Витяг

з протоколу № 7 від 19 грудня 2024р.
засідання кафедри КБ та ТЗІ

Порядок денний:

Розгляд дисертаційної роботи Аль-Файюмі Халеда для отримання висновку про наукову новизну, теоретичне та практичне значення результатів на тему «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 Кібербезпека.

Присутні:

З кафедри КБ та ТЗІ:
професори: зав. каф.Корчинський В.В., Гаджиєв М.М., Василіу Є.В.
доценти:, Кірєєв І.А., Кільдішев В.Й., Стайкуца С.В., Онацький О.В., Кононович В.Г.
ст. викладачі: Басов В.Є., Рябуха О.М., Голев Д.В., Севастєєв Є.О., Лімарь І.В.
викладачі: Бєлова Ю.В., Гавель С.М., Сєдов К.С., Івахненко М.С., Шпильова М.І.

Головуючий - д.т.н., проф. Василіу Є.В.
Секретар - викл. Ю.В. Бєлова

СЛУХАЛИ: Аль-Файюмі Халеда з публічною презентацією дисертаційної роботи для отримання висновку про наукову новизну, теоретичне та практичне значення результатів на тему «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 Кібербезпека.

ВИСТУПИЛИ: д.т.н., проф. Василіу Є.В., к.т.н., доц. Онацький, д.т.н., проф. Гаджієв М.М., к.т.н., доц. Кільдішев В.Й., які зазначили актуальність вирішення наукового завдання, що пов’язано з розробкою моделей, методів та алгоритмів інтегрованого захисту інформації на основі різних механізмів перетворення даних, що включає процеси розширення спектра непозиційних сигналів, статистичного шифрування з поєднанням додаткових функцій завадостійкого кодування та декореляцією помилок.
Наукова новизна одержаних результатів полягає в наступному:
– подальший розвиток теорії динамічного хаосу для розробки нових систем захисту інформації;
– розробка нових інтегрованих методів захисту інформації, в яких поєднуються процеси шифрування, завадостійкого кодування та декореляції помилок;

– подальший розвиток теорії розширення спектра на основі непозиційних таймерних сигналів, що дало змогу розробити різні алгоритми формування шумоподібних сигналів на основі псевдовипадкового перескоку робочої частоти;
– запропонованований метод синтезу шумоподібних сигналів на основі розширення спектра таймерних сигналів за допомогою лінійної частотної модуляції, що дало змогу підвищити завадостійкість, енергетичну та структурну прихованість.
Науковий керівник д.т.н., проф. Корчинський В.В. відзначив, що здобувач Аль-Файюмі Халед, виконуючи дослідження під час навчання в аспірантурі, надав оцінку щодо сучасного стану проблематики, заявленої у дисертації. Зокрема було обрано об'єкти, матеріали та методи проведення досліджень, та сформульована актуальність теми, мета та задачі. Здобувач Аль-Файюмі Халед брав безпосередню участь під час постановки завдань, планування та виконання експериментів, обговорення результатів. Виявив себе відповідальною, наполегливою та старанною людиною.

УХВАЛИЛИ: прийняти наступний висновок про наукову новизну, теоретичне та практичне значення результатів дисертації.

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій»
(назва роботи)

здобувача наукового ступеня доктора філософії

Аль-Файюмі Халеда
(прізвище, ім'я, по батькові)

з галузі знань 12 – Інформаційні технології
(шифр, назва галузі знань)

за спеціальністю 125 Кібербезпека.
(*шифр, назва спеціальності)*

Публічна презентація проведена на кафедрі Кібербезпеки та технічного захисту інформаці
(назва)

«19» грудня 2024 року, протокол № 7 .

1. Актуальність теми дослідження обумовлена потребою у створенні й вивченні нових методів захисту інформації, заснованих на поєднанні позиційних, непозиційних та хаотичних сигналів, а також методів розширення спектра, що сприяють підвищенню рівня прихованості сигнально-кодових конструкцій під час передавання конфіденційних повідомлень.
В роботі обґрунтовується новий підхід до вирішення актуальної наукової проблеми захисту інформації, яка полягає в розробці й удосконаленні методів підвищення прихованості передавання інформації в інформаційно-комунікаційних системах шляхом інтеграції статистичного шифрування,

завадостійкого кодування, декореляції помилок та синтезу шумоподібних сигналів. Отримала подальший розвиток теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації. Отримано результати досліджень статистичних характеристик та варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей для використання їх в системах захисту інформації. Отримала подальший розвиток теорія синтезу шумоподібних сигналів, яка спрямована на розширення спектра непозиційних сигнально-кодових конструкцій, за допомогою яких можна змінювати структуру таймерних комбінацій та коригувальну здатність по виявленню та виправленню помилок.

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

Тематика дисертаційного дослідження відповідає вимогам та професійним компетентностям освітньо-наукової програми підготовки докторів філософії за спеціальністю 125 Кібербезпека Державного університету інтелектуальних технологій і зв’язку. Напрями дисертаційного дослідження тісно пов’язані з науково-технічними завданнями, визначеними Постановою Кабінету Міністрів України № 942 від 7 вересня 2011 року (з урахуванням змін, внесених Постановою КМ № 463 від 9 травня 2023 року) «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року». Зокрема, дослідження відповідає розділу «Інформаційні та комунікаційні технології», підрозділу «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека».

Тема роботи узгоджується з пріоритетними напрямами наукових досліджень Державного університету інтелектуальних технологій і зв’язку, зокрема: інформаційно-комунікаційні та радіоелектронні системи і технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони, а також системи захисту інформації від несанкціонованого доступу.

3. Наукова новизна отриманих результатів.

У дисертації вперше одержані такі нові наукові результати:

1. Надана оцінка варіативним можливостям дискретних генераторів хаосу у формуванні множини псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями. Це знайшло застосування у системах потокового шифрування, прямого розширення спектра таймерних сигналів, а також у системах маніпуляцій, де хаотичні коливання використовуються для маскування процесу передавання непозиційних цифрових комбінацій.
2. Запропоновано підвищення інформаційної прихованості завдяки інтегрованим методам перетворення даних, що поєднують статистичне шифрування, завадостійке кодування та декореляцію помилок. Це забезпечило можливість об'єднання процесів захисту інформації від несанкціонованого доступу та випадкових завад у єдину систему.
3. Вдосконалена теорія синтезу шумоподібних сигналів на основі непозиційних таймерних сигналів. Це забезпечило можливість гнучкого керування структурою шумоподібних сигналів таймерних комбінацій та покращення здатності до виявлення і виправлення помилок.
4. Вперше запропоновано метод синтезу шумоподібних сигналів, заснований на розширенні спектра непозиційних таймерних сигналів за

допомогою лінійної частотної модуляції. Це дозволило значно підвищити завадостійкість, а також енергетичну та структурну прихованість сигнальних конструкцій під час їх передавання.

4. Теоретичне та практичне значення результатів дисертації

Одержані результати забезпечують збільшення енергетичної та структурної прихованості сигнальних конструкцій шляхом застосування непозиційних таймерних сигналів для розширення спектра. Запропоновані методи розширення спектра відрізняються від існуючих, в яких використовуються позиційні розрядно-цифрові коди. Це сприяло розробці нових методів розширення та прийому непозиційних сигнальних конструкцій.

Результати досліджень генераторів хаосу дали змогу встановити, що незначні зміни їх параметрів дають можливість створювати безліч квазіортогональних послідовностей двійкових чисел, взаємний коефіцієнт кореляції яких знаходиться в межах $6{,}9*10^{-4}$ - $8{,}1*10^{-3}$.

Сумісне використання статистичного шифрування, ітеративного коду та декореляції помилок дало змогу поєднати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі зв'язку. Така інтеграція дозволяє на кожному кроці перетворення інформації підвищувати інформаційну прихованість та завадостійкость комбінацій шифрограм. Встановлено, що застосування декореляції помилок дозволяє зменшити кратність помилок у випадкових комбінаціях та використовувати режим виявлення помилок кратності $t_{\text{вияв}} = 2 \ldots 3$ в сполученні з виправленням помилок з кратністю $t_{\text{вип}} = 1$.

Синтез шумоподібних непозиційних таймерних сигналів на основі лінійної частотної модуляції дозволив встановити, що при застосуванні кореляційного прийому виділення фронтів таймерного сигналу при відношенні сигнал-завада на вході приймача $h = \frac{P_c}{P_i} = 0{,}25$. Енергетична прихованість забезпечується за умови, що шум перевищує корисний передаваний сигнал в 2-4 рази. Застосування таймерних сигналів дало змогу підвищити структурну прихованість у порівнянні з розрядно-цифровим кодом.

Отримані в роботі результати впроваджені в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, що підтверджується відповідним актом впровадження. Практична цінність роботи в тому, що отримані результати придатні для застосування в діяльності ТОВ «АЙСАЙБЕРО», що підтверджено відповідним актом впровадження основних результатів дослідження.

5. Використання результатів роботи

Результати дисертаційного дослідження мають практичне значення та можуть бути використані в різних сферах інформаційної безпеки, зокрема в системах захисту даних, криптографії, а також у технічних рішеннях для забезпечення захищеності сигнальних кодових конструкцій від виявлення та перехоплення засобами радіоелектронної розвідки.

1. Результати досліджень варіативних можливостей дискретних генераторів хаосу у формуванні множини псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями знайшла своє практичне застосування в системах потокового шифрування та прямого розширення

спектра таймерних сигналів. Ці результати також можуть використовуватися в системах маніпуляцій на основі хаотичних коливань.

2. Запропоновані методи підвищення інформаційної прихованості та завадостійкості на основі інтегрованих підходів, що поєднують статистичне шифрування, завадостійке кодування та декореляцію помилок, можуть бути застосовані у складних інформаційно-комунікаційних системах для захисту інформації від несанкціонованого доступу.

3. Вдосконалена теорія синтезу шумоподібних сигналів на основі непозиційних таймерних сигналів забезпечила можливість гнучкого керування структурою таймерних комбінацій. Це дозволяє підвищити прихованість та ефективність виявлення та виправлення помилок у сигнальних конструкціях, що є особливо важливим для систем зв'язку, що працюють в умовах радіоелектронної боротьби.

4. Запропонований метод синтезу шумоподібних сигналів на основі лінійної частотної модуляції дозволив досягти значного підвищення завадостійкості, а також енергетичної та структурної прихованості сигнальних конструкцій під час їх передавання. Цей метод може бути застосований у системах зв'язку спеціального призначення, де необхідна висока надійність та конфіденційність переданих даних.

Результати дослідження можуть бути використані в розробці сучасних систем захисту інформації, криптографічних протоколах, а також для підвищення ефективності систем управління інформаційною безпекою у державних і приватних установах.

6. Особиста участь автора в отриманні наукових та практичних результатів, що викладені в дисертаційній роботі.

Основні наукові та практичні результати дослідження отримані автором особисто. В дисертаційній роботі використані лише ті з результатів, що були опубліковані у наукових працях у співавторстві, які є індивідуальним внеском автора.

Основні положення та результати дисертаційної роботи отримані автором самостійно. Автор виконав усі теоретичні та практичні дослідження, що становить основу дисертаційної роботи. При цьому в роботах, що написані в співавторстві, здобувачу належить:

[1] – розробка алгоритму розширення спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції;

[2] – розробка алгоритму об’єднання літер, що близькі за показниками ймовірності появи в текстах в групи для завдання статистичного шифрування та аналіз результатів дослідження;

[3] – аналіз доцільності застосування непозиційних таймерних сигналів для підвищення структурної прихованості сигнальних конструкцій та аналіз результатів дослідження;

[4] – розробка алгоритму дослідження для завдання аналізу варіаційних можливостей програмних генераторів хаосу для формування числових послідовностей;

[5] – розробка алгоритму методу формування початкових параметрів програмних генераторів хаосу на основі перетворення хеш-функції символів пароля користувача криптографічної системи;

[6] – проведення експериментальної частини роботи, аналіз та обговорення результатів дослідження;
[7] – проведення експериментальної частини роботи, аналіз та обговорення результатів дослідження.

Дисертаційна робота виконана на кафедрі КБ та ТЗІ Державного університету інтелектуальних технологій і зв'язку
(назва кафедри (відділу), назва установи)
науковий керівник д.т.н.,проф., зав. каф. КБ та ТЗІ Корчинський В.В.
(науковий ступінь, вчене звання, посада, прізвище, ініціали)

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Аль-Файюмі Халеда
(прізвище, ініціали здобувача)
є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.
Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.
За результатами досліджень опубліковано 16 наукових праць, у тому числі 1 монографія, 6 статей у наукових фахових виданнях (з них 1 стаття у періодичних наукових виданнях України категорії «А» Scopus), 9 тез доповідей в збірниках матеріалів конференцій, у тому числі 2 тези доповіді у журналах, які цитуються у наукометричних базах даних Scopus.

Монографія
1. Сталий розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б.В. та ін. ; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. – Одеса : ДУ «ІРЕЕД НАНУ», 2024. – С. 543.

Статті у фахових виданнях, що входять до переліку, затвердженого МОН України

2. Volodymyr Korchynskyi, Valerii Hordiichuk, Vitalii Kildishev, Oleksandr Riabukha, Sergii Staikutsa, Khaled Alfaiomi. Method of information protection based on the integration of probabilistic encryption and noise immune coding. – *Radioelectronic and computer systems*, 2023.4.13, P.184-185. http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2023.4.13. (**SCOPUS**)
3. Корчинський В.В. Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів / Корчинський В.В., Назаренко О.А., Степанов В.О., Аль-Файюми Халед // Науковий журнал «*Інфокомунікаційні та комп'ютерні технології*» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». № 2 (02) 2022, – С.25-31.
https://www.viti.edu.ua/files/science/II_konf_2022/II_konf_2022_theses.pdf

4. Корчинський Володимир Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей / Корчинський Володимир, Рябуха Олександр, Аль-Файюмі ХАЛЕД, Гавель Сергій // Міжнародний науково-технічний журнал «*Вимірювальна та обчислювальна техніка в технологічних процесах*», 2023, № 1 – С. 180-186. https://vottp.khmnu.edu.ua/index.php/vottp/issue/view/9.

5. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// *Наукові праці ОНАЗ*. – Одеса: ОНАЗ, 2020. – № 2, – P. – 65-69.
https://ojs.onat.edu.ua/index.php/sbornik_onat/issue/view/84.

6. Корчинський В.В. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційними системах веб-сервісів / В.В. Корчинський, В.Й. Кільдішев, В.В. Онищук, Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2021, – С. 195-201.
https://ela.kpi.ua/server/api/core/bitstreams/69ad0866-c78c-47d3-a6d4-00369c3c478d/content.

7. Корчинський В.В. Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// *Наукові праці ОНАЗ ім. О. С. Попова* – Одеса: ОНАЗ, 2019, № 2. – С. 112-116.

Наукові праці, які засвідчують апробацію матеріалів дисертації

8. Volodymyr Korchynskyi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services / Valentyn Onyshchuk, Vitalii Kildishev, Volodymyr Korchynskyi and Khaled Alfaiomi // Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022 P. 331-334 (**SCOPUS**).

9. V. Hordiichuk, V. Korchynskyi, V. Kildishev, B. Molodetskyi, S. Staikutsa and K. Alfaiomi, "Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare," 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1-4, doi: 10.1109/TCSET64720.2024.10755658. (**SCOPUS**)

10. Корчинський, В., Мар'ян, М., Богданюк, І., & Аль-Файюмі Халед. (2024). Метод захисту інформації від несанкціонованого доступу на основі динамічного хаосу. Scientific Collection «InterConf», (194), 448–453.
https://archive.interconf.center/index.php/conference-proceeding/article/view/5775

11. Корчинський В.В. Методи застосування динамічного хаосу в системах захисту інформації / В.В. Корчинський, Халед Аль-Файюмі // Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. – К.: НУОУ, 2023. – С 81-83.

12. Корчинський В.В. Метод захисту інформації на основі

ймовірнісного шифрування / В.В. Корчинський, О.М. Рябуха, Х.О. Аль-Файюмі, А.Ю. Василенко // 78-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одесса, ДУІЗ, 21-22 листопада 2023 року. – С.154-156.

13. Корчинський В.В. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції /В.В. Корчинський Кільдішев В.И., Аль-Файюми Халед, Валігурський Ю.П // Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня – 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 31-33.

14. Корчинський В.В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції / Корчинський В.В., Рябуха О. М., Бердніков О.М., Аль-Файюми Халед, Поліщук К.В.// Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня – 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 27-30.

15. Корчинський В.В. Прогнозування та оцінки ризиків інсайдерських загроз / Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П. //«Перспективні напрями захисту інформації: Матеріали шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С.64-65.

16. Корчинський В.В. Мінімізація ризиків інсайдерських загроз в системах захисту /В.В. Корчинський, Аль-Файюми Халед // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. Ч.І., Одеса, 12-14 грудня. – 2019. – С. 139.

ВВАЖАТИ, що дисертаційна робота _____Аль-Файюмі Халеда_____
(прізвище, ініціали здобувача)

«Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій»,
(назва)

яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, та відповідає напрямку наукового дослідження освітньо-наукової програми Державного університету інтелектуальних технологій і зв'язку зі спеціальності _____125 Кібербезпека_____.
(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій»
назва роботи

подану Аль-Файюмі Халедом
прізвище, ім'я, по батькові

на здобуття ступеня доктора філософії, до захисту.

Запропонувати наступних опонентів як членів **разової спеціалізованої вченої ради** для захисту дисертації здобувача ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 Кібербезпека:

1. Рудницький Володимир Миколайович, доктор технічних наук, професор, головний науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки;
2. Фесенко Андрій Олексійович, кандидат технічних наук, доцент, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут».

Головуючий публічної презентації:

д.т.н., проф.
(науковий ступінь,
декан ф-ту ІТК
вчене звання, посада)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ Факультет інформаційних технологій та кібербезпеки 43997355 УКРАЇНА

Євген ВАСИЛЬЧУК
Ім'я ПРІЗВИЩЕ