Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U000662

Особливі позначки: відкрита

Дата реєстрації: 26-01-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Цмоканич Іван Володимирович
2. Ivan Tsmokanych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

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:

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.861.001

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, 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 інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та алгоритми захисту інформації від високочастотного нав'язування
2. Methods and algorithms for protecting information from high-frequency interference.

Реферат:

1. АНОТАЦІЯ Цмоканич І.В. Методи та алгоритми захисту інформації від високочастотного нав'язування – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека». – Державний університет інформаційно-комунікаційних технологій Міністерства освіти і науки України, Київ, 2023. У дисертаційній роботі вирішується актуальне науково-технічне завдання щодо розробки методів та алгоритмів захисту інформації від високочастотного нав'язування. Для досягнення поставленої мети в роботі потрібно вирішити наступні окремі завдання дослідження: 1. Проаналізувати сучасний стан захищеності інформації від витоку каналами високочастотного нав'язування на обєктах інформаційної діяльності та критичної інфраструктури. 2. Дослідити сучасні методи та способи захисту інформації від витоку каналами високочастотного нав'язування. 3. Розробити модель блокування перехоплення інформації, яка забезпечує руйнацію

інформативних параметрів небезпечних сигналів, сформованих високочастотним нав’язуванням. 4. Розробити модель захисту інформації, яка забезпечує пошук оптимальних параметрів ефективних завадових захисних сигналів, здатних забезпечити руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування на основній частоті та комбінаційних гармоніках зондуючого сигналу. 5. Експериментально перевірити достовірність розроблених моделей та методу захисту інформації від витоку каналами високочастотного нав’язування. 6. Розробити модель розрахунку коефіцієнту захищеності інформації від небезпечних сигналів високочастотного нав’язування 7. Розробити методику захисту інформації від небезпечних сигналів високочастотного нав’язування. 8. Провести оцінку ефективності впливу захисних сигналів на небезпечні сигнали високочастотного нав’язування, в якій використано інформаційно-ентропійний критерій якості приймання радіосигналів. Об'єктом дослідження є процес захисту інформації від витоку каналами, утвореними методом високочастотного нав’язування. Предметом дослідження є методи та алгоритми захисту інформації від високочастотного нав’язування. Методи досліджень ґрунтуються на використанні теорії ймовірностей, параметричної ідентифікації систем, спектрального оцінювання, методів цифрової обробки сигналів, кореляційного аналізу, математичного аналізу, лінійної алгебри, математичного та комп'ютерного моделювання, а також теоретичних основ статистичної радіотехніки. Наукова новизна одержаних результатів. У процесі теоретичних і експериментальних досліджень та моделювання одержано наступні нові наукові результати: 1. Вперше запропоновано модель блокування процесу перехоплення інформації каналами високочастотного нав’язування, яка на основі процесу суперпозиції близьких по частоті гармонічних коливань дозволяє забезпечити ефект «биття» частот шляхом руйнування інформативних параметрів небезпечних сигналів і блокує витік інформації каналами високочастотного нав’язування. 2. Удосконалено модель захисту інформації від витоку каналами високочастотного нав’язування, яка, на відміну від існуючих, побудована на основі навмисного «качання» частоти і забезпечує руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках небезпечного зондуючого сигналу. 3. Удосконалено модель розрахунку коефіцієнта оцінки захищеності інформації, яка, на відміну від існуючих, побудована на основі порівняння енергетичних складових, виміряних в смугах, достатніх для перехоплення, небезпечних та захисних сигналів і забезпечує кількісну оцінку захищеності на основі встановленого значення коефіцієнта з врахуванням параметрів та значень небезпечного зондуючого сигналу. 4. Вперше розроблено метод захисту інформації від витоку каналами високочастотного нав’язування, який базується на основі алгоритму блокування та руйнування інформативних параметрів небезпечного сигналу високочастотного нав’язування, що забезпечує захист інформації по заданих значеннях коефіцієнта захищеності. Практичне значення одержаних результатів: Запропоновані моделі та методи можуть бути використані дослідно-конструкторськими організаціями та державними структурами при розробці та удосконаленні оцінки захищеності інформації під час проведення інструментального контролю різнотипних об’єктів інформаційної діяльності критичної інфраструктури та вирішення комплексних проблем щодо захисту інформації на об’єктах інформаційної діяльності критичної інфраструктури.

2. ABSTRACT Tsmokanych I.V. Methods and algorithms for protecting information from high-frequency interference - Qualifying scientific work on manuscript rights. Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 - "Cyber Security". - State University of Information and Communication Technologies of the Ministry of Education and Science of Ukraine, Kyiv, 2023. The thesis solves the current scientific and technical task of developing methods and algorithms for protecting information from high-frequency interference. In order to achieve the set goal in the work, it is necessary to solve the following separate research tasks: 1. To analyze the current state of information security against leakage through high-frequency interference channels on objects of information activity and critical infrastructure. 2. To study modern methods and ways of protecting information from leakage through channels of high-frequency imposition. 3. To develop a model of blocking the interception of information, which ensures the destruction of informative parameters of dangerous signals formed by high-frequency imposition. 4. To develop an information protection model that

ensures the search for optimal parameters of effective interference protective signals capable of destroying informative parameters of dangerous signals of high-frequency imposition on the fundamental frequency and combinational harmonics of the probing signal. 5. Experimentally verify the reliability of the developed models and the method of information protection against leakage through channels of high-frequency imposition. 6. Develop a model for calculating the information security factor against dangerous high-frequency interference signals 7. Develop a method of protecting information from dangerous high-frequency interference signals. 8. To evaluate the effectiveness of the impact of protective signals on dangerous signals of high-frequency interference, in which the information-entropy criterion of the quality of reception of radio signals is used. The object of the research is the process of protecting information from leakage through channels formed by the method of high-frequency imposition. The subject of research are methods and algorithms for protecting information from high-frequency imposition. Research methods are based on the use of probability theory, parametric identification of systems, spectral estimation, methods of digital signal processing, correlation analysis, mathematical analysis, linear algebra, mathematical and computer modeling, as well as theoretical foundations of statistical radio engineering. Scientific novelty of the obtained results. In the process of theoretical and experimental research and modeling, the following new scientific results were obtained: 1. For the first time, a model of blocking the process of interception of information by channels of high-frequency imposition is proposed, which, based on the process of superposition of harmonic oscillations close in frequency, allows to ensure the effect of "beating" frequencies by destroying the informative parameters of dangerous signals and blocks the leakage of information through channels of high-frequency imposition. 2. The model of information protection against leakage through high-frequency interference channels has been improved, which, unlike the existing ones, is built on the basis of intentional frequency "swinging" and ensures the destruction of the informative parameters of dangerous high-frequency interference signals not only on the main frequency, but also on combination harmonics of a dangerous probing signal. 3. The model for calculating the information security assessment coefficient has been improved, which, unlike the existing ones, is built on the basis of a comparison of the energy components measured in the bands sufficient for interception of dangerous and protective signals and provides a quantitative assessment of security based on the established value of the coefficient, taking into account the parameters and values of the dangerous probing signal. 4. For the first time, a method of protecting information from leakage through high-frequency jamming channels was developed, which is based on the algorithm of blocking and destroying informative parameters of a dangerous high-frequency jamming signal, which ensures information protection according to the given values of the security factor. Practical significance of the obtained results: The proposed models and methods can be used by research and development organizations and state structures in the development and improvement of information security assessment during the instrumental control of various objects of information activity of critical infrastructure and solving complex problems regarding information protection at objects of information activity of critical infrastructure.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

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

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Larysa Kriuchkova, & Ivan Tsmokanych. (2021). Overview of methods of protection of acoustic information against leaks by channels formed by highfrequency impositions. International Journal of Innovative

Technologies in Social Science, 3(31). https://doi.org/10.31435/rsglobal_ijitss/30092021/7685

- Крючкова, Л., Цмоканич І., Вовк. М. (2022). Удосконалений метод захисту конфіденційної інформації від перехоплення методами високочастотного нав'язування. Computer Systems and Information Technologies, 2021, № 3, с. 14–20. https://doi.org/10.31891/CSIT-2021-5-2.
- Крючкова, Л., & Цмоканич, І. (2022). Методичні аспекти визначення параметрів захисних впливів на зондувальні сигнали високочастотного нав'язування. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), с. 197–204. https://doi.org/10.28925/10.28925/2663-4023.2022.18.197204.
- Крючкова, Л., & Цмоканич, І. (2023). Удосконалення захисних впливів на небезпечні сигнали високочастотного нав'язування. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), с. 243–253. https://doi.org/10.28925/2663-4023.2023.19.243253.
- Larysa Kriuchkova, Maksym Vovk, Ivan Tsmokanych, and Denys Tarasenko. Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition, CEUR Workshop Proceedings CPITS-II-2 2021, pp. 265-272. (Scopus) https://ceur-ws.org/Vol-3188/short9.pdf.
- Larysa Kriuchkova, Ivan Tsmokanych, Svitlana Shevhenko, Oleksandr Bohdanov, and Nataliia Mazur. Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, CEUR Workshop Proceedings CPITS-II-2 2023, pp. 261-268. (Scopus) https://ceur-ws.org/Vol-3550/short10.pdf.
- Л.П. Крючкова, І.В. Цмоканич / Удосконалений метод захисту інформації від перехоплення методом високочастотного нав'язування // Науково-практична інтернет-конференція «Цифрова трансформація кібербезпеки». – Державний університет телекомунікацій. Навчально- науковий інститут захисту інформації, 2020. – С. 146 – 149. https://duikt.edu.ua/uploads/n_9126_17047934.pdf?file=n_9126_17047934.
- Л.П. Крючкова, І.В. Цмоканич / Удосконалений метод захисту інформації від витоку каналами високочастотного нав'язування// Комп'ютерні системи та мережні технології: XIII Міжнародна науково-практична конференція - Національний авіаційний університет.–Київ, 2021. – С. 62–63. https://er.nau.edu.ua/handle/NAU/50696;
- Л.П. Крючкова, І.В. Цмоканич / Захист інформації від високочастотного нав'язування на об'єктах критичної інфраструктури // IV Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)" – Київський національний університет імені Тараса Шевченка. – Київ, 2021. – С. 37 – 38.
- Л.П. Крючкова, І.В. Цмоканич // XII Всеукраїнська науково- практична конференція «Актуальні проблеми управління інформаційною безпекою держави» - Національна академія Служби безпеки України. – Київ, 2021. – С. 227 – 229.

Наукова (науково-технічна) продукція:

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. Крючкова Лариса Петрівна

2. Larisa P. Kryuchkova

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-8509-6659

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, 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. Наконечний Володимир Сергійович
2. VOLODYMYR NAKONECHNYI

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

Ідентифікатор ORCID ID: 0000-0002-0247-5400

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович
2. IVAN OPIRSKYI

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

Ідентифікатор ORCID ID: 0000-0002-8461-8996

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Макаренко Анатолій Олександрович
2. ANATOLII MAKARENKO

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-4081-328X

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Туровський Олександр Леонідович
2. OLEKSANDR TUROVSKYI

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

Ідентифікатор ORCID ID: 0000-0002-4961-0876

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Савченко Віталій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Савченко Віталій Анатолійович
Відповідальний за підготовку облікових документів	Вишнівський В.В.
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна