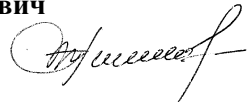


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ШАТИЛО Ярослав Леонідович



УДК 004.621:004.681

**МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ
ФУНКЦІОНУВАННЯ КОМПЛЕКСІВ
ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

Спеціальність 05.13.21 – Системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ 2015

Дисертацією є рукопис.

Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, професор
Бриль Василь Михайлович
Національний авіаційний університет,
професор кафедри інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Скопа Олександр Олександрович,
Одеський національний економічний
університет, завідувач кафедри інформаційних
систем в економіці

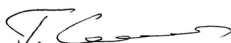
кандидат технічних наук, доцент
Зибін Сергій Вікторович,
Державний університет телекомунікацій,
доцент кафедри комп'ютерних систем і мереж

Захист відбудеться «24» листопада 2015 р. о 15³⁰ на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий « _____ » _____.

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент



С. О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В умовах глобалізації та зростаючої конкурентної боротьби інформаційні системи розвиваються неймовірними темпами, перетворюються на розподілені системи з безліччю об'єктів із різноманітними інформаційними потоками. Наслідком ускладнення інформаційних систем є зростання множини факторів, що впливають на інформаційну безпеку.

Разом із цим постійно зростають загрози несанкціонованого доступу до інформації, порушення її цілісності та конфіденційності. Все це призводить до того, що забезпечення захисту інформаційного ресурсу на сучасному етапі стає найбільш пріоритетною задачею для переважної більшості служб інформаційної безпеки як державних установ так і комерційних організацій. Різні аспекти цього процесу набувають все більшої актуальності.

Оскільки в наш час фактично узаконена деяка лібералізація використання радіочастотного спектру та ринку радіозасобів, що у свою чергу призвело до появи багатьох неконтрольованих пристроїв прихованого зйому інформації та неліцензійованих засобів її передавання, то на зовсім новий, якісний рівень вийшла проблема адекватного протистояння можливим вишкам конфіденційної інформації, а саме виявлення і локалізації потенційно небезпечних сигналів по джерелам їх розповсюдження. Вирішити її відомими математичними методами, які потребують виконання значного обсягу обчислень протягом обмеженого часу наразі стає все більш проблематичним.

У зв'язку з цим виникає необхідність розробки нових аналітичних і чисельно-аналітичних методів рішення складних крайових задач, які суттєво зменшують обчислювальну архітектуру моделювання фізичних процесів при виявленні небезпечних сигналів, а також удосконалення прискорених методів з аналізу та обробки небезпечних сигналів у комплексах технічного захисту інформації (ТЗІ), що і обумовило актуальність теми дисертаційної роботи.

Теоретичні та прикладні питання виявлення та обробки небезпечних сигналів комплексами ТЗІ є предметом досліджень багатьох вітчизняних і зарубіжних вчених, серед яких Скуріхін В. І., Ценков Г. В., Тихонов В. І., Колмогоров А. М., Поляков П. Ф., Петрович М. Т., Розмахнін М. К., Рембовский А. М., Варакін Л. Є., Ашихмін А. В., Баранов В. Л. та ін.

Водночас, дослідження проблеми виявлення і локалізації потенційно небезпечних джерел радіовипромінювання комплексами ТЗІ не набули завершеного характеру, що обумовило вибір теми дисертаційної роботи, визначило її мету і завдання.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах розробки і виконання науково-дослідної роботи «Безпека – 07П», яка виконувалась у відповідності із Постановою Кабінету Міністрів України від 25.12.2005 року № 01086 у Навчально-науковому інституті захисту інформації Державного університету інформаційно-комунікаційних технологій. Автором у межах даної теми удосконалено тео-

ретико-методичні засади підвищення ефективності функціонування комплексів ТЗІ у задачах захисту інформації

Мета і завдання дослідження. Мета дисертаційної роботи полягає у підвищенні ефективності функціонування комплексів ТЗІ шляхом розробки нових та удосконалення існуючих методів виявлення та обробки небезпечних сигналів, які виникають у каналах витоку інформації. Досягнення поставленої мети обумовило постановку та вирішення наступних завдань:

- проаналізувати причини виникнення джерел і каналів витоку інформації, можливості існуючих комплексів ТЗІ при виявленні та обробці небезпечних сигналів у вирішенні задач захисту інформації;
- розробити методи для побудови удосконалених моделей фізичних процесів (полів) у комплексах ТЗІ для виявлення небезпечних сигналів у межах припустимих похибок за заданий час;
- удосконалити метод оцінки місцеположення джерела небезпечного сигналу і виявлення каналів витоку інформації;
- удосконалити прискорені методи аналізу та обробки небезпечних сигналів комплексами ТЗІ.

Об'єктом дослідження виступають процеси вимірювання і обчислення параметрів небезпечних сигналів комплексами ТЗІ.

Предметом дослідження є методи виявлення, аналізу та обробки небезпечних сигналів комплексами ТЗІ небезпечних сигналів, виникаючих у каналах витоку інформації.

Методи досліджень. Теоретичною та методичною основою дисертаційної роботи стали наукові роботи провідних вітчизняних і зарубіжних вчених у сфері забезпечення інформаційної безпеки. У процесі дослідження використано такі теорії та методи: теорія диференціальних рівнянь, графів, ймовірностей, автоматів та інформаційних структур – для моделювання фізичних процесів (полів) та побудови структурно-автоматної марківської моделі комплексів ТЗІ, теорія систем – для аналізу можливостей комплексів ТЗІ щодо захисту інформаційних ресурсів, метод факторного аналізу – для визначення сукупності показників ефективності комплексів ТЗІ, ситуаційного аналізу – для виявлення та ідентифікації небезпечних сигналів, графічного аналізу – для наочного представлення результатів оцінювання ефективності комплексів ТЗІ, кореляційного аналізу – для удосконалення прискореного методу аналізу небезпечних сигналів.

Наукова новизна одержаних результатів. Основним науковим результатом дисертаційної роботи є розвиток теоретичних і методичних засад підвищення ефективності функціонування комплексів ТЗІ та розробка пропозицій щодо моделювання нових та удосконалення існуючих комплексів ТЗІ, їх складу та структури.

Найбільш суттєві теоретичні і практичні результати, що характеризують новизну дослідження, такі:

вперше запропоновано:

– методи моделювання фізичних процесів, які використовують одновимірні зміщені диференціальні перетворення нелінійних крайових задач з лінійними та нелінійними граничними умовами для рішення задач виявлення небезпечних сигналів комплексами ТЗІ за заданий час у межах припустимої похибки, які простіші системо-аналогового методу, заснованого на двовимірних диференціальних перетвореннях, що значно розширює клас вирішуваних задач, а отже і можливості виявлення небезпечних сигналів комплексами ТЗІ; крім того, методи не мають методологічної похибки відображення математичної моделі фізичного процесу в область відображень;

– метод балансу диференціальних спектрів, запропонований для моделювання фізичних процесів, який зводить граничну задачу для рівнянь в частинних похідних до більш простої задачі інтегрування системи звичайних диференціальних рівнянь, яка може бути вирішена одновимірними зміщеними диференціальними перетвореннями або числовими методами, що при заданій похибці підвищує точність виявлення небезпечного сигналу комплексами ТЗІ;

удосконалено:

– метод пошуку та виявлення місцеположення джерела несанкціонованого впливу за рахунок введення процедури оцінки його знаходження та виділення опорного каналу, що, у разі проведення декількох сеансів прийому, дозволяє розширити пошуковий радіус та підвищити точність пошуку місцезнаходження джерела небезпечного сигналу;

– прискорений метод аналізу небезпечних сигналів на основі визначення кореляційної функції при обробці небезпечного сигналу комплексами ТЗІ за рахунок використання адаптивної затримки сигналів, що, на відміну від найбільш відомого мультиплікативного методу кореляційного аналізу визначення функції, дозволяє скоротити час його обробки;

– прискорений метод аналізу небезпечних сигналів на основі виділення стохастичного базису дискретного аргументу при обробці небезпечного сигналу за рахунок представлення в функції послідовності її парних екстремумів, що дозволяє, на відміну від класичних методів, обробку нестационарних процесів та скорочення часу обробки небезпечного сигналу комплексами ТЗІ.

Практичне значення одержаних результатів полягає у тому, що основні положення, викладені автором у дисертації, доведено до рівня методичних розробок та прикладних рекомендацій, призначених для використання у підвищенні ефективності функціонування комплексів ТЗІ.

Науково-практичні висновки та рекомендації прийняті до використання при виконанні науково-дослідної роботи у Навчально-науковому інституті захисту інформації Державного університету інформаційно-комунікаційних технологій «Безпека – 07П», яка виконувалась у відповідності із Постановою Кабінету Міністрів України від 25.12.2005 року № 01086 (Акт реалізації

№ 77 / 391 від 26.06.2012 р.) та у лабораторно-методичному забезпеченні навчального процесу в Інституті Управління державної охорони України Київського національного університету імені Тараса Шевченка у рамках постановки лекційної та лабораторної бази дисципліни «Технічні засоби охорони» (Акт реалізації № 3 / 11 / 3 – 210 від 18.10.2014 р.).

Особистий внесок здобувача. Дисертаційна робота є самостійно виконаною науковою працею, в якій викладено авторський підхід щодо розробки та удосконалення методів підвищення ефективності функціонування комплексів ТЗІ. Всі положення, висновки і пропозиції, винесені на захист, отримані дисертантом самостійно і опубліковані у наукових професійних спеціалізованих виданнях. З наукових праць, опублікованих у співавторстві, використовуються лише ті положення, що є результатом самостійних досліджень здобувача. Особисто здобувачем отримані нові результати дисертаційної роботи. У працях, виконаних у співавторстві, особистий внесок здобувача полягає у наступному: [4] – сформульовано ствердження 1 і 2; [2] – запропоновано алгоритм попереднього стиснення сигналу перед його обробкою; [3] – запропоновано метод застосування лінійних інтегральних перетворень для відновлення небезпечного сигналу за заданим модулем; в [7] – запропонована процедура удосконалення мультиплікативного методу визначення кореляційної функції; [8] - розроблено структуру технічного комплексу.

Апробація результатів дисертації. Основні теоретичні результати дисертаційної роботи та їх практичне застосування доповідались, обговорювались і отримали позитивну оцінку на міжнародних науково-технічних і науково-практичних конференціях, а саме на: Міжнародній науково-технічній конференції «Інформаційні технології та захист інформації», Харків (2012); Першій Міжнародній науковотехнічній конференції «Захист інформації і безпека інформаційних систем», Львів (2012); Міжнародній науково-технічній конференції «Інформаційні технології та безпека інформаційно-комунікаційних систем», Вінниця (2012); International Scientific-Practical Conference «Information Control Systems and Technologies», ICST- Odessa (Одеса, 2013); Міжвідомчій науково-практичній конференції «Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку» (Київ, 2015).

Публікації. За темою дисертаційної роботи опубліковано 13 наукових праць, загальним обсягом 2,52 д.а., (з них 1,57 д.а. належать особисто автору), з них 8 публікацій у наукових спеціалізованих фахових виданнях, затверджених МОН України (2,0 д.а., з них 1,13 д.а. – авторські), 5 тез доповідей на науково-технічних та науково-практичних конференціях. Додатково основні наукові результати відображені у звітах про проведення НДР «Безпека – 07П» і НДР «Технічні засоби охорони», що підтверджується відповідними Актами реалізацій.

Структура і обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків.

Основний зміст дисертації викладено на 141 сторінках комп'ютерного тексту. Дисертація містить 31 рисунок, 15 таблиць, список використаних джерел, що включає 105 найменування на 9 сторінках, 4 додатки на 27 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі дисертаційної роботи проаналізовано стан проблеми, визначено актуальність теми та зв'язок роботи із науковими програмами, планами, темами, сформульовано мету і задачі дослідження, визначено об'єкт, предмет і методи дослідження, вказано наукову новизну, практичне значення отриманих результатів, відомості про особистий внесок здобувача, про апробацію результатів дисертації, публікації, структуру і обсяг дисертації.

Перший розділ *«Аналіз можливостей існуючих комплексів ТЗІ у рішенні задач виявлення та обробки небезпечних сигналів»* присвячений виявленню, систематизації та аналізу причин виникнення каналів несанкціонованого отримання інформації. Проведено порівняльний аналіз фізичної природи носіїв інформації та можливості їх використання в якості каналів витоку інформації. Розглянуті фізичні принципи існування прямих і побічних носіїв інформації, що утворюють систему інформаційного обміну. Показано, що прямі носії інформації породжують чисельні побічні носії, у результаті чого виникає можливість проникнення нелігитимних отримувачів інформації (зловмисників) у систему інформаційного обміну. Проведена класифікація каналів витоку інформації. Розроблено перелік необхідних дій для виявлення побічних електромагнітних випромінювань і наводок комплексами ТЗІ.

Для рішення цих задач виконано аналіз поширених засобів ТЗІ, побудована модель цифрової системи моніторингу ефіру, яка включає виявлення, прийом, обробку і передачу інформації. Проаналізовані переваги та недоліки цифрової обробки сигналу, проведена класифікація комплексів ТЗІ за часом реалізації алгоритмів процедур обробки. Вибір конкретних апаратно-програмних засобів комплексів ТЗІ залежить від ступеню захищеності об'єкта, його діяльності, задач і функцій.

Формалізація проблем виявлення каналів витоку інформації засобами обробки небезпечних сигналів комплексами ТЗІ показала, що аналітичні та чисельно-аналітичні методи, які використовуються на практиці, мають обмежені області застосування. Тому необхідна розробка нових методів з метою розширення можливостей моделювання фізичних процесів і полів при виявленні небезпечних сигналів, удосконалення прискорених методів обробки небезпечних сигналів комплексами ТЗІ, що включено у постановку задач досліджень.

У другому розділі *«Особливості моделювання фізичних процесів і полів при виявленні небезпечних сигналів комплексами ТЗІ»* розроблені методи моделювання фізичних процесів для рішення задач виявлення небезпечних сигналів комплексами ТЗІ.

Вперше запропоновано метод моделювання фізичних процесів на основі одновимірних зміщених диференціальних перетворень нелінійних крайових задач у межах припустимої помилки за заданий час для рішення задач виявлення небезпечних сигналів комплексами ТЗІ.

Розглядаються фізичні процеси, які описуються функцією $u(x_1, x_2)$ двох незалежних змінних в області, що визначається обмеженнями: $0 \leq |x_1| \leq H_1$, $0 \leq |x_2| \leq H_2$, де $H_1, H_2 > 0$.

Для побудови моделі такого процесу виконуються два одновимірні зміщення процесу з використанням системи двох одновимірних зміщених диференціальних перетворень

$$U_v(k_1, x_2) = \frac{H_1^{k_1}}{k_1!} \left(\frac{\partial^{k_1} u(x_1, x_2)}{\partial x_1^{k_1}} \right) x_1 = x_{1v},$$

$$U_v(x_1, k_2) = \frac{H_2^{k_2}}{k_2!} \left(\frac{\partial^{k_2} u(x_1, x_2)}{\partial x_2^{k_2}} \right) x_2 = x_{2v},$$
(1)

де $k_1, k_2 \in (0, 1, 2, \dots, C)$.

Виконується моделювання диференційного спектра замість моделювання реального фізичного процесу $u(x_1, x_2)$ та отримується деяка модель фізичного процесу у вигляді диференціального рівняння, яке має безліч часткових рішень:

$$f \left(x_1, x_2, u, \frac{\partial u}{\partial x_1}, \frac{\partial u}{\partial x_2}, \frac{\partial^2 u}{\partial x_1^2}, \frac{\partial^2 u}{\partial x_2^2}, \dots, \frac{\partial^m u}{\partial x_1^m} \right) = 0.$$
(2)

Для моделювання конкретного фізичного процесу необхідний вибір рішення, яке задовольняє граничним умовам, заданим у вигляді: умови Діріхле

$u(x)|_{x \in \Gamma} = \varphi(x)$, умови Неймана $\frac{du(x)}{dn} \Big|_{x \in \Gamma} = \bar{\varphi}(x)$, зміщеної умови

$$\left| \frac{du(x)}{dn} + \beta u \right|_{x \in \Gamma} = \varphi^*(x),$$
(3)

де $\varphi, \bar{\varphi}, \varphi^*, \beta$ неперервні функції, визначені на граничній поверхні Γ , а $\frac{du(x)}{dn}$

означає похідну, взяту у точці поверхні Γ у напрямку нормалі до неї.

Виконуємо обернені зміщення – диференціальні перетворення:

$$u(x_1, x_2) = \sum_{k_1=0}^{\infty} \left(\frac{x_{1v}, x_{1v}}{H_1} \right)^{k_1} U_v(k_1, x_2),$$
(4)

або

$$u(x_1, x_2) = \sum_{k_2=0}^{\infty} \left(\frac{x_2, x_{2v}}{H_2} \right)^{k_2} U_v(x_1, k_2). \quad (5)$$

Підставимо конкретні значення для k_1, k_2 , порівняємо результати, за їх різницею отримаємо абсолютні похибки. Якщо вони не задовольняють заданій точності рішення, підставимо у праву частину $(k+1) \dots$, доки не отримаємо потрібну точність.

Запропонований метод моделювання простіше відомого методу, заснованого на двовимірних диференціальних перетвореннях. Порівняння запропонованого методу з відомим комбінованим методом, що використовує кінцево-різницеву апроксимацію похідних по одній змінній та одновимірні диференціальні перетворення по іншій, показало перевагу запропонованого методу, який не містить методологічної похибки відображення математичної моделі фізичного процесу в область відображень.

В роботі також розглянуті **крайові задачі з нелінійними граничними умовами**.

Диференціальні перетворення дозволяють розширити область застосування системоаналогового методу на нелінійні крайові задачі та виконувати моделювання за заданий час у межах припустимої похибки.

Пропонується поетапний алгоритм цього методу.

Етап 1. Обирається аналітичний опис фізичного процесу.

Математична модель фізичного процесу $u(x_1, x_2)$ двох незалежних змінних в області, що визначається обмеженнями:

$$0 \leq |x_1| \leq H_1, 0 \leq |x_2| \leq H_2, \text{ де } H_1, H_2 > 0, \quad (9)$$

а H_1, H_2 – задані додаткові константи, представляється у вигляді нелінійної крайової задачі, яка складається з диференціального рівняння в частинних похідних:

$$f\left(x_1, x_2, u, \frac{\partial u}{\partial x_1}, \frac{\partial u}{\partial x_2}, \frac{\partial^2 u}{\partial x_1 \partial x_2}, \frac{\partial^2 u}{\partial x_1^2}, \frac{\partial^2 u}{\partial x_2^2}\right) = 0 \quad (10)$$

і граничних умов трьох основних видів: умови Діріхле, Неймана і змішаної умови (3).

Етап 2. Виконується моделювання процесу у вигляді крайової задачі з нелінійними граничними умовами.

Етап 3. Проводиться переведення рівнянь в область відображень за допомогою диференціальних перетворень:

$$U(k_1, x_2) = \frac{H_1^{k_1}}{k_1!} \left(\frac{\partial^{k_1} u(x_1, x_2)}{\partial x_1^{k_1}} \right)_{x_1=x_{1v}}, \quad (11)$$

$$U(x_1, k_2) = \frac{H_2^{k_2}}{k_2!} \left(\frac{\partial^{k_2} u(x_1, x_2)}{\partial x_2^{k_2}} \right)_{x_2=x_{2v}}, \quad (12)$$

де x_{1v}, x_{2v} – координати фіксованої точки в межах області (9);
 k_1, k_2 – цілочисельні аргументи, що приймають значення $0, 1, 2, \dots, \infty$.

Граничні умови

$$u|_{x_1=\gamma} = \alpha, \quad \frac{\partial u}{\partial x_2}|_{x_2=0} = 0,$$

дозволяють задати початкові значення диференційного спектра $U(k_1, x_2)$ у вигляді

$$U(0, x_2) = \alpha, \quad U(1, x_2) = H_1 \varphi(x_2), \quad (13)$$

де $\varphi(x_2)$ – довільна функція, яку необхідно визначити.

Етап 4. Виконується аналітичне визначення дискрет диференційного спектра $U(k_1, x_2)$ шляхом надання аргументу k значень $0, 1, 2, \dots$. В результаті виконання етапу отримається диференційний спектр.

Етап 5. Здійснюється зворотній перехід з області відображень в область оригіналів зворотніми диференціальними перетвореннями:

$$u(x_1, x_2) = \sum_{k_1=0}^{\infty} \left(\frac{x_1 - x_2}{H_1} \right)^{k_1} U(k_1, x_2), \quad (14)$$

$$u(x_1, x_2) = \sum_{k_2=0}^{\infty} \left(\frac{x_2 - x_{2v}}{H_2} \right)^{k_2} U(x_1, k_2). \quad (15)$$

Відновлюємо оригінал рішення граничної задачі $u(x_1, x_2)$, використовуючи диференційний спектр.

В рішенні граничної задачі міститься невідома функція $\varphi(x_2)$, яка повинна задовольняти граничним умовам:

$$u|_{x_1=\gamma} = \alpha, \quad \frac{\partial u}{\partial x_2}|_{x_2=0} = 0, \quad \left(\frac{\partial u}{\partial x_1} + hu^4 \right) \Big|_{x_1=\beta} = 0, \quad \left(\frac{\partial u}{\partial x_2} + hu^4 \right) \Big|_{x_2=1} = 0.$$

Етап 6. Визначається значення невідомої функції $\varphi(x_2)$ за допомогою граничних умов. Підставимо рішення (13) в граничну умову

$$\left(\frac{\partial u}{\partial x_1} + hu^4 \right) \Big|_{x_1=\beta} = 0. \quad (16)$$

Отримане нелінійне диференціальне рівняння зводиться до лінійного диференціального рівняння, таким чином рішення нелінійної граничної задачі можна отримати в аналітичному вигляді, який містить невідомі параметри.

Етап 7. Для визначення невідомих параметрів рішення некоректної задачі є тільки одна гранична умова (16). Цю некоректність задачі вирішується методом Тихонова А.М. шляхом введення регуляризуючого функціоналу і пошуку його мінімуму.

Запропонований метод розширює область застосування аналітичних моделей на задачі з нелінійними граничними умовами у межах припустимої помилки за заданий час для виявлення небезпечних сигналів комплексами ТЗІ.

Вперше для моделювання фізичних процесів у комплексах ТЗІ запропоновано **метод балансу диференціальних спектрів**, який вирішується створенням балансу сукупності одновимірних зміщених диференціальних перетворень для точного виявлення небезпечних сигналів. Цей метод складається із наступних етапів:

Етап 1. Обирається аналітичний опис фізичного процесу

$$u(x_1, x_2) = \begin{cases} f_1[A(x_1, x_2, a)] \\ f_2[x_1 B(x_2), \beta] \end{cases}, \quad (17)$$

що задовольняє умовам Діріхле, Неймана і змішаній умові на границі Γ середовища.

Етап 2. Диференціальними перетвореннями (4) або (5) переводиться аналітичний опис (17) фізичного процесу в область відображень:

$$U(k_1, x_2) = F_2[k_1, B(x_2), \beta], \quad (18)$$

$$U(x_1, k_2) = F_1[A(x_1), k_2, \alpha], \quad (19)$$

де F_1 – відображення функції f_1 у виразі (17);

F_2 – відображення функції f_2 у виразі (17).

Виконується моделювання процесів вигляду $u(x_1, x_2)$ з використанням системи двох одновимірних зміщень диференціальних перетворень функції $u(x_1, x_2)$ у функцію $U(k_1, x_2)$ цілочисельного аргумента k_1 і незалежної змінної x_2 . Обернені диференціальні перетворення дозволяють по диференціальних спектрах $U(k_1, x_2)$ відновити в області оригіналів процес $u(x_1, x_2)$. Точно так отримуються відповідно прями та обернені зміщені диференціальні перетворення по змінній x_2 .

Етап 3. Переводиться математичну модель фізичного процесу (18, 19) диференціальними перетвореннями в область відображень.

Етап 4. Виконується розрахунок диференціальних спектрів $U(k_1, x_2)$, $U(x_1, k_2)$ по рекурентних виразах (11, 12), використовуючи дискрети диференційного спектра.

Етап 5. Складається баланс одноіменних дискретних диференціальних спектрів відображень математичної моделі фізичного процесу та його аналітичного опису в одних й тих самих точках відліків.

Таким чином, метод балансу диференційних спектрів зводить крайову задачу для рівнянь в частинних похідних до більш простої задачі інтегрування системи звичайних диференціальних рівнянь, яка може бути розв'язана одновимірними зміщеними диференціальними перетвореннями для найбільш точного виявлення небезпечних сигналів комплексами ТЗІ.

У третьому розділі «*Методи виявлення та обробки небезпечних сигналів комплексами ТЗІ*» удосконалюються метод оцінки місцеположення джерела виникнення небезпечних сигналів і прискорені методи їх обробки комплексами ТЗІ.

Запропоновано удосконалений **метод оцінки місцеположення джерела небезпечного сигналу.**

Етап 1. По відліках енергетичного спектру випадкового вхідного процесу, спостережуваного в сигнальному каналі, розраховується оцінка інтенсивності шуму.

Етап 2. У сигнальному і опорному каналах проводиться виявлення вузькополосних сигналів у смузі частот одночасного аналізу.

Етап 3. Для кожного із виявлених у сигнальному каналі сигналів розраховується оцінка відмінності у спостережуваній інтенсивності по відношенню до опорного каналу.

Етап 4. Визначається клас джерела небезпечних сигналів ξ_m у відповідності із правилом:

$$\xi_m = \begin{cases} S_{\text{контр}}, & \text{при } \Delta P_c > \Delta_{\text{пор}2}, \\ \text{невизначений}, & \text{при } \Delta_{\text{пор}1} < \Delta P_c < \Delta_{\text{пор}2}, \\ S_{\text{зовн}}, & \text{при } \Delta P_c < \Delta_{\text{пор}1}, \end{cases} \quad (22)$$

де $S_{\text{контр}}$ – джерело небезпечного сигналу, приналежного зоні контролю;

$S_{\text{зовн}}$ – віддалені джерела радіовипромінювань;

P_c – спостережувальна інтенсивність виявлених сигналів;

$\Delta P_{\text{пор}1}$ і $\Delta P_{\text{пор}2}$ – використовувані пороги, які можуть у кожному конкретному випадку коректуватись з урахуванням властивостей області контролю та розміщення приймальних антен.

Етап 5. Будуються та аналізуються варіанти залежності кількості відліків від відстаней між антенами (сигнальною та опорною), заданого значення ймовірності правильного виявлення сигналу від часу аналізу і кількості сканувань приймача, кількості відліку від вибору параметрів комплексу ТЗІ і наявності екрануючої перешкоди.

Показано, що для підвищення точності визначення місцеположення джерела небезпечного сигналу доцільно проводити декілька сеансів прийому. Від сеансу до сеансу когерентність у кожному із каналів не зберігається. Але

між каналами когерентність у кожному із сеансів зберігається, оскільки на обидві антени надходить один й той самий сигнал.

Для реалізації можливості виявлення малопотужних джерел в умовах складної перешкоджувальної радіообстановки на контрольованому об'єкті розміщуються декілька антен із квазіізотропними діаграмами спрямованості. Одна з антен використовується як «опорна» і розміщується на достатньому віддаленні від об'єкту. Це суттєво збільшує ймовірність розрізнення зовнішніх і внутрішніх джерел випромінювань у складному електромагнітному оточенні та підвищує швидкість пошуку нових сигналів.

Також показано, що при використанні комплексу ТЗІ параметри порогу виявлення і кількості відліку можуть встановлюватись незалежно від умов розміщення об'єкта.

У загальній постановці задача ідентифікації небезпечних сигналів з апріорно невідомими параметрами від джерел їх випромінювання зводиться до побудови вирішального правила виявлення на фоні перешкод. Вона призводить до оптимального приймача радіометричного типу, який аналізує енергетичні параметри сигналу. У роботі показано, що квазіоптимальне рішення дозволяє обмежитись двома приймальними антенами, розміщеними у захищеному приміщенні та поза ним. Це дозволяє з певною ймовірністю зробити висновок про просторове розміщення джерела сигналу відносно захищеного об'єкту.

В дисертації також набули удосконалення **прискорені методи аналізу небезпечних сигналів комплексами ТЗІ**. Підвищення вимог до ефективності аналізу небезпечних сигналів комплексами ТЗІ диктує необхідність подальшого удосконалення існуючих методів.

Кореляційний аналіз є одним з найбільш розповсюджених методів обробки складних сигналів. Розподіл оцінки кореляційної функції $R(\tau)$ випадкових процесів $X(t)$ і $Y(t)$ залежить від закону розподілу самих процесів, від алгоритму обчислення оцінки та від зміни довжини часу реалізації T і кореляції зсуву τ .

На цей час найбільш відомим є мультиплікативний метод визначення $R(\tau)$ засобами комплексів ТЗІ. В дисертації пропонується удосконалений прискорений метод визначення $R(\tau)$, заснований на використанні адаптивної затримки сигналів, що призводить до заміни постійної величини Δt змінною (рис.1). Оскільки амплітудно-часові значення сигналів на ділянках між екстремумами суттєвої інформації не містять, при виконанні операцій із визначенням $R(\tau)$ значення $\{\tau_i\}$ повинні відповідати часовим значенням $x(t)$ та/або $y(t)$. Кореляційна функція при цьому буде представлена нерівномірною послідовністю значень ординат $\{R(\tau_i)\}$, обчислених із тією точністю, яку забезпечує використовуваний кореляційний метод.

У цілому, для розрахунку $R(T)$ доцільно визначати додатково декілька ординат кореляційної функції в області $T=0$. Тим самим досягається спроможність надійного визначення $R(0)$ навіть тоді коли інтервали між початко-

вими та кінцевими екстремумами аналізованого сигналу достатньо великі. В аналізованому сигналі, що дискретизується з кроком $\Delta t = \frac{1}{2} f_{\max}$, де f_{\max} – максимальна частота спектру $x(t)$ кількість екстремумів в середньому в 3–5 разів менше загальної кількості дискретів. Таким чином, використання адаптивної затримки при вирахуваннях $R(t)$ теж пропорційно скорочується.

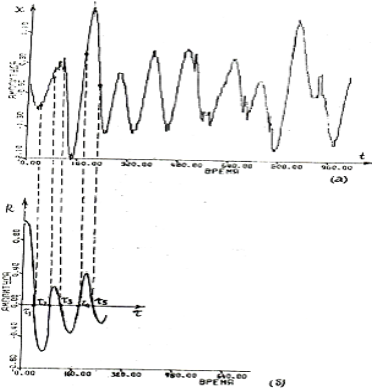


Рис. 1. Реалізація кореляційного методу

В роботі показано, що алгоритмічною простотою формування системи ортогональних функцій також відрізняється стохастичний базис дискретного аргументу. Цей базис є теоретичною основою удосконаленого методу, який за швидкістю на 1,5–2 порядки перевищує найбільш відомі спектральні розходження. Даний метод забезпечує аналіз $x(t)$, який представлений послідовністю його екстремумів і, таким чином, допускає обробку нестационарних процесів, що особливо важливо для комплексів ТЗІ. Базисна система

$\{\varphi_i(t)\}$ функцій утворюється при виконанні наступних операцій (рис. 2):

- із випадкового (небезпечного) сигналу $x(t)$ виділяються екстремуми та після вимірювання їх амплітудно-часових значень обчислюються часові інтервали $\{\Delta t_i\}$ і знаки амплітудних перетворень $\{sgn \Delta x_i\}$;
- за значенням $\{\Delta t_i\}$, $\{sgn \Delta x_i\}$ формуються послідовності прямокутних імпульсів, кожна з яких i утворює $\varphi_i(t)$, при цьому тривалість кожного i -го імпульсу визначається значенням $\Delta t_i = t_{i+1} - t_i$;
- полярність імпульсу визначається знаком Δx_i , амплітуда – одиничною φ ;
- перша базисна функція $\varphi(t)$ формується з початкового масиву N екстремумів, подальші – після виключення парних (або непарних) екстремумів із попереднього масиву та виділення нових екстремумів.

Нехай $X_2(t)$, показаний на рис. 2, б є результатом синтезу 3-х синусних функцій (рис. 2, а). Отримавши екстремуми $X_3(t)$, які наведені на рис. 2, в, описаним способом формування дискретного стохастичного базису знаходимо $\varphi_1(t)$ (рис. 2, г).

На наступному етапі обробки, виключивши з початкового масиву парні екстремуми, отримаємо нові вибірки сигналу $X_3(t)$. Після представлення нових екстремумів формується $\varphi_2(t)$, потім – повторення аналогічних операцій – $\varphi_3(t)$ (рис. 2, д, е).

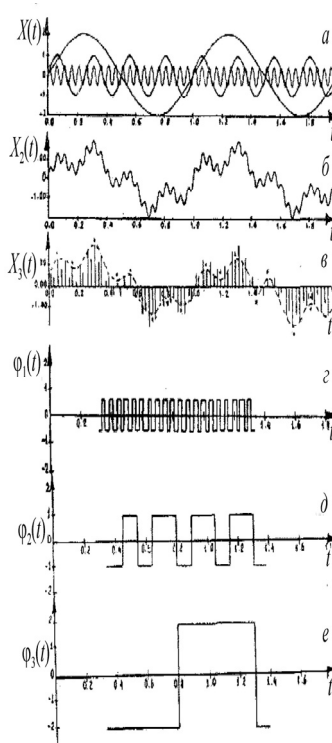


Рис. 2. Формування базисної системи функцій $\{\varphi_c(t)\}$

У загальному випадку повторення операцій продовжується до тих пір поки не буде вичерпаним весь масив проріджуваних дискрет.

Таким чином показано, що удосконалені методи спрощують математичний апарат обчислення небезпечних сигналів та скорочують час їх обробки комплексами ТЗІ.

У четвертому розділі «*Оцінка показників ефективності комплексів ТЗІ*» проведені дослідження ефективності функціонування комплексу ТЗІ, змодельованого за рахунок розроблених та удосконалених методів у дисертаційній роботі.

Для рішення поставленої задачі проведена апробація процедури періодичного радіоконтролю комплексу ТЗІ в автоматичному і ручному режимах на прикладі спеціального програмного забезпечення СМО-Д5.

За результатами науково-дослідної роботи «Безпека 07П» побудовані порівняльні графіки залежності ймовірності виявлення небезпечних сигналів від часу змодельованого та існуючих комплексів ТЗІ (рис. 3, 4) при заданій продуктивності ($\nu = 1500$ МГц) у діапазонах пошуку:

- 1) $\Delta F = 300$ МГц; 3) $\Delta F = 2000$ МГц;
 2) $\Delta F = 900$ МГц; 4) $\Delta F = 3000$ МГц,

де --- $P_{\text{виявл.}}$ змодельованого комплексу ТЗІ;
 --- $P_{\text{виявл.}}$ існуючого комплексу ТЗІ.

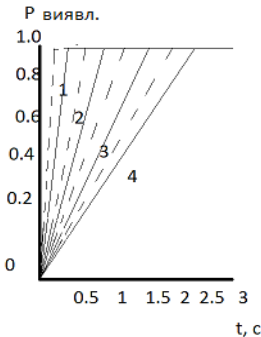


Рис. 3. Залежність ймовірності виявлення ($P_{\text{виявл.}}$) багаточастотного сигналу від часу (t)

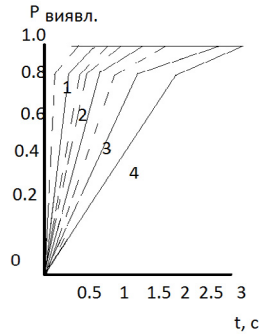


Рис. 4. Залежність ймовірності виявлення ($P_{\text{виявл.}}$) сигналу ППРЧ від часу (t)

Також, у результаті впровадження розроблених методів моделювання фізичних процесів (полів) виявлення небезпечних сигналів у другій частині, удосконалення прискорених методів їх обробки у третій частині, та узагальнюючих результатів за рахунок вирішення задач дослідження ефективності функціонування таких засобів у четвертій частині дисертаційної роботи в рамках науково-дослідної роботи «Безпека - 07П» зі всієї множини параметрів, що характеризують функціональні особливості комплексів ТЗІ, були вибрані та розраховані 20 параметрів, що найбільшою мірою впливають на їх ефективність.

Для проведення порівняльного аналізу якості пошукових засобів існуючих комплексів ТЗІ з комплексом, який був змодельований на базі наших досліджень, були відібрані 5 часто використовуваних на практиці комплексів ТЗІ: Астра В (Україна), АКОР (Україна), Дельта (Росія), RS-1000/8 (Німеччина-Японія), Крона 6Н (Росія). Результати дослідження представлені в табл. 1.

Таблиця 1

Показники ефективності	З _{мод.} * К.ТЗІ	Астра В	АКОР	RS- 1000/8	Дельта	Крона 6Н
1. Час виявлення небезпечного сигналу (НС), сек.	до 7	до 10	до 30	до 30	до 40	до 20
2. Точність вимірювання часових характеристик НС, мк/сек.	± 0,01	± 0,01	± 0,01	± 0,01	± 0,03	± 0,04
3. Час виявлення НС без адапт. комплексу до радіофіру, Мсек.	10	15	20	25	30	3
4. Час виявлення НС після адаптації комплексу до радіофіру, Мсек	0,7	1	1	2	3,5	3

5. Радіус контрольованої зони виявлення НС, м	250	200	50	150	50	100
6. Точність визначення місцеположення НС, м	$\pm 0,1$	$\pm 0,1$	$\pm 0,2$	$\pm 0,5$	$\pm 0,5$	$\pm 0,7$
7. Точність виявлення НС від швидкості обробки	92 %	92 %	80 %	80 %	75 %	75 %
8. Паке́т програмного забезпечення	власна розробка	власна розробка	власна розробка	стандарт	стандарт	стандарт
9. Приймальний пристрій	Будь-який	Аналізатор спектру НР-18	AR-5000	IC-8500	AR-3000A	AR-3000A
10. Кількість обсягів контролю	до 24	до 28	до 16	до 16	до 12	до 16
11. Швидкість сканування част. каналів, МГц/сек**	50	50	50	50	75	75
12. Крок перенастроювання, КГц	7,5	10	15	10	15	15
13. Точність визначення НС КГц	± 5	± 7	± 7	± 7	± 10	± 10
14. Точність вимірювання спектр. характеристик НС, КГц	± 10	± 15	± 20	± 15	± 25	± 25
15. Зручність застосування	+	+	+	+	+	+
16. Середовище функціонування (Windows)	+	+	+	+	+	+
17. Комплекс вимірювальних антен	+	+	+	+	+	+
18. Вид модуляції (АМ, ФМ, ЧМ,ОФМ, ДЧМ, ДОФМ, КАФМ,АФМ)	+	+	+	+	+	+
19. Вид імпульсної модуляції (АИМ, ФИМ, ШИМ,КИМ)	+	+	+	+	-	-
20. Наявність засобів ОТ	+	+	+	+	+	+

* Стендові (ідеальні) умови, ** У залежності від типу ЕОМ.

З аналізу даної таблиці випливає, що 7 показників ефективності змодельованого комплексу ТЗІ перевищують аналогічні показники розглянутих комплексів, інші 13 співпадають з показниками поширених зразків.

ВИСНОВКИ

У дисертації розв'язано актуальну наукову задачу – розроблені та удосконалені методи підвищення ефективності функціонування комплексів ТЗІ. При цьому отримано такі наукові та практичні результати:

1. Розроблені методи моделювання фізичних процесів (полів), які використовують одновимірні зміщенні диференціальні перетворення нелінійних крайових задач з лінійними та нелінійними граничними умовами для рішення задач виявлення небезпечних сигналів комплексами ТЗІ за заданий час у межах припустимої похибки; методи не мають методологічної похибки відо-

браження математичної моделі фізичного процесу в область відображень, вони простіші системо-аналогового методу, заснованого на двовимірних диференціальних перетвореннях, що значно розширює клас вирішуваних задач, а отже і можливості комплексів ТЗІ;

2. Розроблено метод балансу диференційних спектрів, запропонований для моделювання фізичних процесів, який зводить граничну задачу для рівнянь в частинних похідних до більш простої задачі інтегрування системи звичайних диференціальних рівнянь, розв'язаної одновимірними зміщеними диференціальними перетвореннями, що при заданій похибці підвищує точність виявлення небезпечного сигналу при його обробці комплексами ТЗІ.

3. Удосконалено метод оцінки місцеположення джерела небезпечних сигналів, що дозволяє більш чітко визначити відстань від цих джерел до приймальних антен та збільшити радіус контрольованої зони у 1,25–2,5 разів у порівнянні з аналогічними показниками поширених у даний час комплексів ТЗІ.

4. Удосконалено прискорені методи аналізу небезпечних сигналів, що дозволило спростити та підвищити точність визначення небезпечного сигналу та вимірювання його спектральних характеристик у 1,4–2 рази, зменшити час обробки небезпечного сигналу у 1.2–1.6 разів.

Для проведення аналізу ефективності функціонування комплексів ТЗІ у рамках науково-дослідної роботи «Безпека – 07П» сформована сукупність параметрів функціонування комплексу ТЗІ, які суттєво впливають на ефективність його використання (20 параметрів) і для порівняння обрані найбільш використовувані в наш час комплекси: Астра В (Україна), АКОР (Україна), Дельта (Росія), RS-1000/8 (Німеччина-Японія), Крона 6Н (Росія). Побудована таблиця з 20 показників ефективності змодельованого комплексу ТЗІ та існуючих комплексів доводить, що 7 показників даного комплексу перевищують аналогічні показники розглянутих комплексів, а по 13 кількісних і якісних параметрах змодельований комплекс ТЗІ співпадає з існуючими зразками.

Отже, отримані результати дають підґрунтя для проектування більш бистродіючих та потужних комплексів ТЗІ, що підвищить ефективність їх функціонування при вирішенні задач захисту інформації шляхом виявлення, аналізу та обробки небезпечних сигналів у джерелах витoku інформації.

Результати досліджень реалізовані при обґрунтуванні принципів і шляхів удосконалення кількісних та якісних характеристик і параметрів комплексів ТЗІ у науково-дослідній роботі «Безпека – 07П» Навчально-наукового інституту захисту інформації Державного університету телекомунікацій (Акт реалізації № 77/391 від 26.06.2012 р.) та впроваджені при підготовці лабораторно-методичної бази «Технічні засоби охорони» в Інституті Управління державної охорони України Київського національного університету імені Тараса Шевченка (Акт реалізації № 3/11/3–210 від 18.10.2014 р.).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

У наукових фахових виданнях:

1. *Мазуренко Л. Н.* Модель анализа структурной живучести сложной технической системы. / Л. Н. Мазуренко, В. А. Хорошко, Я. Л. Шатило // Сучасна спеціальна техніка № 4, 2011. – С. 68–74.
2. *Хорошко В. А.* Выявление информационных сигналов / В. А. Хорошко, Я. Л. Шатило // Інформаційна безпека № 1(7), 2012. – С. 43–47.
3. *Хорошко В. А.* Определение свойств опасных сигналов / В. А. Хорошко, Я. Л. Шатило // Захист інформації № 2, 2012. – С. 5–9.
4. *Одіяненко О. В.* Выявления небезпечних сигналів при радіомониторингу / О. В. Одіяненко, В. О. Хорошко, Д. В. Чирков, Я. Л. Шатило // Сучасна спеціальна техніка № 2(29), 2012. – С. 19–26.
5. *Шатило Я. Л.* Цифровые методы обработки информационных сигналов при радиомониторинге / Я. Л. Шатило // Сучасний захист інформації, № 1, 2012. – С. 44–48.
6. *Шатило Я. Л.* Оцінка ефективності експлуатації систем радіомониторингу / Я. Л. Шатило // Сучасний захист інформації, № 2, 2012. – С. 53–57.
7. *Бриль В. М.* Программно-аппаратный комплекс мониторинга опасных сигналов / В. М. Бриль, Я. Л. Шатило // Захист інформації 2014 (спеціальний випуск). – С. 12–19.
8. *Хорошко В. А.* Ускоренный метод анализа опасных сигналов в радиомониторинге / В. А. Хорошко, Я. Л. Шатило // Інформаційна безпека № 2, 2013. – С. 170–177.

Тези наукових доповідей:

9. *Мороз Є. С.* Методи програмування для систем захисту інформації. / Є. С. Мороз, А. М. Чернышев, Я. Л. Шатило // Матеріали I-ої МНТК Захист інформації і безпека інформаційних систем, Львів, 2012. – С. 178.
10. *Чернышев А. Н.* Создание банка данных для систем мониторинга / А. Н. Чернышев, Я. Л. Шатило // Тези доповідей III МНПК Інформаційні технології та захист інформації, Харків, 2012. – С. 213.
11. *Шатило Я. Л.* Організація технічного обслуговування мережі передачі інформації / Я. Л. Шатило // Збірник матеріалів МНТК Інформаційні технології та безпека інформаційно-комунікаційних систем, Вінниця, 2012. – С. 290–291.
12. *Одіяненко Е. В.* Анализ надежности и живучести технических систем защиты информации / Е. В. Одіяненко, Я. Л. Шатило // Матеріали МНТК Інформаційні управляючі системи та технології, ІУСТ-Одеса, 2013. – С. 245–247.
13. *Шатило Я. Л.* Підвищення ефективності функціонування комплексів технічного захисту інформації / Я. Л. Шатило // Матеріали Міжвідомчої науково-практичної конференції «Інформаційна безпека у війсьній сфері. Сучасний стан та перспективи розвитку» Київ, 2015. – С. 197–201.

АНОТАЦІЯ

Шатило Я. Л. Методи підвищення ефективності функціонування комплексів технічного захисту інформації. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. Національний авіаційний університет, Київ, 2015.

Дисертацію присвячено дослідженню та розробці теоретичних основ підвищення ефективності функціонування комплексів технічного захисту інформації (ТЗІ). У роботі проаналізовано причини виникнення каналів витoku інформації та комплекси виявлення, аналізу і обробки небезпечних сигналів; запропоновані методи моделювання фізичних процесів і полів для виявлення небезпечних сигналів; удосконалено метод пошуку та виявлення місцеположення джерела несанкціонованого впливу за рахунок введення процедури оцінки його знаходження та виділення опорного каналу, що, у разі проведення декількох сеансів прийому, дозволяє розширити пошуковий радіус та підвищити точність пошуку місцезнаходження джерела небезпечного сигналу; прискорений метод аналізу небезпечних сигналів на основі визначення кореляційної функції при обробці небезпечного сигналу комплексами ТЗІ за рахунок використання адаптивної затримки сигналів, що на відміну від найбільш відомого мультиплікативного методу кореляційного аналізу визначення функції дозволяє скоротити час його обробки; прискорений метод аналізу небезпечних сигналів на основі виділення стохастичного базису дискретного аргументу при обробці небезпечного сигналу за рахунок представлення в функції послідовності її парних екстремумів, що дозволяє, на відміну від класичних методів, обробку нестационарних процесів та скорочення часу обробки небезпечного сигналу комплексами ТЗІ; для проведення порівняльного аналізу якості пошукових засобів існуючих комплексів ТЗІ з комплексом, який був змодельований на базі дисертаційних досліджень, побудовано таблицю, до якої було обрано 20 показників якості, що найбільше впливають на ефективність функціонування комплексів ТЗІ.

Ключові слова: інформаційна безпека, носії інформації, канали витoku, моделювання, небезпечні сигнали, фізичні процеси, комплекси технічного захисту інформації, ефективність комплексів технічного захисту інформації.

АННОТАЦИЯ

Шатило Я. Л. Методы повышения эффективности функционирования комплексов технической защиты информации. – На правах рукописи.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. Национальный авиационный университет, Киев, 2015.

Диссертация посвящена исследованию и разработке теоретических основ повышения эффективности комплексов технической защиты информации

(ТЗИ). В работе проанализированы причины возникновения каналов утечки информации и комплексов выявления, анализа и обработки опасных сигналов. Предложены новые методы моделирования физических процессов и полей для выявления опасных сигналов, которые используют одномерные смещенные дифференциальные преобразования нелинейных краевых задач с линейными и нелинейными граничными условиями для решения задач выявления опасных сигналов комплексами ТЗИ за заданное время в пределах допустимой погрешности. Методы не имеют методологической погрешности отображения математической модели физического процесса в область отображений, они проще системно-аналогового метода, основанного на двумерных дифференциальных преобразованиях, что значительно расширяет класс решаемых задач и, следовательно, возможности комплексов ТЗИ. Разработан метод баланса дифференциальных спектров, предложенный для моделирования физических процессов, который сводит краевую задачу для уравнений в частных производных к более простой задаче интегрирования системы обычных дифференциальных уравнений, решаемой одномерными смещенными дифференциальными преобразованиями. Это повышает точность выявления опасного сигнала, обрабатываемого комплексами ТЗИ. Усовершенствован метод оценки местоположения источника излучения опасных сигналов, который позволяет более четко определить расстояние от неизвестных источников излучения опасных сигналов до приемных антенн и увеличить радиус контролируемой зоны в 1,25–2,5 раза по сравнению с аналогичными показателями часто используемых в настоящее время комплексов ТЗИ. Усовершенствованы ускоренные методы анализа опасных сигналов, что позволило упростить и повысить точность определения опасного сигнала и измерения его спектральных характеристик в 1,4–2 раза, уменьшить время обработки опасного сигнала в 1,2–1,6 раза. Разработана методика оценки эффективности комплексов ТЗИ. Для проведения сравнительного анализа качества поисковых средств существующих комплексов ТЗИ с комплексом, который был смоделирован на базе диссертационных исследований, построена таблица, для которой были отобраны 20 показателей качества, оказывающих наибольшее влияние на эффективность функционирования комплекса ТЗИ и 5 чаще всего используемых на практике комплексов ТЗИ. Анализ этой таблицы показал, что 7 показателей смоделированного комплекса превышают аналогичные показатели рассматриваемых комплексов, а по 13 количественным и качественным параметрам смоделированный комплекс ТЗИ совпадает с существующими образцами.

Полученные результаты дают основания для проектирования более быстрых и мощных комплексов ТЗИ, что повысит эффективность их функционирования при решении задач защиты информации за счет использования новых и усовершенствования существующих методов выявле-

ния, анализа и обработки опасных сигналов, возникающих в каналах утечки информации.

Ключевые слова: информационная безопасность, носители информации, каналы утечки, моделирование, опасные сигналы, физические процессы, комплексы технической защиты информации, эффективность комплексов технической защиты информации.

ABSTRACT

Shatylo Y. L. Methods of Efficiency Improvement of Technical Information Security Complex Functioning. – Manuscript Rights.

Ph.D. Thesis in Engineering Science with a degree in 05.13.21 – Information Security System. National Aviation University, Kyiv, 2015

Thesis work is dedicated to research and development of theoretical foundations in efficiency improvement of technical information security (TIS) complex functioning. This paper analyses the causes of information leakage channels and systems of identification, analysis and processing of compromising signals; methods of modeling physical processes and fields to identify the compromising signals were proposed; search-and-discover approach of the non-authorized source impact was improved by introducing the evaluation procedure of its location and extraction of reference channel, which in case of some reception sessions performance allows to expand the searching radius and improve the search accuracy of the compromising signal source location; accelerated analysis method of compromising signals based on correlation function recognition while processing the compromising signal by means of TIS complexes at the expense of adaptive signal delay application as opposed to the best known multiplying method of function definition correlation analysis allows to shorten time of its processing; accelerated analysis method of compromising signals based on the stochastic basis assignment of discrete argument while processing compromising signal at the expense of the representation as a sequence function of its pair extreme values, as opposed to the classic methods, enabling the processing of the non-steady processes and time shortening to process the compromising signal by means of TIS complexes; a table was formed, to which 20 quality factors have been selected influencing the most on the efficiency of TIS complex functioning, in order to perform the comparative analysis as to the quality of the search means of the existing TIS complexes with the complex being modeled on the base of thesis researches.

Keywords: information security, information media, leakage channels, compromising signals, physical processes, complexes of technical information protection, efficiency of technical information protection complexes.

Підп. до друку 13.10.2015. Формат 60x84/16. Папір офс.
Офс. друк. Ум. друк. арк. 1,16. Обл.-вид. арк. 1,25.
Тираж 100 пр. Замовлення № 174-1.

Видавець і виготівник
Національний авіаційний університет
03680. Київ – 58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002