

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U001995

Державний реєстраційний номер: 0117U001346

Особливі позначки: відкрита

Дата реєстрації: 23-11-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка методів, алгоритмів та програмного забезпечення стеганографічного аналізу та ефективних за швидкодією базових асиметричних криптографічних перетворень

Початок етапу: 06.2016

Закінчення етапу: 11.2017

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:

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 526-02-88

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України

Код за ЄДРПОУ: 20001993

Місцезнаходження:

Форма власності:

Сфера управління: Служба безпеки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 422-75-58

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6521010

Фактичний обсяг фінансування (тис. грн.): 334
--

VII. Відомості про ДіР

Назва роботи українською:

Розробка методів, алгоритмів та програмного забезпечення стеганографічного аналізу та ефективних за швидкістю базових асиметричних криптографічних перетворень

Назва роботи англійською:

Development of methods, algorithms and software of steganography analysis and basic asymmetric cryptographic transformations which are effective on operation speed

Реферат українською:

Досліджено існуючі та створені нові математичні методи і алгоритми стеганографічного аналізу; досліджені можливості оптимізації та тестування якості запропонованих методів та алгоритмів стеганографічного аналізу; досліджено існуючі та створені нові ефективні за швидкістю та пам'яттю алгоритми реалізації базових асиметричних криптографічних перетворень для різних моделей обчислень; розроблено програмне забезпечення на основі створених методів стеганографічного аналізу та базових асиметричних криптографічних перетворень; протестована якість matlab-реалізації алгоритмів стеганоаналізу, зроблений аналіз практичної ефективності алгоритмів реалізації базових криптографічних перетворень для різних моделей обчислень.

Реферат англійською:

The existing and created new mathematical methods and algorithms of steganographic analysis are researched; the possibilities of optimization and testing of the quality of proposed methods and algorithms of steganographic analysis were investigated; existing and new algorithms for implementation of basic asymmetric cryptographic transformations for different computational models are created; the software was developed on the basis of the established methods of steganographic analysis and basic asymmetric cryptographic transformations; the quality of matlab-implementation of the algorithms of steganal analysis was tested, the analysis of the practical efficiency of algorithms for the implementation of basic cryptographic transformations for various computational models was made.

Індекс УДК: 654.1; 654.14; 654.15; 654.16; 654.17; 654.19; 656.8, 621.394/.396.019.3

Коди тематичних рубрик: 49.33.35

Керівники роботи

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

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Методи стеганографічного аналізу та ефективних за швидкістю базових асиметричних криптографічних перетворень

Назва НТП англійською: Methods of steganalysis and basic asymmetric cryptographic transformations which are effective on operation speed

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: Захист інформації

Реєстраційний номер картки технології:

Опис НТП: Математичні методи стеганографічного аналізу, ефективні за швидкістю та пам'яттю алгоритми реалізації базових асиметричних криптографічних перетворень для різних моделей обчислень

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2017

Закінчення етапу:

Споживачі продукції: Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

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:

IX. Бібліографічний опис

1. Терещенко А.Н., Задирака В.К. Оценка сложности операции умножения многоразрядных чисел в параллельной модели вычислений // Компьютерная математика. – 2016. – № 1. – С. 58-71. 2. Задирака В.К., Кошкіна Н.В., Швідченко І.В. Комп'ютерній стеганографії 20 років // Матеріали V міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем" (2-3 червня 2016 р.) – Львів, 2016. – С. 98-99. 3. Задирака В.К., Кудин А.М. Новые модели и методы определения стойкости систем защиты информации

Х. Заключні відомості

Керівник юридичної особи

Сергієнко Іван Васильович

д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Задірака В.К.

Кошкіна Н.В.

Нікітіна О.Ю.

Швідченко І.В.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

