Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003752

Особливі позначки: відкрита

Дата реєстрації: 30-12-2024

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Аль-Файюмі Халед --

2. Khaled Alfaiomi

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0003-4624-2569

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 28-02-2025

Спеціальність за освітою: Телекомунікації та радіотехніка

Місце роботи здобувача: Майкрософт

Код за ЄДРПОУ:

Місцезнаходження: Thames Valley Park, Reading, RG6 1WG, Сонинг, -, Велика Британія

Форма власності: Приватна/недержавна

Сфера управління:

Ідентифікатор ROR: 67890

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 7492

Повне найменування юридичної особи: Державний університет інтелектуальних технологій і зв'язку

Код за ЄДРПОУ: 43997335

Місцезнаходження: вул. Кузнечна, буд. 1, Одеса, 65023, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Державний університет інтелектуальних технологій і зв'язку

Код за ЄДРПОУ: 43997335

Місцезнаходження: вул. Кузнечна, буд. 1, Одеса, 65023, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 49.33.35, 50.37.23

Тема дисертації:

1. Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій

2. Methods for Improving Information Security Based on Concealed Transmission of Signal-Code Constructions

Реферат:

1. Об'єкт дослідження: процеси перетворення позиційних та непозиційних сигнальних конструкцій для забезпечення підвищення прихованості передавання інформації в інформаційно-комунікаційних системах. Предмет дослідження: ансамблі шумоподібних сигналів на основі методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів для збільшення прихованості сигнальних конструкцій. Методи дослідження. Для вирішення поставлених задач, визначення актуальності роботи та наукового завдання в дисертаційній роботі використано методи системного та порівняльного аналізу. При дослідженні варіаційних можливостей дискретних генераторів хаосу був використаний кореляційний аналіз та теорія ймовірності. При розробці методу захисту інформації на основі інтегрування статистичного шифрування, завадостійкого кодування та декореляції помилок було використано: теорія

ймовірності, теорія завадостійкого кодування, теорія прихованості та криптографії. При розробці методу синтезу шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінійної частотної модуляції було використано: теорія захисту інформації, теорія сигналів та завадостійкого кодування, а також методи статистичного й імітаційного моделювання. Наукова новизна одержаних результатів полягає в наступному: 1. Отримала подальший розвиток теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації, що дало змогу в результаті досліджень оцінити варіаційні можливості дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів, а також для систем маніпуляцій, в яких для маскування процесу передавання непозиційних цифрових комбінацій використовуються хаотичні коливання. 2. Отримав подальший розвиток методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Це дало змогу інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі. 3. 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. 4. Вперше запропоновано метод синтезу шумоподібних сигналів на основі розширення спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції, що дало змогу підвищити завадостійкість, енергетичну та структурну прихованості передавання сигнальних конструкцій. Практичне значення одержаних в дисертації результатів полягає в збільшенні енергетичної та структурної прихованості сигнальних конструкцій шляхом застосування хаотичних коливань в системах модуляції для передавання непозиційних таймерних сигналів та в системах потокового шифрування. Встановлено, що незначні зміни параметрів дискретного генератора дають можливість створювати квазіортогональні послідовності чисел, взаємний коефіцієнт кореляції складає в межах 6,9 10-4 - 8,1 10-3. Сумісне використання статистичного шифрування, завадостійкого кодування та декореляції помилок дало змогу поєднати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі зв'язку. При цьому на кожному кроці перетворення інформації відбувається зростання інформаційної прихованості та підвищення завадостійкості. Так застосування декореляції помилок дозволяють зменшити кратність помилок у кодових комбінаціях та використовувати режим виявлення помилок великої кратності твияв = 2 ... 3 в сполученні з виправленням помилок з кратністю твип = 1. Результати досліджень, виконаних в роботі, дозволили встановити наступне: можливість синтезу шумоподібних непозиційних таймерних сигналів на основі ЛЧМ; застосування кореляційного прийому для виділення фронтів ТСК при відношенні сигнал-завада на вході приймача ; забезпечення енергетичної прихованості, тобто можливість передавання за умови, що шум перевішує 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.

2. The subject of research: sets of noise-like signals based on methods of integrating timer coding processes, statistical encryption, and noise-like signal synthesis to increase the concealment of signal constructions. Research methods. To solve the tasks set in the dissertation, methods of systematic and comparative analysis were used to determine the relevance of the work and formulate the scientific problem. Correlation analysis and the theory of probabilistic analysis were applied when analyzing and studying the variation capabilities of discrete chaos generators. When developing the information protection method based on the combined use of statistical encryption, noise-resistant coding, and decorrelation, the theories of statistical modeling, noise-resistant coding, concealment, and cryptography were employed. The scientific novelty of the obtained results is as follows: 1. The

theory of dynamic chaos for information protection and confidential information transmission systems was further developed, allowing an assessment of the variation capabilities of discrete chaos generators for forming a multitude of pseudo-random sequences with specified mutual correlation properties. These sequences are applicable in stream encryption systems, direct spectrum expansion of timer signals, and manipulation systems where chaotic oscillations mask the transmission process of non-positional digital combinations. 2. The methods for enhancing information concealment and noise resistance in information transmission were further developed based on integrated data transformation methods: combining statistical encryption, noise-resistant coding, and error decorrelation. This allowed the integration of information protection processes against unauthorized access and accidental noise in communication channels. 3. The theory of noise-like signal synthesis was further developed to expand the spectrum of non-positional signal-code constructions, enabling modifications to timer combination structures and their error detection and correction capabilities. 4. A method for synthesizing noise-like signals based on spectrum expansion of non-positional timer signals using linear frequency modulation was proposed for the first time. This method improved the noise resistance, energy, and structural concealment of transmitted signal constructions. The practical significance of the dissertation results lies in increasing the energy and structural concealment of signal constructions through the application of chaotic oscillations in modulation systems for transmitting non-positional timer signals and in stream encryption systems. Minor parameter changes in the discrete generator enable the creation of quasi-orthogonal number sequences with mutual correlation coefficients ranging between 6,9 × 10п⁴ and 8,1 × 10п³. The combined use of statistical encryption, noise-resistant coding and error correction made it possible to combine the protection of information from unauthorised access and accidental interference in the communication channel into a single process. At each step of information transformation, information concealment and noise immunity increase. Thus, the use of error correction made it possible to reduce the error rate in code combinations and use the high error rate detection mode твияв = 2 ... 3 in combination with error correction with a multiplicity of твип = 1. The results of the research carried out in this work allowed us to establish the following: the possibility of synthesising noise-like non-positional timer signals based on the LFM; the use of correlation reception to isolate the TSC fronts at the signal-to-noise ratio at the input the receiver h=P_c/(P_i=0,25); ensuring energy concealment, i.e., the possibility of transmission provided that the noise outweighs the useful transmitted signal by a factor of 2-4. The use of timer signals made it possible to increase the structural concealment compared to the bit-digital code. The results obtained in the dissertation have been implemented in the educational process of the Department of Cybersecurity and Technical Information Protection at the State University of Intellectual Technologies and Telecommunications, as evidenced by the relevant act of implementation. The practical value of the work lies in the applicability of the obtained results for the engineering design of radio and telecommunication systems, confirmed by the act of implementing the main research results at the enterprise LLC "ICYBERO".

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 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.
- 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)
- 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
- 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.
- 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.
- 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.
- 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.
- 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).
- 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)
- 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
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація; аналітичні матеріали

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Корчинський Володимир Викторович

2. Volodymyr Korchynskyi

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3972-0585

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інтелектуальних технологій і зв'язку

Код за ЄДРПОУ: 43997335

Місцезнаходження: вул. Кузнечна, буд. 1, Одеса, 65023, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій Олексійович

2. Andriy Fesenko

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: 0000-0001-5154-5324

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Рудницький Володимир Миколайович

2. Volodymyr Rudnytskyi

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7362-3263

Додаткова інформація:

Повне найменування юридичної особи: Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

Код за ЄДРПОУ: 26614573

Місцезнаходження: вул. Стрілецька, буд. 1, Чернігів, Чернігівський р-н., 14033, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Онацький Олексій Віталійович

2. Oleksiy Onatskyi

Кваліфікація: к. т. н., доц., 05.12.13

Ідентифікатор ORCID ID: 0000-0002-7362-3263

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інтелектуальних технологій і зв'язку

Код за ЄДРПОУ: 43997335

Місцезнаходження: вул. Кузнечна, буд. 1, Одеса, 65023, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Гаджиєв Матін Магсуд-огли
2. Matin Hadzhyiev

Кваліфікація: д. т. н., професор, 05.12.13

Ідентифікатор ORCID ID: 0000-0001-7280-3863

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інтелектуальних технологій і зв'язку

Код за ЄДРПОУ: 43997335

Місцезнаходження: вул. Кузнечна, буд. 1, Одеса, 65023, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Василіу Євген Вікторович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Василіу Євген Вікторович
Відповідальний за підготовку облікових документів	Бєлова Юлія Володимирівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна