Sustainability. 2022. Vol. 14, No. 5. Article 2957. DOI: 10.3390/su14052957.
13. Yara Cifuentes L.M., Cadena Muñoz E., Cubillos Sánchez R. Development of a Model for Detecting Spectrum Sensing Data Falsification Attack in Mobile Cognitive Radio Networks Integrating Artificial Intelligence Techniques. Algorithms. 2025. Vol. 18, No. 10. Article 596. DOI: 10.3390/a18100596.
14. Wang Q. et al. When Machine Learning Meets Spectrum Sharing Security: Methodologies and Challenges. 2022.
15. Pelechrinis K., Koufogiannakis C., Krishnamurthy S.V. On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks. IEEE Transactions on Wireless Communications. 2010. Vol. 9, No. 10. P. 3258–3271. DOI: 10.1109/TWC.2010.082310.100113.
16. Wang S. etal. Improved Stability Criteria for Delayed Neural Networks via Lyapunov–Krasovskii Functional. Mathematics. 2022. Vol. 10, No. 15. Article 2768.
17. Shao H. A Lyapunov–Krasovskii Functional Plus Approach for Stability of Networked Control Systems with Transmission Delay and Packet Dropouts. 2023.

Дата першого надходження до видання: 04.05.2026
Внутрішня рецензія отримана: 22.05.2026
Зовнішня рецензія отримана: 27.05.2026
Дата прийняття статті до друку: 05.06.2026
Дата публікації: 29.06.2026

Про авторів:

[1]Шуклін Герман Вікторович,
кандидат технічних наук, доцент
Shuklin German,
Ph.D. (technical sciences), associate professor
https://orcid.org/0000-0003-2507-384X
E-mail: mathacadem-kiev@ukr.net.

[1]Барабаш Олег Володимирович,
доктор технічних наук, професор
Barabash Oleg,
Ph.D. (doctor, technical sciences),
professor
https://orcid.org/0000-0003-1715-0761
E-mail: bar64@ukr.net.

[2]Гребенніков Асаді Болдхоягович,
заступник директора
Grebennikov Asadi,
deputy director
https://orcid.org/0000-0002-1207-7609
E-mail: g_as_b@ukr.net.

[3]Данілов Ігор Дмитрович,
аспірант
Danylov Igor,
post-graduate student
https://orcid.org/0009-0000-1426-6414
E-mail: danylovihor@gmail.com.

[3]Пепа Юрій Володимирович,
Доцент
Pepa Yuriy,
Ph.D., associate professor
https://orcid.org/0000-0003-2073-1364
E-mail: yurka14@ukr.net.

Місце роботи авторів:

[1]Національний технічний університет України «КПІ імені Ігоря Сікорського»
NTU of Ukraine “Igor Sikorski Kyiv Politechnical Institute”

[2]Інститут програмних систем НАН України
Institute of Software Systems of the NASU

[3]Державний університет інформаційно-комунікаційних технологій
State university of info-communication technology