

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U000904

Державний реєстраційний номер: 0115U001573

Особливі позначки: відкрита

Дата реєстрації: 17-03-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробити методи аналізу потокових шифрів

Початок етапу: 05.2015

Закінчення етапу: 12.2016

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

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

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: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6541030

Фактичний обсяг фінансування (тис. грн.): 465
--

VII. Відомості про ДіР

Назва роботи українською:

Розробити методи аналізу поточкових шифрів

Назва роботи англійською:

To develop the methods stream ciphers

Реферат українською:

В роботі розглянуто методи аналізу поточкових шифрів та системи аналізу випадкових та псевдовипадкових послідовностей. Розроблено комплекси програм оцінки якостей систем захисту інформації та систем побудови ключової інформації.

Реферат англійською:

The methods of analysis of stream ciphers and systems analysis and pseudo-random sequences are considered. The software package of quality assessment of information protection systems is made.5481

Індекс УДК: 002:651, 002:651.928(083.73)

Коди тематичних рубрик: 20.53.31

Керівники роботи

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

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Методи аналізу поточкових шифрів

Назва НТП англійською: The methods stream ciphers

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 72.діяльність у сфері інформатизації. Системи захисту інформації

Реєстраційний номер картки технології:

Опис НТП: Розроблені системи оперативної оцінки якостей поточкових шифрів за допомогою застосування новітніх типів атак на зашифрованні тексти. Такі методи аналізу поточкових шифрів дають можливість на попередніх етапах їх дослідження виявити їх слабкості, які в подальшому приводять до розкриття розшифрованих текстів.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 2017-2020

Закінчення етапу:

Споживачі продукції: Міністерство оборони України, Служба Безпеки України, Служба спеціального зв'язку та захисту інформації, Міністерства іноземних справ 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

Х. Заключні відомості

Керівник юридичної особи

Сергієнко Іван Васильович

д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Кочубінський А.І.

Савчук М.М.

Фаль О.М.

Шаталов О.С.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

