

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U004812

Державний реєстраційний номер: 0112U000743

Особливі позначки: відкрита

Дата реєстрації: 06-03-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробити на основі нових теоретичних результатів методи захисту інформації в телекомунікаційних та комп'ютерних системах

Початок етапу: 01.2012

Закінчення етапу: 12.2016

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут кібернетики ім. В. М. Глушкова НАНУ

Код за ЄДРПОУ: 05417176

Місцезнаходження:

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 526-41-78, 526-74-18

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, 54, м. Київ, Київська обл., 01030, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442396594

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.): 4158

VII. Відомості про ДіР

Назва роботи українською:

Розробити на основі нових теоретичних результатів методи захисту інформації в телекомунікаційних та комп'ютерних системах

Назва роботи англійською:

To develop on the basis of new theoretical results methods of information security in telecommunication and computer systems

Реферат українською:

В роботі отримані фундаментальні результати, що впливають на швидкість криптоаналізу поточкових шифрів при їх застосуванні для захисту інформації в інформаційно-обчислювальних системах. Прикладні результати оформлені у вигляді пакетів програм, що дають можливість безпосередньо будувати системи захисту інформації за декларованими вимогами та ключові послідовності із заданими властивостями. Розроблено підходи до аналізу побудови та віднайдення стеганографічних контейнерів графічного та звукового інформаційного наповнення.

Реферат англійською:

We obtain fundamental results affecting the speed of stream cipher cryptanalysis in their application for information protection. Application results are designed in the form of software packages that make it possible to build information security system directly for the declared requirements and key sequences with desired properties. The approaches to the analysis of construction and finding steganographic container of graphic and audio content are developed.

Індекс УДК: 002, 002:651.928(083.73)

Коди тематичних рубрик: 20.01

Керівники роботи

Власне Прізвище Ім'я По-батькові: Коваленко Ігор Миколайович, Задірака Валерій Костянтинович,
Кузнєцов Микола Юрійович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Криптографічні протоколи автентифікації, різноманітні схеми цифрового підпису та спеціальні протоколи з використанням нових важкооборотних функцій. Методи вкраплення додаткової інформації в зображення, аудіо та відеосигнали, а також методика оцінки їх якості. Стеганоаналітичні методики виявлення прихованої інформації в графічних файлах.

Назва НТП англійською: Cryptographic authentication protocols, various schemes of the digital signature and special protocols using new functions. Methods blotches additional information in the image, audio and video signals and methods of assessing their quality. Steganographic methods of detecting hidden information in image files.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 72. Діяльність у сфері інформатизації

Реєстраційний номер картки технології:

Опис НТП: Розроблені системи застосування новітніх атак на системи захисту інформації, що використовують алгоритми потокового шифрування. Побудовані прикладні програми, що аналізують системи захисту інформації та сприяють побудові ключової інформації із заданими властивостями. Розроблені математичні методи аналізу побудови стеганографічних контейнерів для різного роду інформації.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: -

Закінчення етапу:

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:

ІХ. Бібліографічний опис

Х. Заключні відомості

Керівник юридичної особи

Сергієнко Іван Васильович

д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Кочубінський А.І.

Кошкіна Н.В.

Нікітіна О.Ю.

Савчук М.М.

Фаль О.М.

Шаталов О.С.

Швідченко І.В.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

