ВІДГУК

офіційного опонента на дисертаційну роботу
ШАТИЛА ЯРОСЛАВА ЛЕОНІДОВИЧА
«Методи підвищення ефективності функціонування комплексів технічного захисту інформації»,
представлену на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми

Підвищення ефективності та надійності систем захисту інформації потребує впровадження та повноцінного використання можливостей комплексів технічного захисту, контролю ефіру та діагностики небезпечних сигналів. Необхідність підвищення рівня автоматизації процесів пошуку, виявлення та обробки сигналів диктується сучасними умовами глобалізації, яка поступово стає одним з визначальних факторів, що впливають на развиток як окремих галузей науки і техніки, так і пов'язаних із ними проблем захисту інформації на всіх рівнях. Враховуючи, що постійно зростають загрози несанкціонованого доступу до інформації, порушення її цілісності та конфіденційності, забезпечення захисту інформаційного ресурсу на сучасному етапі розвитку цивілізації стає найбільш пріоритетною задачею для більшості служб інформаційної безпеки державних установ, комерційних підприємств та організацій. Різні аспекти цього процесу набувають все більшої актуальності.

В наш час фактично стала законною деяка лібералізація використання радіочастотного спектру та ринку радіозасобів, що призвело до появи неконтрольованих пристроїв таємного отримання інформації та неліцензійованих засобів її передавання. Отже, на новому, якісному рівні постала проблема адекватного протистояння можливим загрозам під час проведення контролю радіообстановки, виявлення та локалізації потенційно небезпечних джерел радіовипромінювання. Вирішувати її можливо тільки методами, що дозволяють виконувати значний об'єм обчислень за обмежений час або в режимі онлайн. Виникає необхідність в адаптації відомих математичних методів або в розробці нових аналітичних і чисельно-аналітичних методів рішення складних крайових задач, що суттєво зменшують обчислювальну складність моделювання фізичних процесів з використанням ПЕОМ, а також теоретичних засад побудови комплексів технічного захисту інформації, що визначило актуальність теми досліджень.

Розширення функціональних можливостей систем захисту інформації на сучасному етапі інформатизації сфер людської діяльності вимагає розгляду питань захисту інформації від несанкціонованого доступу. Принциповим, при цьому є врахування особливостей досліджуваних інформаційних систем, до яких, зокрема, належать обмін інформацією в реальному часі та критичність показників надійності. Саме тому дисертаційна робота Шатила Я.Л., яка присвячена розробці методів підвищення ефективності функціонування комплексів технічного захисту інформації шляхом впровадження методів, запропонованих у дисертації, є ***актуальною*** і своєчасною.

2. Зв'язок дисертаційної 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 теоретико-методичні засади підвищення ефективності функціонування комплексів ТЗІ у задачах захисту інформації.

3. Оцінка змісту дисертації, її завершеності

Дисертація акуратно оформлена і складається зі вступу, чотирьох розділів, загальних висновків, списку літератури з 105 найменувань на 9 сторінках, 4 додатків загальним обсягом 25 сторінки.

Загальний обсяг дисертації становить 177 сторінок, у тому числі 141 сторінки основного тексту.

У вступі обґрунтовано актуальність теми, сформульовано мету і задачі досліджень, викладено наукову новизну і практичну цінність одержаних результатів, наведено дані про публікації та апробацію матеріалів дисертації.

У *першому розділі* проаналізовано можливості існуючих комплексів ТЗІ у рішенні задач виявлення, систематизації та аналізу причин виникнення каналів несанкціонованого отримання інформації та обробки небезпечних сигналів. Показано, що прямі носії інформації породжують чисельні побічні носії, у результаті чого виникає можливість проникнення нелегітимних отримувачів інформації у систему інформаційного обміну.

Для рішення задач захисту побудована модель цифрової системи моніторингу ефіру, яка включає виявлення, передачу, прийом і обробку інформації технічними засобами. Проаналізовані переваги та недоліки цифрової обробки сигналу, проведена класифікація комплексів ТЗІ за часом реалізації алгоритмів процедур обробки.

Другий розділ присвячено аналізу особливостей моделювання фізичних процесів і полів при виявленні небезпечних сигналів, розробці методів 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 для рішення задач виявлення небезпечних сигналів комплексами ТЗІ. Запропонований метод моделювання простіше відомого методу, заснованого на двовимірних диференціальних перетвореннях, він не містить методологічної похибки відображення математичної моделі фізичного процесу в область відображень.

Для рішення крайових задач з нелінійними граничними умовами запропоновано диференційні перетворення, які дозволяють розширити область застосування системоаналогового методу на нелінійні крайові задачі та виконувати моделювання за заданий час у межах припустимої похибки.

Вперше для моделювання фізичних процесів у комплексах ТЗІ запропоновано метод балансу диференціальних спектрів, який зводить крайову задачу для рівнянь в частинних похідних до більш простої задачі інтегрування системи звичайних диференціальних рівнянь.

У третьому розділі розроблено метод оцінки місцеположення джерела виникнення небезпечних сигналів та удосконалюються прискорені методи їх обробки у комплексах ТЗІ. Показано, що для підвищення точності визначення місцеположення джерела небезпечного сигналу доцільно проводити декілька сеансів прийому.

Для реалізації можливості виявлення малопотужних джерел в умовах складних перешкоджаючих радіообставин на контрольованому об'єкті розміщуються декілька антен, одна з яких використовується як «опорна» і розміщується на достатньому віддаленні від об'єкта. У роботі показано, що для квазіоптимального рішення можна обмежитись двома приймальними антенами, розміщеними у захищуваному приміщені та поза ним.

В дисертації набув удосконалення прискорений метод аналізу небезпечних сигналів у комплексах ТЗІ. Одним з найбільш розповсюджених методів обробки складних сигналів є кореляційний аналіз. В дисертації пропонується прискорений метод визначення кореляційної функції, заснований на використанні адаптивної затримки сигналів із заміною постійної величини часової дискретизації сигналу змінним кроком.

Запропонований удосконалений прискорений метод аналізу небезпечних сигналів, заснований на виділенні стохастичного базису дискретного аргумента при обробці небезпечного сигналу за рахунок представлення функції послідовністю ее парних екстремумів дозволяє обробку нестаціонарних процесів і скорочує час обробки небезпечного сигналу комплексами ТЗІ.

Таким чином показано, що запропоновані удосконалені методи спрощують математичний апарат виявлення небезпечних сигналів та скорочують час їх обробки у комплексах ТЗІ.

У четвертому розділі досліджено ефективність функціонування комплексу ТЗІ на моделі, побудованій у результаті впровадження розроблених методів моделювання фізичних процесів (полів) і виявлення небезпечних сигналів у другому розділі, удосконалення прискорених методів їх обробки у третьому розділі та узагальнення результатів вирішення окремих задач дослідження ефективності функціонування засобів захисту у четвертому розділі дисертаційної роботи в рамках науково-дослідної роботи «Безпека - 07П».

Із множини параметрів, що характеризують функціональні особливості комплексів ТЗІ, були вибрані та розраховані 20 параметрів, що найбільш впливають на ефективність комплексів. Для проведення порівняльного аналізу якості пошуко-вих засобів існуючих комплексів ТЗІ з комплексом, який був змодельований на базі дисертаційних досліджень, були відібрані 5 найбільш часто використовуваних на практиці комплексів ТЗІ. Детальний аналіз таблиці показників ефективності довів, що розроблений комплекс ТЗІ перевищує кращі з використовуваних в наш час комплекси. Використання отриманих результатів дослідження дозволить скоротити час і суттєво зменшити витрати на проектування і функціонування комплексів ТЗІ та значно підвищити їх

ефективність при вирішенні задач захисту інформації.

Текст дисертації викладено грамотною технічною мовою логічно, який має певну послідовність. Стиль викладання – доказовий.

4. Найбільш суттєві результати, які отимано у дисертації

1. Для рішення задач захисту інформації засобами ТЗІ запропоновано та обґрунтовано удосконалені методи моделювання фізичних процесів з використанням одномірних диференційних перетворень нелінійних крайових задач з лінійними та нелінійними граничними умовами, що є вкладом здобувача у теорію та практику функціонування ТЗІ;

2. Виконано моделювання процесу пошуку, виявлення, розпізнавання сигналу, встановлення його адекватності до певного класу сигналів, визначення ступеня небезпечності для інформаційної системи та об'єкта в цілому, удосконалено прискорений метод аналізу небезпечних сигналів у комплексі ТЗІ, що дозволяє дослідити шляхи підвищення показників надійності і ефективності та розширення функціональних можливостей систем захисту інформації;

3. Удосконалено метод оцінки місцеположення джерела небезпечного сигналу, який реалізовано у вигляді марковської структурно-автоматної моделі комплексу ТЗІ, що дозволяє вирішувати окремі науково-практичні задачі проектування та удосконалення систем захисту інформації;

4. Удосконалено метод оцінки передбачуваної ефективності комплексів ТЗІ, за допомогою якого можуть бути проведені розрахунки кількісної оцінки впливу факторів, які характеризують комплекс ТЗІ, на показник ефективності комплексу, що дозволяє здійснити вибір окремих підсистем комплексу, порівнюючи варіанти реалізації алгоритму поведінки комплексу при обмеженому часі виконання завдання.

5. Ступінь обґрунтоваиості наукових положень, висновків і рекомендацій дисертації, їх достовірність

Робота має чітку послідовність постановки задач та отриманих рішень, достатню доказову базу та аргументованість результатів. Використано сучасний математичний апарат для реалізації сформованої мети, як розвиток теоретичних основ і дослідження запропонованих рішень.

Вибрані здобувачем початкові передумови і рішення, представлені у вигляді математичних моделей, алгоритмів і структурних схем, не викликають сумнівів в коректності визначення, обґрунтованості висновків і рекомендацій.

Порівняльні оцінки запропонованих автором нових рішень щодо результатів, які отримані провідними вченими та дослідниками в області систем захисту інформації, достатньо аргументовані та відповідають списку приведених першоджерел.

Висновки та рекомендації, які сформульовані в дисертаційній роботі, враховують сутність та актуальність наукової задачі роботи, її мету та є значущими для розвитку систем захисту інформації. Представляється, що вони є придатними для практичного використання.

Достовірність наукових положень, висновків і рекомендацій, які приведені в дисертаційній роботі, обґрунтовані наступними положеннями:

- *передумови, які вибрані для постановки мети та вирішення задач дисертаційного дослідження, в достатній мірі аргументовані та виключають неоднозначні трактування;*
- *строгість, коректність та достовірність результатів, які наведені в дисертаційній роботі, базуються на використанні при дослідженнях сучасного математичного апарату і методів моделювання, які є адекватними виконаним розрахункам;*
- *методи та пропоновані рішення відповідають теоретичним положенням та практиці, які є базовими для дослідження систем захисту інформації, а також в достатній мірі корелюються з аналогічними теоретико-практичними роботами інших авторів;*
- *нові технології, а також пропоновані моделі та методи, які запропоновані в роботі, добре узгоджуються та не перечать існуючим стандартам в галузі інформаційної безпеки;*
- *науковими публікаціями здобувача основних результатів дисертаційного дослідження, його окремих матеріалів та сформульованих рекомендацій у фахових виданнях за переліками ВАК України;*
- *обговоренням результатів на семінарах, симпозіумах та конференціях різного рівня;*
- *актами впровадження отриманих результатів у науково-дослідні розробки та у виробництво.*

6. Оцінка висновків здобувача щодо значущості його праці для науки та практики

В дисертаційній роботі створено теоретичну та удосконалено практичну базу для проектування і удосконалення комплексів технічного захисту інформації, підвищення ефективності їх функціювання та надійності. Апробація матеріалів дисертації, а також впровадження результатів роботи доводять її значення для практики.

Нові наукові результати, отримані в дисертаційній роботі, складають підгрунтя для розробки:

- *методики моделювання процесів виявлення небезпечних сигналів у комплексах ТЗІ дискретним способом, що збільшує швидкість обробки і розширює можливості аналізу небезпечних сигналів;*
- *методики моделювання фізичних процесів, що дозволяє розширити область застосування аналітичнких моделей ТЗІ на задачі з нелінійними крайовими умовами;*
- *методики виділення антени комплексу, що має найбільший рівень сигналу, для підвищення точності визначення місцеположення джерела небезпечного сигналу;*
- *алгоритму пошуку каналів витоку інформації ТЗІ, коли в довільні моменти часу вимірюються параметри, що характеризують режим його використання;*
- *прискореного методу аналізу небезпечних сигналів комплексом ТЗІ, який за сво-єю швидкодією перевищує найбільш швидкі відомі класичні методи;*
- *методики побудови марківської структурно-автоматної моделі станів і переходів функціонування комплексу ТЗІ;*
- *методики вибору показників ефективності комплексів ТЗІ, що дозволяє скоротити час і зменшити витрати на проектування та функціонування комплексів за рахунок зменшення обсяги випробувань.*

У вступі, висновках до другого, третього та четвертого розділів дисертації здобувачем наведено дані щодо можливості застосування результатів дисертації, що дає підставу зробити висновок про її важливість для науки та практики при створенні та організації ефективного функціонування систем ТЗІ.

7. Повнота викладу результатів досліджень в опублікованих працях

Результати досліджень за темою дисертації викладені в 13 публікаціях в журналах і збірниках наукових праць та в матеріалах науково-технічних конференцій. У тому числі 8 статей у фахових наукових виданнях. Наведений перелік публікацій, їх зміст та обсяг відповідають темі дисертації, у повному обсязі відображають отримані положення, наукові результати та висновки, свідчать про їх новизну.

8. Можливі шляхи використання результатів дисертаційного дослідження

Отримані в дисертаційній роботі нові теоретичні положення можуть бути використані в наукових дослідженнях і навчальному процесі науково-педагогічним колективом Національного авіаційного університету та інших навчально-наукових організацій, галузь діяльності яких пов'язана з питаннями технічного захисту інформації, а також фахівцям в галузі інформаційної безпеки.

9. Ідентичність змісту автореферату основним положенням дисертації

Автореферат відповідає змісту та основним положенням дисертації.

10. Проблеми дискусійного характеру, недоліки та зауваження

До проблем дискусійного характеру, окремих недоліків та до зауважень, на мій погляд, слід віднести такі:

1). Аналіз матеріалів, які викладено у дисертаційному дослідженні, показав, що багато з них є достатньо вагоми для забезпечення безпеки інформаційних ресурсів як держави, так і об'єктів спеціального призначення та окремих суб'єктів господарювання. У цьому сенсі вважаю, що здобувачеві у підрозділі автореферату та дисертації, де мова йде про зв'язок роботи з науковими програмами, планами, темами, слід було б відзначити ті матеріали, які відносяться виконання положень Закону України «Про Концепцію Національної програми інформатизації» від 04 лютого 1998 р., № 75/98-ВР, «Концепції розвитку зв'язку України» від 09 грудня 1999 р., № 2238, до мети та завдань розділу 3, 4 та 6 «Концепції розвитку телекомунікацій в Україні», схваленої розпорядженням КМ України від 7 червня 2006 року.

Крім того, вважаю, що частину виконаних досліджень слід було б ідентифікувати з пунктами 1.2.5.4, 1.2.7.1 та 1.2.8.1 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009-2013 р.р.», які визначені постановою Президії НАН України від 25.02.2009 р., №55.

Вважаю, що доцільність виконаних наукових досліджень підтверджуються Розпорядженням Кабінету Міністрів України від 5 листопада 2014 року № 1135-р «Про затвердження плану заходів щодо захисту державних інформаційних ресурсів», що необхідно було б зазначити у відповідних висновках у авторефераті та дисертації.

2. *Розділ 1 містить достатньо великий обсяг оглядових матеріалів, які стосуються характеристик та інших відомостей, що відносяться до різноманітних носіїв інформації та до різноманітних технічних каналів її витоку. Вважаю, що достатньо велику частину результатів огляду можна було б сформувати у вигляді таблиць та винести їх у додатки. У тексті дисертаційної роботи доцільно було б обмежитись тільки оглядом радіоканалів витоку інформації, так як далі розглядаються небезпечні сигнали тільки таких каналів.*
3. *Вважаю, що дискусійним є питання щодо коректності формування наукової новизна відносно положень про «запропоновано вперше». Як на мій погляд, то слід було б чіткіше обґрунтувати особливості застосування відомих методів дослідження для вирішення задач виявлення небезпечних сигналів комплексами ТЗІ вказавши, що вони є лише засобами досліджень, тобто такими, наприклад, як перетворення Фур'є є засобом дослідження спектральних характеристик сигналів.*
4. *Вважаю, що при проведенні порівняльного аналізу існуючих методів аналізу небезпечних сигналів, який виконано у підрозділі 3.2, доцільним було б зробити посилання на піонерські роботи в цій області. Крім того, матеріали оглядового характеру на основі яких виконано аналіз, як правило, слід приводити у розділі 1.*
5. *При викладі принципів побудови алгоритму моделювання моделі удосконаленого комплексу ТЗІ, логіка автора, що розробляв алгоритм, не є прозорою. Вважаю, що з метою усунення цього недоліку, слід було б привести хоча б невелике обґрунтування стосовно використання структурно-автоматної моделі або хоча б короткий аналіз існуючих моделей.*
6. *Не зовсім вдалою є назва підрозділу 4.2 – «Оцінка передбачуваної ефективності використання комплексів ТЗІ». Як очікувалося, підрозділ повинен містити саме оцінку ефективності, але в ньому приводиться лише методика (опис) послідовності дій фахівців щодо роботи з комплексом.*
7. *У дисертації (та у авторефераті) здобувачем сформульовано завдання стосовно п'яти задач, рішення яких дозволяє досягти поставленої мети. Втім вважаю, що не зважаючи на очевидність їх актуальності, слід було б привести коротке обґрунтування зазначених в них проблем, враховуючи вимоги, що ставляться до комплексів ТЗІ та обслуговуючого персоналу.*
8. *У роботі зустрічаються термінологічні неточності, русизми та окремі стилістичні помилки, які не впливають на суть роботи.*

Зазначені зауваження не зменшують наукову цінність дисертаційної роботи та не впливають на отримані рішення та висновки. Більшість з них обумовлена новизною задачі, що розглядаються, необхідністю проведення міждисциплінарних досліджень та розгляду широкого кола питань. Їх можна розглядати як побажання звернути увагу автора на важливі аспекти розглянутої проблеми у його подальшій роботі.

Висновки

1. *Дисертаційна робота «Методи підвищення ефективності функціонування комплексів технічного захисту інформації» є науковим дослідженням на актуальну тему, яке самостійно виконав здобувач – Шатило Ярослав Леонідович.*
2. *В дисертаційній роботі отримано нові науково обґрунтовані результати, які вирішують науково-практичну задачу щодо проектування та удосконалення систем ТЗІ, підвищення показників надійності й ефективності та розширення функціональних можливостей систем ТЗІ, що в сукупності є значним досягненням для розвитку систем ТЗІ.*
3. *Новою суттю науково-прикладної задачі, яка вирішена у роботі, є створення методів підвищення ефективності функціонування комплексів технічного захисту інформації при її обробленні, збереженні та пересиланні.*
4. *Рішення науково-прикладної задачі, у порівнянні з існуючими теоретичними та практичними, методами, способами та алгоритмами, надає можливості значно удосконалити методи та засоби активного захисту інформації. Це дозволяє розширити теоретичні і практичні межі підвищення рівня реалізації функціональних послуг з забезпечення конфіденційності, цілісності та доступності інформації та інформаційних процесів.*
5. *Основні положення дисертації повно і об'єктивно викладені в авторефераті та публікаціях.*
6. *Дисертація відповідає п.п. 1, 2, 7 паспорту спеціальності 05.13.21 – «Системи захисту інформації» та може бути прийнята до захисту за нею.*
7. *Дисертація відповідає вимогам п.п. 9, 10, 11, 13 та 14 «Порядку присудження наукових ступенів і присвоєння вчених звань старшого наукового співробітника», затвердженого Постановою Кабінету Міністрів № 567 від 24 липня 2013 року, а її автор, Шатило Ярослав Леонідович, заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – «Системи захисту інформації».*

Офіційний опонент

завідувач кафедри інформаційних систем в економіці
Одеського національного економічного університету

доктор технічних наук зі спеціальності
05.13.21 – «Системи захисту інформації»

професор **О.О. Скопа**

Підпис: О.О. Скопа
Засвідчую:
Нач. відділу кадрів
20__ р.