

# Облікова картка ДіР



## I. Загальні відомості

**Державний обліковий номер:** 0211U008742

**Державний реєстраційний номер:** 0110U006728

**Особливі позначки:** відкрита

**Дата реєстрації:** 15-09-2011

## II. Етап виконання ДіР

**Номер етапу:** 2

**Назва етапу:** Дослідження застосування спеціальних сучасних математичних методів у криптоаналізі.  
Визначення початкових станів певних класів генераторів псевдовипадкових послідовностей

**Початок етапу:** 03.2011

**Закінчення етапу:** 04.2011

**Вид звітнього документа:** Остаточний звіт

## III. Відомості про виконавця ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки, молоді та спорту України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 406-81-76

## IV. Відомості про співвиконавців ДіР

## V. Відомості про замовника ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Служба зовнішньої розвідки України; військова частина К1410

**Код за ЄДРПОУ:** 33240845

**Місцезнаходження:** вул. Володимирська, 33, м. Київ, Київ, 01034, Україна

**Форма власності:**

**Сфера управління:** Служба безпеки України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 0442262124

## 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):** 6621010

|                                                    |
|----------------------------------------------------|
| <b>Фактичний обсяг фінансування (тис. грн.):</b> 0 |
|----------------------------------------------------|

## **VII. Відомості про ДіР**

### **Назва роботи українською:**

Дослідження застосування спеціальних сучасних математичних методів у криптоаналізі. Визначення початкових станів певних класів генераторів псевдовипадкових послідовностей.

### **Назва роботи англійською:**

Research of application of the special modern mathematical methods is in cryptoanalysis. Determination of the initial states of certain classes of generators of pseudorandom sequences»

### **Реферат українською:**

Проведено аналіз сучасних генераторів псевдовипадкових послідовностей, узагальнені існуючі та створені нові математичні методи аналізу криптографічних алгоритмів, визначені початкові стани певних класів генераторів псевдовипадкових послідовностей.

### **Реферат англійською:**

The analysis of modern pseudorandom sequences generators is made; the existing mathematical methods of cryptographic algorithms analysis are generalized and new ones are developed; the initial states of some classes of pseudorandom sequences generators are determined.

**Індекс УДК:** 681.3.06:004.92, 681.3.06:519.248.681

**Коди тематичних рубрик:** 81.14.11.05

### **Керівники роботи**

**Власне Прізвище Ім'я По-батькові:** Савчук Михайло Миколайович

### **Науковий ступінь:**

**Вчене звання:**

**Ідентифікатор ORCID ID:**

**Додаткова інформація:**

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

**Назва НТП українською:** Спеціальні сучасні математичні методи у криптоаналізі. Визначення початкових станів певних класів генераторів псевдовипадкових послідовностей.

**Назва НТП англійською:** The special modern mathematical methods is in cryptanalysis. Determination of the initial states of certain classes of generators of pseudorandom sequences»

**НТП, яку передбачалося створити:**

**Причини, через які НТП не було створено:**

**Отримані результати:**

**Галузь застосування:** 73.10.1- Дослідження і розробки в галузі природничих та технічних наук

**Реєстраційний номер картки технології:**

**Опис НТП:** Отримано оцінки багатократного перекриття гамми для генераторів випадкових та псевдовипадкових послідовностей. Розроблено декілька нових алгоритмів побудови лінійних апроксимацій псевдобулевих функцій. Проведено аналіз криптографічного примітиву для побудови криптосистем з відкритим ключем. Встановлено співвідношення між часом та пам'яттю що підвищують ефективність варіанту trade-off атаки. Запропоновано новий тест оцінки якості випадкової послідовності.

**Соціально-економічна спрямованість НТП:**

**Вплив НТП на довкілля:**

**Впровадження НТП:** Впроваджено

**Практична реалізація НТП**

**Початок етапу:** без обмежень

**Закінчення етапу:**

**Споживачі продукції:** Служба зовнішньої розвідки 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**

Новіков Олексій Миколайович

**Перелік осіб-виконавців**

Єндовицький П.

Завадська Л.О.

Ковальчук Л.В.

Олексійчук А.

Фесенко А.

Шевцов А.

Яковлев С.

**Відповідальний за підготовку  
облікових документів**

**Телефон**

**Реєстратор**

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

