

# Облікова картка ДіР



## I. Загальні відомості

**Державний обліковий номер:** 0211U008947

**Державний реєстраційний номер:** 0110U004094

**Особливі позначки:** відкрита

**Дата реєстрації:** 02-12-2011

## II. Етап виконання ДіР

**Номер етапу:** 1

**Назва етапу:** Протоколи забезпечення невідслідковуваності та автентифікації інформації в автоматизованих інформаційних системах і розширення функціональності стандартів цифрового підпису

**Початок етапу:** 06.2010

**Закінчення етапу:** 12.2011

**Вид звітнього 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:** 2.1 - фундаментальні дослідження

### Джерела фінансування

7713 - кошти держбюджету

**Код програмної класифікації видатків і кредитування (КПКВК):** 6541030

|                                                      |
|------------------------------------------------------|
| <b>Фактичний обсяг фінансування (тис. грн.):</b> 316 |
|------------------------------------------------------|

## **VII. Відомості про ДіР**

### **Назва роботи українською:**

Протоколи забезпечення невідслідковуваності та автентифікації інформації в автоматизованих інформаційних системах і розширення функціональності стандартів цифрового підпису

### **Назва роботи англійською:**

Protocols of providing of untraceability and authentication of information in informational systems and expansion of functionality of digital signature standards

### **Реферат українською:**

Об'єкт дослідження: Алгоритми сліпого, колективного та сліпого колективного електронного цифрового підпису(ЕЦП). Мета дослідження: розроблення протоколів сліпого, колективного та сліпого колективного ЕЦП, які використовують базові процедури формування і перевіряння справжності ЕЦП, що рекомендовані офіційними стандартами України. Методи дослідження: теорія груп, теорія скінченних полів, теорія еліптичних кривих, обчислювальні методи алгебри та теорії чисел. Результати виконання роботи: розроблені та реалізовані протоколи сліпого , колективного та сліпого колективного підпису що ґрунтуються на використанні стандарту ЕЦП України в якості базового алгоритму; виконана оцінка безпеки запропонованих протоколів стосовно різних типів атак; сформульовані вимоги до розмірів параметрів, використовуваних в алгоритмах автентифікації інформації; здійснено аналіз безпеки протоколів сліпого колективного підпису, що ґрунтуються на стандарті ЕЦП України, стосовно атак, направлених на обчислення секретного ключа одного з підписантів, що здійснюються рештою підписантів; Ключові слова: СЛІПІЙ ЦИФРОВИЙ ПІДПИС, ЦИКЛІЧНІ ГРУПИ, СКІНЧЕННІ ПОЛЯ, ЕЛІПТИЧНІ КРИВІ, АСИМЕТРИЧНІ КРИПТОГРАФІЧНІ АЛГОРИТМИ.

### **Реферат англійською:**

Object of research: Algorithms for the blind, the collective and the collective blind digital signature (DS). Aim: develop protocols blind, collective and collective blind digital signature, using the basic procedure of forming and checking the authenticity of the DS recommended by the official standards of Ukraine. Methods: group theory, the theory of finite fields, the theory of elliptic curves, computational methods of algebra and number theory. The results of the work: developed and implemented protocols blind, collective and collective blind signature based on the use of standard DS Ukraine as the basic algorithm; the estimation of the proposed security protocols on different types of attacks; formulated requirements to the size of the parameters used in algorithms authentication information, the analysis of security protocols collective blind signature based on the standard DS Ukraine, on attacks aimed at calculating the private key of one of the signatories, which made the rest of the signatories; developed scenarios for the application of the results obtained in applied science evaluated the possibility of extending the functionality of standard DS others. Keywords: the blind digital signature, cyclic group, finite field , elliptic curve asymmetric cryptographic algorithms.

**Індекс УДК:** 004.89:004.4, 004.89:004.4

**Коди тематичних рубрик:** 28.23.29

### **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:** Протоколи забезпечення невідслідковуваності та автентифікації інформації в автоматизованих інформаційних системах і розширення функціональності стандартів цифрового підпису

**Назва НТП англійською:** Protocols of providing of untraceability and authentication of information in informational systems and expansion of functionality of digital signature standards

**НТП, яку передбачалося створити:**

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

**Отримані результати:** Поліпшення якості продукції

**Галузь застосування:** 72.Діяльність у сфері інформатизації

**Реєстраційний номер картки технології:**

**Опис НТП:** Розроблені, досліджені та реалізовані у вигляді комплексу комп'ютерних програм протоколи сліпого , колективного та сліпого колективного підпису, які ґрунтуються на використанні стандарту ЕЦП України в якості базового алгоритму;

**Соціально-економічна спрямованість НТП:**

**Вплив НТП на довкілля:**

**Впровадження НТП:** Не впроваджено

**Практична реалізація НТП**

**Початок етапу:** 2014-2015 р.р

**Закінчення етапу:**

**Споживачі продукції:** Державні установи, банки

**Перспективні ринки:** Україна, Росія

**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**

Завірюха О.В.

Коваленко І.М.

Кочубінський А.І.

Кошкіна Н.В

Савчук М.М.

Синявський В.Ф.

Фаль О.М.

**Відповідальний за підготовку  
облікових документів**

**Телефон**

**Реєстратор**

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

