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

Актуальність теми. Ефективності функціонування систем технічного захисту інформації (ТЗІ) та її надійності приділяється багато уваги в сучасному світі. Необхідність підвищення рівня автоматизації процесів керування системами ТЗІ вимагає реалізації удосконалення систем підтримки оперативного персоналу у прийнятті рішень щодо вибору засобів захисту на будь-якому етапі пошуку, виявлення та обробки небезпечних сигналів.

Розширення функціональних можливостей систем ТЗІ на сучасному етапі інформатизації всіх сфер людської діяльності вимагає розгляду питань захисту інформації від несанкціонованого доступу на новому рівні. Принциповим, при цьому є врахування особливостей систем ТЗІ, що досліджуються, до яких, зокрема, відносяться обмін інформацією в реальному часі та критичність показників надійності.

Поява множини неконтрольованих пристроїв прихованого зняття інформації та неліцензійних засобів її передавання призвела до необхідності створення й використання методів і засобів адекватної протидії можливим витокам конфіденційної інформації, а саме: виявлення і локалізації потенційно небезпечних джерел їх розповсюдження. Вирішити її відомими математичними методами, які потребують виконання значного обсягу обчислень за обмежений час, стає все більш проблематичним. Дисертаційна робота Шатила Я.Л. присвячена розробці нових аналітичних і чисельно-аналітичних методів розв'язання складних крайових задач, що суттєво зменшують обчислювальну складність моделювання фізичних процесів при виявленні небезпечних сигналів, а також удосконаленню прискорених методів аналізу та обробки небезпечних сигналів у комплексах ТЗІ. Тому тема дисертації є актуальною і своєчасною.

Зв'язок дисертаційної роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах розробки і впровадження науково-дослідної роботи "Безпека – 07П", яка виконувалась відповідно до Постанови Кабінету Міністрів України від 25.12.2005 року № 01086 у Навчально-науковому інституті захисту інформації Державного університету інформаційно-комунікаційних технологій. Автор у межах даної теми удосконалив теоретико-методичні принципи підвищення

ефективності функціонування комплексів ТЗІ для розв'язання задач захисту інформації.

Оцінка змісту дисертації, її завершеності. Дисертація оформлена у відповідності до вимог оформлення дисертаційних робіт, складається із вступу, чотирьох розділів, висновків до кожного розділу і загального висновку, списку літератури, який містить 105 найменувань на 9 сторінках, 4 додатків обсягом 27 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, а також результати впровадження.

У *першому розділі* проаналізовано сучасний стан проблем функціонування існуючих комплексів ТЗІ та їх можливості у розв'язанні задач виявлення, систематизації та аналізу причин виникнення каналів несанкціонованого отримання інформації і обробки небезпечних сигналів. Приведені причини виникнення можливостей несанкціонованого проникнення у систему інформаційного обміну в комплексах ТЗІ.

Для розв'язання задач захисту побудована модель цифрової системи моніторингу ефіру, яка включає виявлення, передачу, прийом і обробку інформації технічними засобами, виконано класифікацію комплексів ТЗІ за часом реалізації алгоритмів процедур обробки.

Виявлені недоліки існуючих рішень та обґрунтовано задачі досліджень.

Другий розділ містить аналіз особливостей моделювання фізичних процесів і полів для виявлення небезпечних сигналів та розробку нових методів моделювання цих процесів для розв'язання задач виявлення небезпечних сигналів комплексами ТЗІ. Вперше запропоновано метод моделювання фізичних процесів в комплексах ТЗІ з використанням одновимірних зміщених диференціальних перетворень нелінійних крайових задач виявлення небезпечних сигналів комплексами ТЗІ. Запропонований метод моделювання являється більш простим існуючого методу, заснованого на двовимірних диференціальних перетвореннях. Крім того, він не містить методологічної похибки при переведенні фізичного процесу в область відображень.

Для розв'язання крайових задач з нелінійними граничними умовами запропоновано використовувати диференційні перетворення, які дозволяють розширити область застосування системоаналогового методу на нелінійні крайові задачі та виконувати моделювання за заданий проміжок часу 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 удосконалено прискорені методи їх обробки у комплексах ТЗІ. Показано, що для підвищення точності визначення місцеположення джерела небезпечного сигналу доцільно проводити декілька сеансів приймання. А для виявлення малопотужних джерел в умовах складного радіооточення з перешкоджанням на контрольованому об’єкті доцільно розміщувати декілька антен, одна з яких використовується як "опорна" і розташовується на достатньому віддаленні від об’єкта. Для отримання прийнятного квазіоптимального рішення достатньо обмежитись двома приймальними антенами, які розміщуються у приміщені, що захищається та поза ним.

В дисертації удосконалено прискорений кореляційний метод аналізу небезпечних сигналів у комплексах ТЗІ. Запропоновано у прискореному методі визначення кореляційної функції, заснованому на використанні адаптивної затримки сигналів, замінити постійну величину часової дискретизації сигналу змінною.

Запропоновано прискорений метод аналізу небезпечних сигналів, заснований на виділенні стохастичного базису дискретного аргументу при обробці небезпечного сигналу. Цей метод удосконалено за рахунок представлення функції послідовністю її парних екстремумів, що 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.

Четвертий розділ присвячено дослідженню ефективності функціонування комплексу ТЗІ на моделі, яку побудовано як результат впровадження методів моделювання фізичних процесів (полів) і виявлення небезпечних сигналів, розроблених у другому розділі, удосконалення прискорених методів їх обробки у третьому розділі та узагальнення результатів розв'язання окремих задач дослідження ефективності функціонування засобів захисту, наведених у четвертому розділі дисертаційної роботи в рамках науково-дослідної роботи "Безпека - 07П".

Було відібрано 20 параметрів, які характеризують комплекси ТЗІ в процесі їх функціонування. Ці параметри найбільшим чином впливають на ефективність функціонування комплексів. Для проведення порівняльного аналізу якості пошукових засобів існуючих комплексів ТЗІ з комплексом, який був змодельований на базі дисертаційних досліджень, були відібрані п'ять найбільш часто використовуваних у практиці комплексів ТЗІ. Детальний аналіз таблиці показників ефективності довів, що

розроблений комплекс ТЗІ перевищує кращі з використовуваних в наш час комплекси ТЗІ. 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 логічно і послідовно, грамотною технічною мовою. Стиль викладання доказовий.

В цілому дисертація являється закінченою науковою роботою, що відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

Найбільш суттєві результати дисертації:

1. Розроблені методи моделювання фізичних процесів (полів) для розв'язання задач виявлення небезпечних сигналів комплексами ТЗІ за заданий проміжок часу у межах припустимої похибки, які використовують одновимірні зміщенні диференціальні перетворення нелінійних крайових задач з лінійними та нелінійними граничними умовами.

2. Удосконалено метод оцінки місцеположення джерела небезпечних сигналів, що дозволяє збільшити радіус контрольованої зони у 1,25–2,5 рази у порівнянні з аналогічними показниками поширених комплексів ТЗІ.

3. Удосконалені прискорені методи аналізу небезпечних сигналів дозволили спростити та підвищити точність визначення небезпечного сигналу, зменшити час на його обробку у 1,2–1,6 разів.

4. Удосконалено метод оцінки передбачуваної ефективності комплексів ТЗІ, за рахунок кількісної оцінки впливу факторів, які характеризують комплекс ТЗІ.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій дисертації, їх достовірність. Основні наукові положення, висновки та рекомендації дисертаційної роботи базуються на результатах аналізу властивостей систем ТЗІ. Проведені в дисертації перетворення, виявлені закономірності та встановлені залежності обґрунтовані відповідними законами математичних методів обробки сигналів, методів теорії ймовірностей, теорії диференціальних рівнянь та диференціальних перетворень, методів теорії графів, факторного та кореляційного аналізу, методів математичного моделювання, і тому, достовірність отриманих в дисертації теоретичних положень і наукових результатів не викликає сумніву.

Таким чином, основні наукові положення, висновки і рекомендації дисертаційної роботи обґрунтовані результатами математичного моделювання, широким обсягом публікацій і апробацій матеріалів дисертації, а також впровадженням результатів роботи.

Оцінка висновків здобувача щодо значущості його праці для науки й практики. Дисертаційна робота полягає у створенні теоретичної бази для

проектування і удосконалення систем захисту інформації та підвищення показників їх ефективності та надійності. Крім того для систем ТЗІ розроблено структурно-автоматну марківську модель функціонування комплексу ТЗІ з автоматичним вибором стратегії технічного обслуговування, що забезпечують заданий рівень надійності.

Нові наукові результати, отримані в дисертаційній роботі, складають підґрунтя 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 аналітичних моделей ТЗІ на задачі з нелінійними крайовими умовами;
- алгоритму пошуку каналів витоку інформації ТЗІ;
- прискореного методу аналізу небезпечних сигналів комплексом ТЗІ, що являється швидшим за 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 витрати на проектування та функціонування комплексів.

Наведені здобувачем обґрунтовані дані щодо можливості застосування результатів дисертації дають підставу зробити висновки про її важливість для науки й практики створення та удосконалення систем ТЗІ.

Повнота викладу результатів досліджень в опублікованих працях. Результати досліджень за темою дисертації викладені в 13 публікаціях у 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.

Можливі шляхи використання результатів дисертаційних досліджень. Отримані в дисертаційній роботі нові теоретичні положення доцільно використовувати в наукових дослідженнях і навчальному процесі науково-педагогічним колективом Національного авіаційного університету та інших навчально-наукових організацій, пов’язаних із дослідженням сучасних технічних систем захисту інформації та інформаційної безпеки взагалі.

Ідентичність змісту автореферату й основним положенням дисертації. Автореферат відповідає змісту та основним положенням дисертації.

Відповідність теми та змісту дисертації паспорту спеціальності, за якою вона подана на захист. Тема дисертації та її зміст відповідають формулі й галузі досліджень

паспорта спеціальності 05.13.21 - системи захисту інформації відповідно до вимог діючих стандартів.

Недоліки та зауваження по роботі.

1. На мою думку, перший розділ перенасичений інформацією, яка напряму не пов’язана з подальшими міркуваннями та дослідженнями. А саме: можливості комплексів ТЗІ; переваги та недоліки комплексів цифрової обробки сигналів; види радіоприймальних пристроїв тощо.

2. На мій погляд, не достатньо чітко обґрунтовано застосування методу одновимірних диференційних перетворень при рішенні задач виявлення і аналізу небезпечних сигналів.

3. На сторінці 94 наведено рис. 3.9 "Збільшений алгоритм виявлення каналів витоку інформації", а посилання на нього і опис в дисертації відсутні. Також на сторінці 96 наведено рис. 3.10 "Збільшений алгоритм виявлення каналів витоку інформації комплексом ТЗІ", а його докладний опис відсутній. Це дещо ускладнює розуміння принципу його роботи та його переваги у порівнянні з існуючими.

4. Назва підрозділу 4.2. не зовсім вдала. Очевидно цей матеріал слід було б назвати "Оцінка ефективності використання розроблених методів і моделей".

5. На мій погляд, в табл. 4.2 "Варіанти досліджень ефективності комплексу ТЗІ з урахуванням кваліфікації оператора" слід було б врахувати і середню кваліфікацію оператора. Оскільки практика показує, що більшість операторів мають середню кваліфікацію.

6. Не зовсім зрозуміло призначення і доцільність рис. 4.8 "Залежність ймовірності виконання завдання від вибору основного джерела інформації комплексу ТЗІ".

7. В рисунках дисертації зустрічається одночасне використання російської і української мов.

Перелічені недоліки не зменшують загального високого враження від дисертації та не впливають на кінцеві результати роботи. Більшість недоліків обумовлена новизною задачі, що розглядається, необхідністю проведення міждисциплінарних досліджень та розгляду широкого кола питань.

Висновки. Дисертація Шатила Ярослава Леонідовича "Методи підвищення ефективності функціонування комплексів технічного захисту інформації", є самостійною завершеною науковою роботою. В дисертації отримані нові науково обґрунтовані результати, які вирішують науково-практичну задачу підвищення ефективності систем технічного захисту інформації.

Матеріал дисертації викладено послідовно, стиль викладання доказовий, чіткий і лаконічний. Висновки до кожного розділу і дисертації в цілому тісно пов’язані з їх змістом і відображають суть виконаних досліджень. Публікації автора повністю

висвітлюють наукові положення і результати дисертації.

Таким чином дисертаційна робота відповідає вимогам пунктів 13, 14 "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого Постановою Кабінету Міністрів України № 567 від 24 липня 2013 р., а її автор, Шатило Ярослав Леонідович, заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації.

С.В. Зибін

Підпис доцента Зибіна С.В.

Офіційний опонент, кандидат технічних наук, доцент кафедри "Комп'ютерних систем і мереж" Державного університету телекомунікацій.