

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0222U003265

Державний реєстраційний номер: 0117U000328

Особливі позначки: відкрита

Дата реєстрації: 22-02-2022

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробити методи захисту інформації в телекомунікаційних та комп'ютерних системах засобами криптографії та стеганоаналізу аудіосигналів і зображень.

Початок етапу: 01.2017

Закінчення етапу: 12.2021

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, м. Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380445262008, 380445264178

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національна академія наук України

Код за ЄДРПОУ: 00019270

Місцезнаходження: вул. Володимирська, буд. 54, м. Київ, 01061, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442343243

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

Напрямок фінансування: 2.1 - фундаментальні дослідження

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6541030

Фактичний обсяг фінансування (тис. грн.): 5378.911

VII. Відомості про ДіР

Назва роботи українською:

Розробити методи захисту інформації в телекомунікаційних та комп'ютерних системах засобами криптографії та стеганоаналізу аудіосигналів і зображень

Назва роботи англійською:

Develop methods of information protection in telecommunication and computer systems by means of cryptography and steganalysis of audio and images

Реферат українською:

Розроблено протоколи функціонування програмного забезпечення серверної частини довіреного центра системи конфіденційного зв'язку з використанням ідентифікаційних даних користувачів. Розроблено бібліотеку базових криптографічних функцій для платформи Linux, інтерфейс якої відповідає вимогам міжнародного стандарту PKCS#11 «Cryptographic Token Interface Standard» та «Вимогам до інтерфейсів засобів криптографічного захисту інформації», наказ Міністерства юстиції України №2782/5/689. Запропоновано, теоретично обґрунтовано та досліджено нове вирішення актуальної науково-практичної проблеми контролю неправової стеганографічної передачі інформації в цифрових аудіосигналах та зображеннях найбільш поширених форматів: wav, mp3, bmp, png, tiff, jpeg.

Реферат англійською:

Protocols for the operation of the software of the server part of the trusted center of the confidential communication system with the use of user credentials have been developed. A library of basic cryptographic functions has been developed for the Linux platform, the interface of which meets the requirements of the international standard PKCS # 11 "Cryptographic Token Interface Standard" and "Requirements for interfaces of cryptographic information protection", order of the Ministry of Justice of Ukraine №2782 / 5/689. A new solution to the current scientific and practical problem of control of illegal steganographic transmission of information in digital audio signals and images of the most common formats: wav, mp3, bmp, png, tiff, jpeg is proposed, theoretically substantiated and investigated.

Індекс УДК: 002+02].002.5; 002:004.8; 002:004, 002:651.928(083.73)

Коди тематичних рубрик: 20.53

Керівники роботи

Власне Прізвище Ім'я По-батькові: Задірака Валерій Костянтинович

Науковий ступінь: д.ф.-м.н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

Власне Прізвище Ім'я По-батькові: Коваленко Ігор Миколайович

Науковий ступінь: д. б. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

Власне Прізвище Ім'я По-батькові: Кузнецов Микола Юрійович

Науковий ступінь: д. т. н.

Вчене звання: член-кор.

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Методи стеганоаналізу цифрових аудіосигналів і зображень найбільш поширених форматів (wav, mp3, bmp, png, tiff, jpeg)

Назва НТП англійською: Methods of digital audio signals and images steganoanalysis for the most common formats (wav, mp3, bmp, png, tiff, jpeg)

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Стеганографічний захист інформації

Реєстраційний номер картки технології:

Опис НТП: Запропоновано, теоретично обґрунтовано та досліджено нове вирішення актуальної науково-практичної проблеми контролю неправової стеганографічної передачі інформації в цифрових аудіосигналах та зображеннях.

Соціально-економічна спрямованість НТП: Створення конкурентноспроможних методик та засобів аналізу стеганосистем, для протидії неправовому використанню комп'ютерної стеганографії

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 11.2021

Закінчення етапу: 12.2021

Споживачі продукції:

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Програмний комплекс для стеганоаналізу та для тестування якості розроблених методів

Назва НТП англійською: Software for steganoanalysis and quality testing of the methods developed

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Програмні продукти

Галузь застосування: Стеганографічний захист інформації

Реєстраційний номер картки технології:

Опис НТП: Створено програмний комплекс, що зокрема реалізує метод на базі атаки контрольним вкрапленням, метод стеганоаналізу програми mp3stego, який її «зламає», методи Sample Pairs Analysis, Triples Analysis, методи з навчанням та класифікацією на основі моделей LIU, CHEN, CC-PEV, CC-CHEN, DCTR, GFR, CC-C300, а також SVM з лінійним та гаусівським ядрами і ансамблевим класифікатором на базі лінійного дискримінанту Фішера.

Соціально-економічна спрямованість НТП: Створення конкурентноспроможних методик та засобів аналізу стеганосистем, для протидії неправовому використанню комп'ютерної стеганографії

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 11.2021

Закінчення етапу: 12.2021

Споживачі продукції:

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Бібліотека базових криптографічних функцій для платформи Linux

Назва НТП англійською: A library of basic cryptographic functions has been developed for the Linux platform

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Програмні продукти

Галузь застосування: Криптографічний захист інформації

Реєстраційний номер картки технології:

Опис НТП: Створена бібліотека базових криптографічних функцій для платформи Linux дозволяє реалізацію криптографічних протоколів і побудову надійних систем захисту інформації, її інтерфейс відповідає міжнародним та вітчизняним вимогам.

Соціально-економічна спрямованість НТП: Створення конкурентноспроможних методик та засобів аналізу криптосистем; підготовка фахівців у галузі безпеки інформації.

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 11.2021

Закінчення етапу: 12.2021

Споживачі продукції:

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

Владислав Лещенко, Ніна Пекарчук, Михайло Савчук. Порівняльний аналіз складності методів лінеаризації та перебору розв'язання систем нелінійних булевих рівнянь. Захист інформації, 2020. Т.22, №1. С. 33-42.

Савчук М.М., Бурлака М.К. Кодування і класифікація перестановок за спеціальним перетворенням з оцінками потужності класів. Вісник Київського національного університету імені Тараса Шевченка. Серія фізико-математичні науки, 2019, №2. С. 35-42.

Савчук М.М., Фесенко А.В. Квантові обчислення: огляд та аналіз. Кібернетика та системний аналіз. 2019. №1. С. 14-29.

Koshkina N.V. Comparison of Efficiency of Statistical Models Used for Formation of Feature Vectors by JPEG Images Steganalysis. Theoretical and Applied Cybersecurity. 2020. №1 (2). Pp. 22 – 28.

Кошкіна Н.В. Дослідження основних компонентів систем JPEG-стеганоаналізу на базі машинного навчання. Захист інформації, 2020. Т. 22, №2. С. 97 – 108.

Кошкіна Н.В. Про вплив параметрів зображень у форматі JPEG на точність їх стеганоаналізу. Cybernetics and Computer Technologies. 2021. № 1. С. 74-85.

Кошкіна Н.В. Стеганоаналіз J-UNIWARD. Кібернетика і системний аналіз. 2021. №3 (57). С. 184 – 192.

Кошкіна Н.В. Про підвищення точності виявлення JPHIDE стеганограм. Фізико-математичне моделювання та інформаційні технології. 2021. №32. С. 170 – 174.

Х. Заключні відомості

Керівник юридичної особи

Сергієнко Іван Васильович

д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Кочубінський Анатолій Іванович

(к. ф.-м. н.)

Кошкіна Наталія Василівна

(д. т. н., 05.13.21)

Нікітіна Ольга Юріївна

(к. ф.-м. н.)

Савчук Михайло Миколайович

(д.ф.-м.н., 01.05.01)

Фаль Олексій Михайлович

(к. ф.-м. н., 01.01.05)

Шаталов Олександр Семенович

Швідченко Інна Віталіївна

(к. ф.-м. н., 01.05.01)

**Відповідальний за підготовку
облікових документів**

Хом'як О.М.

Телефон

+38 (096) 657-25-61

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**

