ВІДГУК

офіційного опонента
доктора технічних наук, професора кафедри комп'ютерних
систем, мереж та кібербезпеки Національного університету
біоресурсів і природокористування України
Лахна Валерія Анатолійовича
на дисертаційну роботу Кільдішева Віталія Йосиповича
«Моделі та методи захисту інформації на основі параметричного
перетворення передаваних сигнально-кодових конструкцій»,
подану на здобуття наукового ступеня
доктора технічних наук за спеціальністю
05.13.21 – системи захисту інформації

Аналіз дисертації Кільдішева В. Й. «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» дозволив сформулювати наступні узагальнені висновки щодо актуальності, ступеня обґрунтованості основних наукових положень, висновків, рекомендацій, достовірності, наукової новизни, практичного значення, а також загальної оцінки роботи.

Актуальність теми дисертаційного дослідження.

Інформаційно-комунікаційні системи та мережі використовуються сьогодні для забезпечення критично важливих процесів у державному управлінні, оборонній сфері, фінансових структурах, а також у повсякденному житті суспільства. Їхнє надійне функціонування є ключовою умовою інформаційної безпеки держави та стабільності цифрової інфраструктури.

Несанкціоноване втручання в роботу таких систем може призводити до витоку конфіденційних даних, порушення цілісності інформації та блокування доступу до важливих сервісів, що особливо небезпечно в умовах зростання кіберзагроз і радіоелектронного протиборства. Серед можливих загроз слід відзначити засоби радіоелектронної розвідки, методи перехоплення інформації, спотворення сигналів у каналах передавання, а також інструменти несанкціонованого доступу, які дедалі вдосконалюються й ускладнюють забезпечення належного рівня захисту інформації. Тому представляється досить актуальним розроблення та дослідження таких методів, які дозволяють інтегрувати шифрування, завадостійке кодування та спектральне розширення

сигналів у єдину систему багаторівневого захисту, що забезпечує одночасно конфіденційність, цілісність та прихованість передавання даних.

Отже, поставлена у дисертаційній роботі науково-прикладна задача розробки нових сигнально-кодових конструкцій і моделей їх функціонування в умовах дії сучасних загроз є надзвичайно актуальною і має важливе значення як для розвитку теорії захищеного зв'язку, так і для практичного впровадження ефективних технологій інформаційної безпеки.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційні дослідження проводилися в рамках науково-дослідних робіт Державного університеті інтелектуальних технологій і зв'язку за темами: «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0111U005680); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0111U007643); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0112U006815); «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0112U006814); «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0113U004750); «Ефективність систем інформаційної безпеки» (державний реєстраційний номер 0113U004749).

За структурою дисертація складається із анотації, вступу, шести розділів, висновків, списку використаних джерел та двох додатків. Матеріали роботи викладено на 340 сторінках, із них 291 − основного тексту з 65 рисунками та 36 таблицями, список використаних джерел нараховує 154 найменувань на 19 сторінках, 8 сторінок додатків.

До основних нових наукових результатів, які одержані в дисертаційній роботі, можна віднести:

1. Поглиблено теоретичні засади формування шумоподібних сигналів шляхом удосконалення методів розширення спектра непозиційних сигнально-кодових конструкцій, що забезпечило можливість визначення оптимальних параметрів таймерних сигналів для підвищення енергетичної ефективності та прихованості передачі інформації.

2. Розроблено концепцію багаторівневого захисту інформації, у якій статистичне шифрування, завадостійке та таймерне кодування розглядаються як взаємопов'язані елементи єдиної моделі безпеки, що дозволяє забезпечити

адаптивний баланс між швидкодією системи, завадостійкістю та структурною прихованістю.

3. Запропоновано новий підхід до параметричного синтезу таймерних сигналів, який враховує статистичні властивості імпульсів, часові варіації та вплив співвідношення сигнал/шум у каналі, що дало змогу побудувати модель керованого вибору параметрів *m*, *s* та *i*.

4. Удосконалено математичний апарат моделювання процесів розширення спектра, який дозволяє враховувати вплив непозиційності елементів сигналу на його спектральні характеристики та оцінювати ступінь структурної прихованості на основі коефіцієнта кореляційної видимості.

5. Обґрунтовано ефективність комбінованого методу розширення спектра таймерних сигналів, у якому реалізується синтез ПРС-ПВП та ППРЧ. Такий підхід забезпечує підвищення рівня структурної прихованості та криптостійкості системи передачі даних.

6. Розроблено вдосконалені алгоритми кореляційного прийому широкосмугових таймерних сигналів, у яких враховано часову структуру та непозиційний характер сигнальних конструкцій, що підвищує точність і достовірність виявлення сигналів у зашумлених каналах зв'язку.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації.

Обґрунтованість отриманих результатів підтверджується співпадінням результатів, що отримані аналітичними методами, із даними імітаційно-математичних моделей та експериментальними оцінками.

Достовірність результатів досліджень, висновків та рекомендацій підтверджується їх несуперечливістю відомим положенням криптології, теорії ймовірностей, відомим теоретичним та практичним результатам, співпадінням результатів статистичних випробувань та досліджень з теоретичними оцінками.

Повнота викладення наукових положень, висновків та рекомендацій в опублікованих працях.

Основні наукові результати дисертації опубліковані в 44 наукових роботах, зокрема: 1 монографія, 22 статті, з яких 20 статей у фахових наукових журналах, що входять до переліку МОН України, зокрема 1 стаття в журналі, який цитується в наукометричній базі даних Scopus та 1 стаття – у наукометричній базі даних Web of Science. Дві статті опубліковано в іноземних фахових виданнях, які цитуються в наукометричній базі даних Scopus.

21 публікація опубліковано в матеріалах міжнародних та всеукраїнських симпозіумів, науково-практичних та науково-технічних конференцій, з яких 5 наукових праць – у виданнях, які цитуються у наукометричній базі даних Scopus. Загальна кількість наукових праць у виданнях, які цитуються у наукометричних базах даних Scopus та Web of Science складає 9, з яких – 4 статті та 5 тез до конференцій.

Отже, кількість та якість наукових робіт здобувача з теми дисертації відповідають вимогам МОН України до дисертацій на здобуття наукового ступеня доктора технічних наук.

Оцінка мови та стилю викладання матеріалів дисертації та реферату.

Дисертація Кільдішева В. Й. написана з дотриманням прийнятої наукової термінології, стиль викладення матеріалу забезпечує доступність його сприйняття спеціалістом, а науковий рівень дисертації у цілому відповідає чинним вимогам до дисертацій на здобуття наукового ступеня доктора технічних наук.

Зміст реферату достатньо повно відображає основні положення, що викладені у дисертаційній роботі Кільдішева В. Й.

Вищевикладене дає змогу позитивно оцінити розглянуте дисертаційне дослідження Кільдішева В. Й., відзначити його наукову новизну, практичне значення, високий теоретичний рівень та відповідність вимогам до докторських дисертацій «Порядку присудження наукових ступенів». Але необхідно зазначити наявність у дисертації деяких дискусійних моментів та висловити наступні **зауваження**:

1. У першому розділі дисертації, де здійснено аналіз сучасних підходів до захисту інформації на основі підвищення завадозахищеності каналів зв'язку, доцільно було б глибше розкрити взаємозв'язок між критеріями енергетичної ефективності, структурної прихованості та завадостійкості. Більш системне узагальнення цих взаємозалежностей дозволило б чіткіше обґрунтувати вибір напрямів подальших теоретичних і прикладних досліджень.

2. У другому розділі дисертації обґрунтовано, що застосування таймерних сигналів дає змогу компенсувати надлишковість блокових кодів, суттєво знизити ймовірність помилкового приймання та майже вдвічі підвищити кодову швидкість. Водночас у роботі не простежується взаємозв'язок між

підвищенням завадостійкості системи та забезпеченням захисту інформації від несанкціонованого доступу, що є важливим для комплексної оцінки ефективності запропонованого підходу.

3. У третьому розділі (п. 3.4), попри обґрунтування впливу рівняння якості на завадостійкість та структурну прихованість таймерних сигналів, відсутній аналіз зміни рівня захисту інформації від несанкціонованого доступу за різних умов якості каналу зв'язку. Проведення такого аналізу дозволило б підвищити прикладну цінність отриманих результатів і забезпечити можливість адаптивного налаштування параметрів системи захисту відповідно до характеристик середовища передачі.

4. У четвертому розділі, в якому розглянуто багаторівневу модель захисту інформації, детально досліджено лише рівень статистичного шифрування. Водночас питання оцінювання криптостійкості завадостійкого, таймерного кодування та процедури декореляції помилок залишилися недостатньо розкритими. Розширення аналізу в цьому напрямі дало б змогу кількісно підтвердити ефективність інтегрованого підходу та обґрунтувати переваги запропонованої системної моделі захисту інформації.

5. У п'ятому розділі (п.п. 5.6.3 та 5.6.4) представлено результати дослідження якості та синтезу псевдовипадкових послідовностей із підвищеною криптографічною стійкістю. Проте отримані результати не були використані для подальшого розширення таймерних сигналів, що обмежує можливість підвищення показників структурної прихованості та завадостійкості системи. Залучення цих послідовностей до формування таймерних сигнальних конструкцій дозволило б підвищити рівень комплексного захисту інформації.

6. У пункті 6.2.2 дисертації лише частково подано аналіз впливу параметрів побудови таймерних сигналів (m, s, i) на автокореляційні функції та спектральні характеристики розширених сигнальних конструкцій на основі ПВП Уолша. Оскільки послідовності Уолша мають відому та детерміновану структуру, розширення спектра за допомогою таймерних сигналів призводить до її модифікації, що ускладнює кореляційне виявлення таких сигналів засобами радіоелектронної розвідки. Більш детальне дослідження взаємозв'язку

між параметрами таймерного сигналу та зміною спектральної щільності могло б глибше обґрунтувати отримані результати та дозволило б кількісно оцінити зниження кореляційної прихованості сигналу після розширення.

Загальна оцінка дисертаційної роботи.

Дисертація Кільдішева Віталія Йосиповича є структурованою, цілісною та завершеною науково-дослідною роботою, у якій розв'язано науково-технічну проблему підвищення захищеності передавання інформації на основі інтегрованих методів параметричного перетворення даних із використанням статистичного шифрування, таймерного кодування та методів розширення спектра сигналів. Зміст дисертації повністю відповідає спеціальності 05.13.21 – системи захисту інформації.

Оформлення дисертації та реферату в цілому відповідає чинним нормативним документам. Представлена дисертаційна робота відповідає вимогам, що висуваються до докторських дисертацій згідно "Порядку присудження наукових ступенів", затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а її автор, Кільдішев Віталій Йосипович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

ОФІЦІЙНИЙ ОПОНЕНТ
Професор кафедри комп'ютерних систем,
мереж та кібербезпеки
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, професор В.А. Лахно

Підпис Лахна В.А. засвідчую

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу кадрів
Підпис С.ГРИЩЕНКО