

# Облікова картка ДіР



## I. Загальні відомості

**Державний обліковий номер:** 0218U007084

**Державний реєстраційний номер:** 0118U001653

**Особливі позначки:** відкрита

**Дата реєстрації:** 17-12-2018

## II. Етап виконання ДіР

**Номер етапу:** 1

**Назва етапу:** Вибір та аналіз напрямків дослідження. Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень.

**Початок етапу:** 08.2018

**Закінчення етапу:** 12.2018

**Вид звітнього документа:** Остаточний звіт

## III. Відомості про виконавця ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Видавничо-поліграфічний інститут Національного Технічного Університету України "Київський політехнічний інститут"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 236-70-98, 204-81-76

## 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> 784 |
|------------------------------------------------------|

## **VII. Відомості про ДіР**

### **Назва роботи українською:**

Розроблення та адаптація математичних методів аналізу систем криптографічного захисту інформації з урахуванням сучасних вимог інформаційного середовища

### **Назва роботи англійською:**

Development and Adaptation of Mathematical Analysis Methods for Cryptographic Security Systems with Respect to Contemporary Demands of Information Environment

### **Реферат українською:**

Звіт про НДР містить: 324 стор., 36 рисунків, 20 таблиць, 171 джерел. Об'єкт дослідження – системи та процеси криптографічного захисту інформації, способи створення криптоатак на системи захисту інформації. Предмет дослідження – методи криптографічного аналізу та синтезу, математичні моделі стійкості криптографічних систем захисту інформації та криптографічних атак. Метою виконання НДР є отримання нових та адаптація існуючих математичних методів, процедур та алгоритмів аналізу сучасних систем криптографічного захисту інформації з урахуванням сучасних вимог інформаційного середовища.

### **Реферат англійською:**

The report contains: 324 pages, 36 figures, 20 tables, 171 sources. The object of research is systems and processes of cryptographic security, and cryptographic attacks on information security systems. The subject of research is methods of cryptographic analysis and synthesis, mathematical models of security for cryptographic systems and cryptographic attacks. The purposes of the work are to obtain new and to adapt existing mathematical methods, procedures and algorithms for analyzing modern cryptographic security systems with respect to the current requirements of the information environment.

**Індекс УДК:** 004.7, 681.3.06:519.248.681

**Коди тематичних рубрик:** 50.37.23

### **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)**

## **IX. Бібліографічний опис**

1)Кудін А.М., Коваленко Б.А., Швідченко І.В. Технологія «блокчейн»: питання аналізу та синтезу / Кібернетика та системний аналіз. – № 6. – 2018 р. (у друку) 2)Bohdan Kovalenko and Anton Kudin Kleptography trapdoor free cryptographic protocols // Cryptology ePrint Archive: Report 2018/989. available from <https://eprint.iacr.org/2018/989>. 3)Сергеев С. Стійкість шифру AES до диференціального криптоаналізу відносно альтернативних алгебраїчних операцій / С. Сергеев, С. Яковлев // «Інтернет-Освіта-Наука 2018», Одинадцята міжнародна науково-практична конференція ІОН-2018, 22-25 травня, 2018 : Збірник праць ІОН

2018. — Вінниця : ВНТУ, 2018 — С. 130-132. 4)Сергеев С. Стійкість шифру «Калина» до диференціального криптоаналізу відносно альтернативних алгебраїчних операцій / С. Сергеев, С. Яковлев // XX Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (22-25 травня 2018 р., м. Буча). — К.: НДЦ «Тезис», 2018. — стор. 186-187.

## **Х. Заключні відомості**

**Керівник юридичної особи**

Ільченко Михайло Юхимович

**Перелік осіб-виконавців**

Коваленко Б.

Ковальчук Л.В.

Кудін А.М.

Олексійчук А.

Поремський М.

Сергеев С.

Фаль О.М.

Фесенко А.В.

Ядуха Д.

Яковлев С.В.

**Відповідальний за підготовку  
облікових документів**

**Телефон**

**Реєстратор**

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

