

# Реєстраційна картка НДДКР

Державний реєстраційний номер: 0124U002565

Відкрита

Дата реєстрації: 25-03-2024

Статус виконавця: 17 - головний виконавець



## 1. Загальні відомості

Підстава для проведення робіт: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

КПКВК: 6541030

Напрямок фінансування: 2.1 - фундаментальні дослідження

### Джерела фінансування

7713 - кошти держбюджету

Загальний обсяг фінансування (тис. грн.): 25961.628

У тому числі по роках (тис. грн.):

Рік	Фінансування
2024	2474.893
2025	3217.361
2026	4504.305
2027	6306.027
2028	9459.042

## 2. Замовник

Назва організації: Національна академія наук України

Код ЄДРПОУ/ІПН: 00019270

Адреса: вул. Володимирська, буд. 54, м. Київ, 01601, Україна

Підпорядкованість:

Телефон: 380442343243

E-mail: prez@nas.gov.ua

WWW: <http://nas.gov.ua>

### 3. Виконавець

**Назва організації:** Інститут кібернетики імені В. М. Глушкова Національної академії наук України

**Код ЄДРПОУ/ІПН:** 05417176

**Підпорядкованість:** Національна академія наук України

**Адреса:** проспект Академіка Глушкова, буд. 40, м. Київ, 03187, Україна

**Телефон:** 380445262008

**Телефон:** 380445264178

**E-mail:** incyb@incyb.kiev.ua

**WWW:** <http://incyb.kiev.ua/>

### 4. Співвиконавець

### 5. Науково-технічна робота

#### Назва роботи (укр)

Розробити ефективні за точністю та швидкістю алгоритми розв'язання задач інформаційної безпеки, цифрової обробки сигналів та зображень, чисельного інтегрування

#### Назва роботи (англ)

Develop algorithms that are effective in terms of accuracy and speed of solving information security problems, digital processing of signals and images, and numerical integration

#### Мета роботи (укр)

Метою роботи є розробка ефективних за точністю та швидкістю алгоритмів розв'язання задач інформаційної безпеки, цифрової обробки сигналів та зображень, оптимального інтегрування, а саме: побудова ефективних за швидкістю алгоритмів обчислення криптопримітивів двоключової криптографії (шифрування, дешифрування, електронний цифровий підпис) в різних моделях обчислень та отримання оцінок їх складності; розробка ефективних алгоритмів швидких мультивейвлет-перетворень з використанням цілочислової арифметики для оброблення та аналізу сигналів і зображень; розробка методів та алгоритмів оперативного обчислення поточних та інтегральних показників станів об'єктів на основі оброблення та аналізу даних моніторингу; побудова оптимальних за точністю та близьких до них квадратурних та кубатурних формул обчислення інтегралів від швидкоосцилювальних функцій з осциляторами різного типу для інтерполяційних класів підінтегральних функцій та отримання апіорних та апостеріорних оцінок характеристик якості побудованих алгоритмів.

#### Мета роботи (англ)

The purpose of the work is to develop algorithms that are effective in terms of accuracy and speed of solving information security problems, digital processing of signals and images, and optimal integration, namely: construction of speed-efficient algorithms for calculating crypto primitives of two-key cryptography (encryption, decryption, electronic digital signature) in various calculation models and obtaining estimates of their complexity; development of efficient algorithms of fast multiwavelet transformations using integer arithmetic for processing and analysis of signals and images; development of methods and algorithms for operational calculation of current and integral indicators of object states based on processing and analysis of monitoring data; construction of quadrature and cubature formulas that are optimal in terms of accuracy and close to them for calculating integrals from fast oscillating functions with oscillators of various types for interpolation classes of integrable functions and obtaining a priori and a posteriori evaluations of the quality characteristics of the constructed algorithms.

**Пріоритетний напрям науково-технічної діяльності:** Фундаментальні наукові дослідження з найважливіших проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу

## Стратегічний пріоритетний напрям інноваційної діяльності:

**Вид роботи:** 39 - фундаментальна

**Очікувані результати:** Методи, теорії

**Галузь застосування:** У математичному моделюванні, яке вимагає великого об'єму обчислень. Зокрема, розроблені методи та алгоритми обчислення криптопримітивів двоключової криптографії становитимуть основу для підвищення ефективності за часом обчислення криптопримітивів для двоключової криптографії на високопродуктивних комп'ютерних системах: в Інституті кібернетики імені В.М. Глушкова, у Державній службі спеціального зв'язку та захисту інформації, в СБ України тощо.

## Експерти

## 6. Етапи виконання

Номер	Початок	Закінчення	Звітний документ	Назва етапу
1	01.2024	12.2028	Остаточний звіт	Розробити ефективні за точністю та швидкістю алгоритми розв'язання задач інформаційної безпеки, цифрової обробки сигналів та зображень, чисельного інтегрування

## 7. Індекс УДК тематичних рубрик НТІ

**Коди тематичних рубрик НТІ:** 27.41.17

**Індекс УДК:** 519.6:517

## 8. Заключні відомості

**Керівник організації:**

Сергієнко Іван Васильович (д. ф.-м. н., академік НАНУ)

**Керівники роботи:**

Задірака Валерій Костянтинівич (д.ф.-м.н., академік НАНУ)

**Відповідальний за подання документів:** Луц Лілія Володимирівна (Тел.: +38 (099) 157-92-42)

**Керівник відділу реєстрації наукової діяльності**  
**УкрІНТЕІ**



Юрченко Т.А.