

МОДЕЛЮВАННЯ РАДІОВИПРОМІНЮВАНЬ ВІД КОМП'ЮТЕРНО - ЕРГАТИЧНИХ СИСТЕМ

Для вирішення проблеми захисту від несанкціонованого доступу до інформації комп'ютерної ергатичної системи розроблено методику моделювання радіовипромінювань, які її виносять у довкілля. Обґрунтовано розсіяння у широкій смузі частот спектральних складових електромагнітних полів від дискретних зі значеннями в скінченних полях сигналів. Побудовано математичну модель такого сигналу на базі стохастичного періодично стаціонарного процесу. Наведено постановку та метод розв'язування задач виявлення витoku інформації та захисту від нього.

Вступ

Сучасна проблематика освоєння інформаційних ресурсів охоплює низку задач. Проте первинне значення мають задачі виявлення та захисту сигналів. Наприклад, у медицині, навігації, енергетиці, військовій справі, комунальному господарстві, торгівлі, банках тощо набуло великого поширення застосування людино-комп'ютерних (ергатичних [1]) систем [2]. Удосконалення комп'ютерної системотехніки значно розширило сферу застосування комп'ютерно-ергатичних систем (КЕС). Це привело до зростання актуальності проблеми контролю та захисту інформації, яка циркулює у їх трактах.

На сьогодні захист "прямих" інформативних каналів КЕС вивчено достатньо [3, 4], проте залишається можливість відбору і реєстрації фізичних величин у їх довкіллі. У випадку, коли зіставити зміни цих величин з відомими даними, вони стають сигналами (носіями інформації) і через їх опрацювання можна отримати методику контролю та навіть відбору інформації, яку вони переносять.

У даній статті на основі аналізу результатів практичного застосування радіоприймальних засобів для віддаленого контролю за стадіями обробки інформації в КЕС запропоновано модель радіосигналу від КЕС та наведено методи його виявлення та захисту від прийому.

1. Основні положення ідентифікації структури математичної моделі радіовипромінювання від комп'ютерної ергатичної системи

1.1. Фізичні та експериментальні підстави. Робота КЕС супроводжується виникненням різноманітних фізичних полів: інфразвукових, звукових та ультразвукових (пружних коливань середовища — повітря, матеріалу конструкції і т.п.); інфрачервоних, ультрафіолетових, видимих електромагнітних; надвисоко-частотних, високочастотних, низькочастотних, інфранизькочастотних електромагнітних; статичних чи еволютивних електричних і магнітних тощо [5, 6]. Значення параметрів та характеристик цих полів є досить малими за величиною, вони швидко спадають з віддаллю. Проте низькочастотні електромагнітні силові поля (електроживлення процесорів, дисплеїв тощо) та високочастотні електромагнітні поля в інформаційних мережах та монтажу фіксуються стандартними радіоприймальними пристроями на значнішій віддалі. Їх особливістю є розподілення спектру сигналу у широкій смузі частот так, що його база більша за одиницю, оскільки він формується складним об'єктом — КЕС.

Автором ці факти було застосовано для віддаленого контролю за станом КЕС за допомогою стандартного радіоприймача. Емпірично було розроблено методи виявлення типу алгоритму, визначення етапів його виконання. При певному досвіді такого контролю стало можливим й визначення значень параметрів та даних. Стало зрозумілим, що існує несанкціонований канал доступу до інформації, яка циркулює в трактах КЕС. Особливо ефективним цей канал є для добре формалізованої інформації — наукових, технічних числових даних тощо.

Фізично подібні проблеми існують та вивчаються і в інших сферах життєдіяльності людини — радіозв'язку, радіолокації, медицині, охороні довкілля, технічній діагностиці, еко-, гео-, гідро-, біології тощо [7].

1.2. Вплив процесу виконання програм. Гарвардська, Стенфордська, Нейманівська структури комп'ютерної техніки, рекурсивність, трансверсальність, систолічність, конвейерність, сітковість тощо алгоритмів обчислень визначають структуру сигнатури електромагнітного поля у довкіллі [8]. Вона віддзеркалює характер послідовностей керуючих чи обчислювальних команд, потоків даних — алгоритму [9]. Алгоритм складається з окремих частин. Декомпозиція алгоритму на частини визначається через абстракції, що будуються при його специфікації [10], яка виконується в рамках моделі алгоритму (оператора, функції, рекурсії, асимптотики, комбінаторної тотожності тощо, або графа; структура останнього визначається за функцією, яку втілює через обчислення процесор, синтезовану шляхом розв'язування відповідної задачі) [11]. Наведені в п.1.1 експериментальні застосування радіовипромінювань від комп'ютерної техніки підтверджують слушність, конструктивність, коректність цих положень. Структури цих радіовипромінювань безвідносно їх походження можна визначати на базі теорії сигналів за їх реєстрограмами [12, 13].

1.3. Задоволення вимог задачі виявлення сигналу. Сформулювати та розв'язати задачу виявлення сигналу у радіовипромінюванні можна у випадку відповідної фізичної інтерпретовності, математичної коректності і практичної конструктивності його математичної моделі [12, 13]. Існують феноменологічний та сигнальний підходи до побудови структури математичної моделі. Оскільки феноменологічний підхід ґрунтується на повному уявленні про механізм породження явища [12] (сигналу, присутнього у радіовипромінюванні), а поставити у відповідність математичні об'єкти до фізичних елементів КЕС та величин і зв'язків електромагнітного випромінювання від неї практично неможливо, то застосовано сигнальний підхід, при якому моделюються тільки зміни у часові зареєстрованих електромагнітних коливань, які імовірно переносять сигнал, тобто, є інформативними [13]. Тому, з математичної точки зору, зареєстровані випромінювання є випадковою функцією. Звідси виходить постановка задачі виявлення, відбору сигналу, реконструювання інформації [14], яку переносить сигнал від КЕС.

Дані, які переносить сигнал, визначаються на основі його імовірнісних характеристик. Функції розподілу імовірностей появи значень сигналу нескінченно вимірні. З огляду на скінченність (фінітність) енергії сигналу, інваріантність його характеристик до трансляцій у часі, його ергодичність застосовано функцію спектрального розподілу — енергії чи потужності за частотами [13]. Для означення функції спектрального розподілу застосовано систему функцій з спеціальними характеристиками (базис), таку, що сигнал є лінійною формою, де коефіцієнти шукаються за допомогою коефіцієнтного функціоналу — скалярного добутку в отриманому функційному просторі через поповнення множини базисних функцій [15]. Для знаходження множин таких функцій застосовано критерій — відповідний функціонал, який визначає близькість сигналу до його зображення через лінійну форму. Смысл функціоналу — метрика в отриманому нормованому просторі, у фінітному випадку норму, а отже, метрику, визначає енергетичний функціонал [13-15]. Оптимальність оцінки характеристики у вибраному базисові визначено за екстремальними властивостями варіаційних функціоналів від неї [16].

Оскільки прийняті випромінювання (з невідомим сигналом та шумом) за означенням є випадковими, то для виявлення сигналу застосовано критерій, побудований на базі стратегії середнього ризику [14]. Поклавши ентропію за критерій та обмеженість перших двох моментів відповідної функції розподілу імовірностей значень радіовипромінювання, а також її нормованість та додатність, застосуємо відомий розв'язок такої варіаційної задачі — нормальну функцію розподілу. Цей

результат підтверджується й іншими можливими означеннями типу функцій розподілу прийнятого випромінювання — через застосування теорії алгоритмів. Зокрема, через відомі частотне (Мізеса-Колмогорова-Лавленда) [17], складнісне (Колмогорова) [18] та кількісне (теоретико-мірне, Мартіна-Лоефа) [19] означення імовірності послідовності. Останнє є розвитком означення функції розподілу Колмогоровим [18], обґрунтовує побудову лінійних форм (розкладів) прийнятого випромінювання з декомпозицією на сигнальну та шумову частину, що уможлиблює побудову статистики виявлення сигналу і оцінок його достовірності та імовірності помилки [20, 21].

2. Інтерпретація результатів експерименту

На рис.1 наведено вигляд низькочастотної обвідної проміжної високої частоти (465 kHz) у радіоприймальному пристрої (супергетеродин, чутливість порядку $10 \mu V/m$, віддаль від комп'ютера — 10 м), налаштованому на одну з ділянок високочастотного діапазону біля офісу під час редагування (редактор Word, операційна система Windows, комп'ютер стандартної фізичної конфігурації) різних текстів (умовно — текст 1 та текст 2).

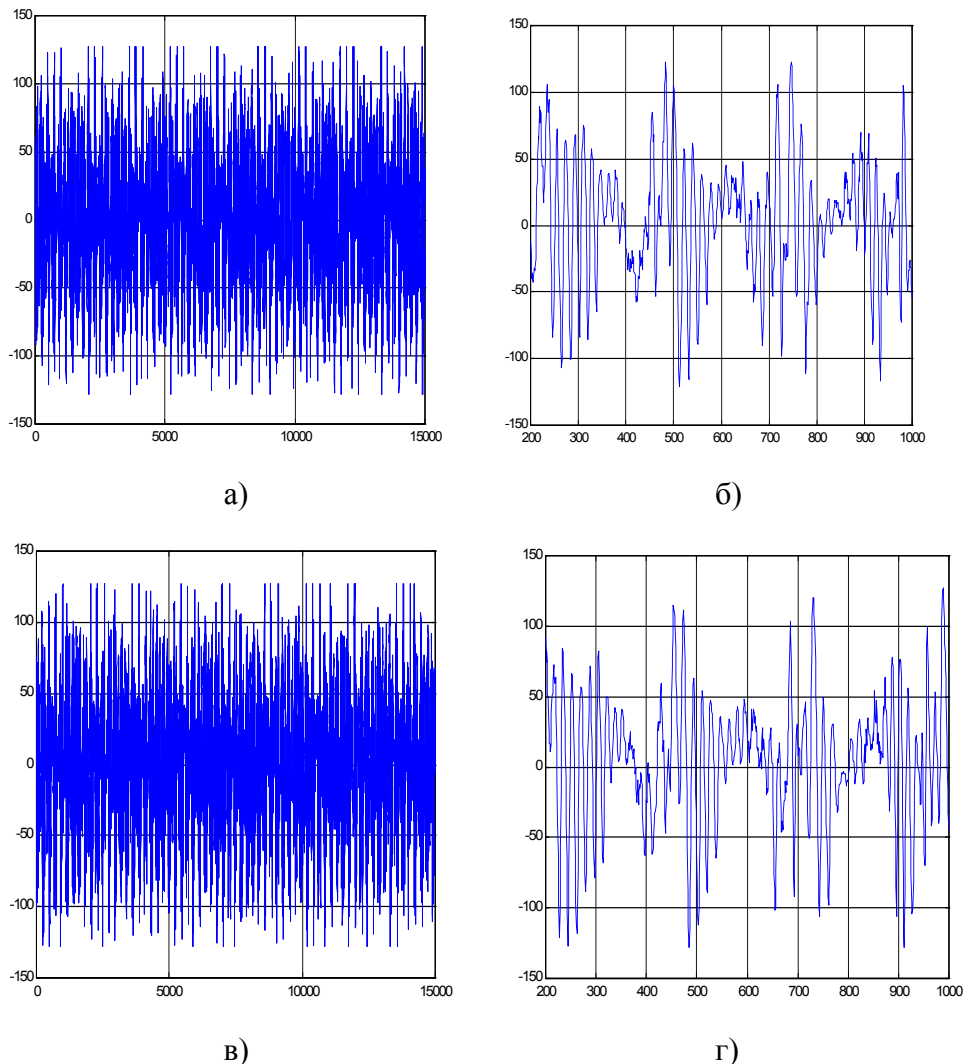


Рис 1. Вигляд низькочастотної обвідної на одній з частот електромагнітного випромінювання офісного комп'ютерного обладнання (а, б -текст 1, в, г - текст 2.

По осі абсцис - номер відліку, період дискретизації 0.1 мS; по осі ординат -значення, рівні $s \cdot \sum_{i=0}^7 2^i$, де s - знак, а i - номер розряду двійкового коду дискретного значення обвідної).

На графіках видно зміни у часові величини низькочастотної обвідної з різними частотами, з різною періодичністю, що пояснюється характером силових та високочастотних електромагнітних полів. Нестрогість періодичності пояснюється впливом дискретних зі значеннями у скінченних полях інформативних електромагнітних полів через накладання, модуляцію та ін. лінійні та нелінійні перетворення. Проте отримати математичні вирази цієї взаємодії практично неможливо, тому подамо її результат методами теорії випадкових процесів, вважаючи, що для одного і того ж тексту відповідні графіки однакові, а для різних — різні в імовірнісному сенсі.

Для побудови алгоритмів оптимального виявлення витоку інформації та ефективного захисту від нього, зарівно ж як і відбору її з каналу витоку, вимагатимемо від моделі радіосигналу відповідних ознак та можливості побудови за ними критерію виявлення його у радіовипромінюванні. Ці ознаки повинні бути стійкими до трансляцій у часові (інваріантними до зсуву у часові), враховуючи специфіку цих зсувів — не обов'язково еквідистантних, як це є у випадку стаціонарних, гармонізованих радіосигналів. Для цього покладемо, що радіосигнал (рис 1) є слабо періодичним. Лінійні моделі АЦП радіовипромінювань у базиса слабоперіодичних функцій застосовано у [20, 21]. Застосуємо їх для моделювання радіовипромінювань від цифрових послідовностей у колах ЕКС. Поклавши радіовипромінювання адитивною сумішшю гармонізованих стохастичних складових — стаціонарної та нестаціонарної, визначатимемо нестаціонарну складову через індикатори складових від різних джерел в ЕКС (за аналогією з [20, 21]).

3. Параметрична ідентифікація структури моделі та застосування її результату

Спектр, який визначається за допомогою індикаторів, назвемо розсіяним, а відповідний йому сигнал — сигналом з розсіяним спектром (СРС). Наприклад, у системах передачі інформації (СПІ) для отримання багатоканальності, зменшення міжканальних завад (інтерференції) аж до ліквідації потреби у розподілі радіоканалів, застосовують розсіювання спектру радіосигналу за випадковим законом у діапазоні частот, набагато більшому за смугу частот, яку займає радіосигнал — $B = \Delta F \cdot T \gg 1$ (тут ΔF — ширина спектру, а T — тривалість радіосигналу) [14, 20, 21]. Теорія уможливорює побудову адекватних до СРС математичних моделей. Феноменологічне математичне моделювання СРС у СПІ принципів труднощів не викликає, оскільки математичні вирази таких сигналів виписуються безпосередньо. У даній роботі застосовано нову, конструктивну з огляду на ефективність її застосування для виявлення невідомих сигналів у радіовипромінюваннях від КЕС, модель СРС. В основу цієї моделі покладено постулати енергетичної теорії сигналів і систем ЕТСС [13], в рамках якої запроваджено та обґрунтовано зображення СРС у вигляді лінійної форми $x(t) = \sum_{i \in I} \alpha_i \varphi_i(t)$, яке уможливорює побудову процедури їх виявлення без синхронізму, безпосередньо з радіовипромінювання.

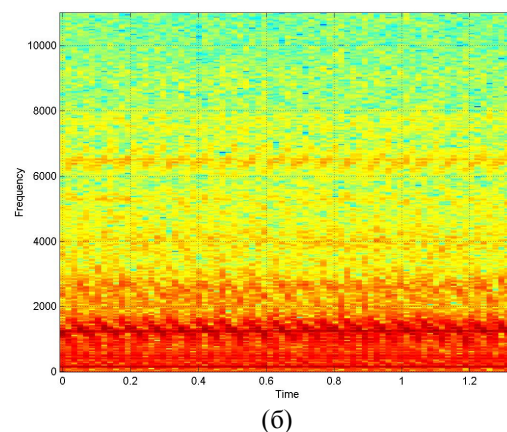
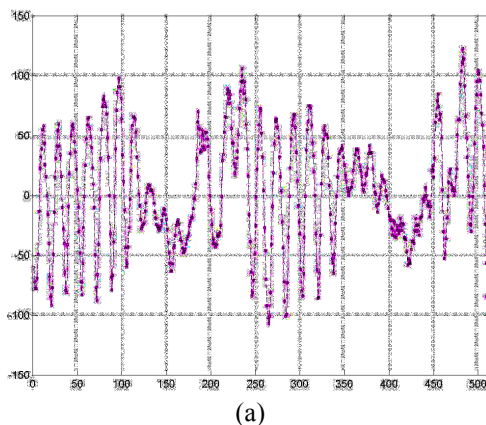
3.1. Спектральний аналіз радіовипромінювання в рамках ЕТСС. Достатньою умовою існування лінійних форм та їх представлень для радіосигналів є обмеженість їх енергії (чи потужності). Необхідні умови визначаються через можливість застосування цих представлень при вирішенні проблеми виявлення, яку забезпечує існування відношення на множині спектральних складових, яке забезпечує їх декомпозицію на дві частини — сигнальну та шумову.

На рис 2 (а) наведено частину графіку з рис. 1 (а), а на рис 2 (а) його звичайну спектрограму. Легко перекопатися у нестаціонарності радіовипромінювання від КЕС — при різних параметрах вікон, довжин вибірки та моментах її відбору для аналізу спектрограма має низьку структурованість, вона розмита..

Покладемо радіовипромінювання, наведене на рис.1 чи рис. 2 (а) таким, що містить періодично корельований процес (ПКП) — радіосигнал. У цьому можна переконаватися, досліджуючи експериментально автокореляційну функцію від нього чи за допомогою візуального аналізу його зареєстрованого графіку. За властивостями спектральної випадкової міри між параметричним виразом та представленням кореляційної матриці раніше встановлено взаємно однозначну відповідність з точністю до пермутаційної еквівалентності, тобто відносно перестановок власних векторів матриці, що відповідають власному значенню. Тому завжди з точністю до цієї умови можна переходити від представлення ПКП через стаціонарні компоненти з повними спектрами до представлення через стаціонарні компоненти з фінітними спектрами, носіями яких є відрізок. Звідси дістанемо потрібну для виявлення сигналу декомпозиційну властивість спектральних компонент. Вона надає можливість визначення порогу виявлення (наприклад, відношення сигнал/шум) при заданні імовірності помилки, а також достовірності виявлення і побудови його тестової статистики в рамках байєсівської стратегії [20, 21].

На рис. 2 (в-е) наведено спектральні компоненти для сигналу "текст 1". (Значення величин, наведені на графіках в умовних одиницях, можна перевести в абсолютні значення через дані, наведені в п. 2; графіки отримано за допомогою GUI Matlab, орієнтація — Az 68, El 72; аналіз проведено за допомогою компонентного методу, програма SPEGRA2 [22]).

3.2. Виявлення сигналу. Спектральні компоненти є інваріантами до еквідистантних зсувів по часовій осі, є ознаками сигналу, який переносить інформацію ("текст 1"), алгоритми його автоматичного виявлення будуються із їх застосуванням. Для цього потрібно апріорно знати вигляд спектральних компонент, що виявляються, та шумів. Для виявлення витікання інформації, а також для контролю роботи КЕС можна користуватися наведеними на рис. 2 компонентами й операторові. (При цьому застосування поворотів, розтягів та інших можливостей опрацювання графіків підвищує ефективність його роботи. Параметри — період кореляції, кількість компонент, кількість суттєвих частотних та часових координат i , відповідно, цін поділок осей визначаються за встановленими апріорно співвідношеннями або шляхом параметричної адаптації (див. [20-22]).



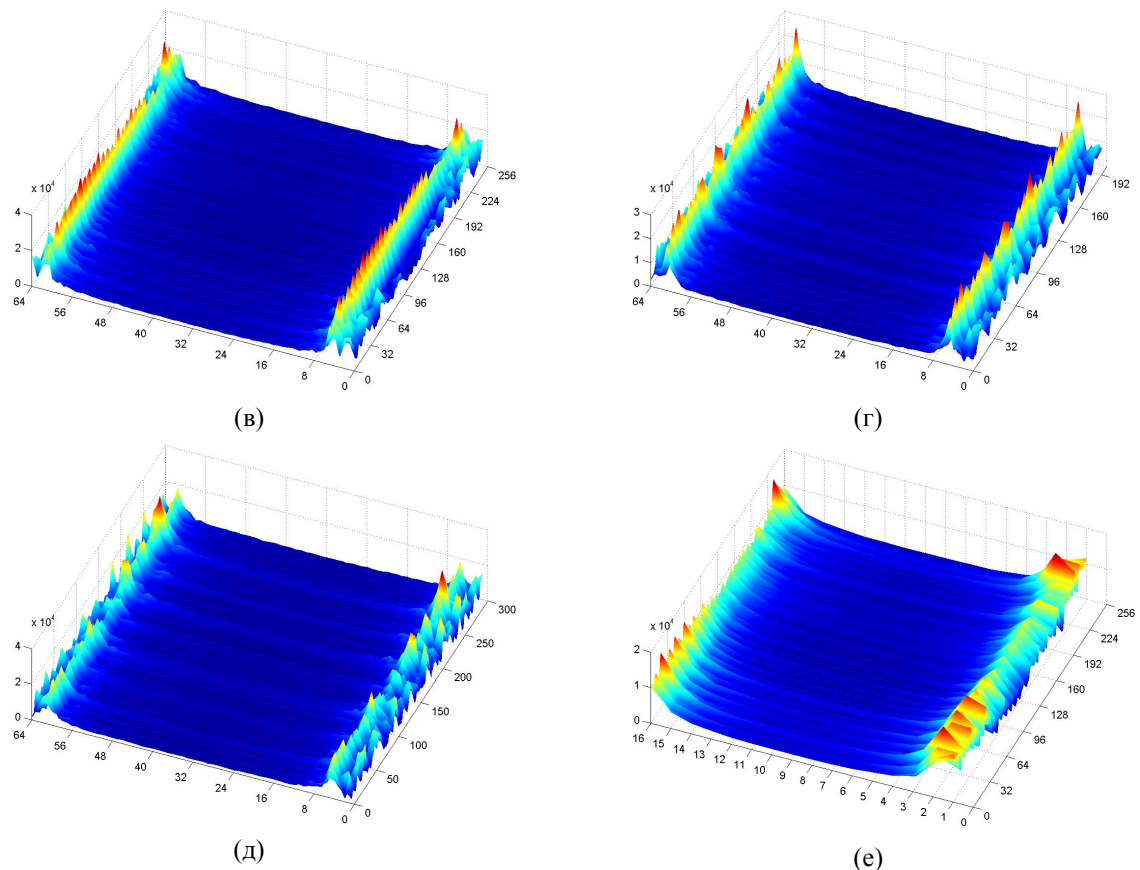


Рис. 2. Результати аналізу радіовипромінювань від КЕС: а — вибірка значень радіовипромінювання (вісь ординат — номер відліку, вісь абсцис — значення двійкового коду); б — спектрограма (вісь абсцис — час, с, вісь ординат — частота, Гц, амплітуда спектральних складових — у псевдокольорі); спектральні (в-е) компоненти (вісь ординат — номери компонент, вісь абсцис — номери частот, апліката — значення спектральної густини потужності в умовних одиницях)

3.3. Маскування сигналу. При розробці методів захисту від несанкціонованого доступу до каналів витоку інформації необхідно дотримуватися стратегії екстремуму ентропії випромінювання від КЕС. Для цього при специфікації алгоритму, яка здійснюється на основі моделі розв'язуваної задачі, потрібно визначити функцію розподілу енергії випромінювань від КЕС під час виконання алгоритму за ізоморфним до часу аргументом спектрального зображення функції, що його моделює. За отриманою функцією розподілу визначається варіабельність інформації в каналах її витоку. Захист від несанкціонованого доступу полягає у зменшенні варіації цієї функції, що, практично, означає згладжування сумарної енергії у всіх каналах випромінювання, наприклад, за допомогою введення в алгоритм спеціальних, неінформативних, а "захисних" операторів.

Висновки

Ідентифіковано структуру математичної моделі радіовипромінювань від КЕС через вирази спектральних представлень слабкоперіодичних функцій. За рахунок застосування нового скалярного добутку модель надає можливість побудови функціоналу відношення правдоподібності (ФВП) та статистики виявлення.

Модель дозволяє побудову адаптивного алгоритму аналізу радіовипромінювань відразу у всій смузі частот їх спектрального представлення та визначення значення ФВП для енергетичного виявлення присутності сигналу у радіовипромінюванні від КЕС та оцінки його достовірності.

Захист від несанкціонованого прийому сигналу полягає у впровадженні додаткових, нефункціональних операторів у програму для збільшення ентропії радіовипромінювання від КЕС.

A problem of defenses a man-computer system relating to without license acceptance of information is explored. A method of modeling of radio waves, are this information carried out in the environment, is developed. It is argue a spreading onto a wide band of electromagnetic field spectral frequencies the energy of discreet with values in finite number fields electrical signals. The mathematical model of such signal is created on a base of a random periodically stationary process. A formulation and solving method of tasks of the information defense are given.

Література

1. Павлов В. В. Начала теории ергатических систем.— Киев: Наукова думка, 1975.— 240 с.
2. Глушков В. М. Основы безбумажной информатики.— М.: Наука, 1982.—552 с.
3. Хоффман Л. Дж. Современные методы защиты информации.— М.: Сов. радио, 1980.— 264 с.
4. Защита информации// ТИИЭР, 1988.— Т.76.— №5.— С. 24-104.
5. Косінов М., Харченко П. Електромагнітний смог — страшне зло сучасної цивілізації. Але може стати і благом, якщо приручити його. //Час, 21.06.1996.
6. Левина А. Мадонна у комп'ютера: с младенцем или без? //Работница, 1991.— №5.— С. 14-15.
7. Информационные связи био-, гелио-, геофизических явлений и элементы их прогноза.//К. С. Войчишин, Я. П. Драган, В. И. Куксенко, В. Н. Михайловский. — Киев: Наукова думка, 1974.— 208 с.
8. Frohwerk R. A. Signature Analysis: a New Digital Field Services Method //Hewlett Paccard Journal, 1977.— May.— P. 2-8.
9. Грин Д., Кнут Д. Математические методы анализа алгоритмов.— М.: Мир, 1987.— 120 с.
10. Лисков Б., Гатэг Дж. Использование абстракций и спецификаций при разработке программ.— М.: Мир, 1989.— 424 с.
11. Dragan Ya. P., Chorna L., Javorskyi B. Energy Theory of Stochastics Signals, Separation of Classes and Specification of Statistical Algorithms.//Proc. of ECSAP—97.—Prague: 1997.—P. 129—132.
12. Пешель М. Моделирование сигналов и систем.— М. :Мир, 1981.— 300 с.
13. Драган Я. Енергетична теорія лінійних моделей стохастичних сигналів.— Львів: Центр стратегічних досліджень еко- біо- технічних систем, 1997.—362 с.
14. Трифонов А. П., Нечаев Е. П., Парфенов В. И. Обнаружение стохастических сигналов с неизвестными параметрами.— Воронежский государственный университет, 1991.— 246 с.
15. Балакришнан А. Введение в теорию оптимизации в гильбертовом пространстве. - М.: Мир, 1974. - 260 с.
16. Драган Я.П., Крива Н.Р., Яворський Б.І. Проблема апостеріорного визначення темпу ритміки// Вісник Тернопільського державного технічного університету.- 1997.- Т.2, № 1.- С. 115-125.
17. Колмогоров А.Н. О таблицах случайных чисел // Семиотика и информация.- М.: ВИНТИ, 1981.- Вып. 2.- С. 3-13
18. Колмогоров А.Н. К логическим основам теории информации и теории вероятностей // Проблемы передачи информации.- 1969.-Т.5, вып. 3.- С. 3-7
19. Martin-Löf P. The definition of random sequences // Information and control.- 1966.- V.9, №6.- P. 602-619.
20. Яворський Б.І. Побудова функціоналу відношення правдоподібностей для сигналів з розсіяним спектром // Відбір і обробка інформації.- К.: Наукова думка, 2004.- Вип. 20(96).- С. 16-21.
21. Яворський Б.І. Цифрове виявлення сигналів з розсіяним спектром і невідомими параметрами // Вісник ТДТУ .- 2004.- Т.9, № 2.- С. 94-103.
22. Система еколого -медичного моніторингу довкілля: Звіт про НДР (заключний) / ТДТУ імені Івана Пулюя. - ДІ-72-97; Інв. № 0200U001720.- Тернопіль, 2000. - 122 с.

Одержано 21.12.2004 р.