

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0222U001690

Державний реєстраційний номер: 0119U101915

Особливі позначки: відкрита

Дата реєстрації: 31-01-2022

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження методів, механізмів та криптографічних засобів для застосування у перехідний період та пост-квантовий період

Початок етапу: 08.2018

Закінчення етапу: 06.2019

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577021013, 380577021807

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Приватне акціонерне товариство "Інститут інформаційних технологій"

Код за ЄДРПОУ: 22723472

Місцезнаходження: вул. Бакуліна, буд. 12, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577142205

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: 2.1 - фундаментальні дослідження

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 400.000
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження методів, механізмів та криптографічних засобів для застосування у перехідний та пост-квантовий період

Назва роботи англійською:

Research of methods, mechanisms and cryptographic means for use in the transition and post-quantum period

Реферат українською:

Метою НДР є дослідження методів, механізмів та засобів симетричних криптоперетворень та обґрунтування пропозицій щодо їх застосування у перехідний період та пост-квантовий період. В результаті роботи було досліджено властивості різних сімейств криптографічних геш-функцій, проаналізовано шляхи їхньої побудови та вивчено сучасний стан у галузі стандартизації та практичного застосування криптографічних функцій гешування для побудови розподілених інформаційних систем типу блокчейн. Проведено статистичні дослідження алгоритмів гешування.

Реферат англійською:

The purpose of the research is to study the methods, mechanisms and means of symmetric crypto creations and substantiate the proposals for their use in the transition period and post-quantum period. As a result, the properties of different families of cryptographic hash functions were studied, the ways of their construction were analyzed and the current state in the field of standardization and practical application of cryptographic hash functions for building distributed information systems such as blockchain was studied. Statistical research of hashing algorithms is carried out.

Індекс УДК: 004.45

Коди тематичних рубрик: 50.05.15

Керівники роботи

Власне Прізвище Ім'я По-батькові: Кузнецов Олександр Олександрович

Науковий ступінь: д. т. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Дослідження методів, механізмів та криптографічних засобів для застосування у перехідний та пост-квантовий період

Назва НТП англійською: Research of methods, mechanisms and cryptographic means for use in the transition and post-quantum period

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Комп'ютерне програмування, консультування та пов'язана з ним діяльність

Реєстраційний номер картки технології:

Опис НТП: Удосконалено методи формування параметрів і ключів та вдосконаленого цифрового підпису на основі геш-функцій та розроблені та протестовані їх програмні реалізації. Обґрунтовані вимоги, щодо побудови національних стандартів електронного підпису на основі геш-функцій для застосування у постквантовий період.

Соціально-економічна спрямованість НТП: Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу:

Закінчення етапу:

Споживачі продукції:

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

Семенець Валерій Васильович

Д. Т. Н.

Перелік осіб-виконавців

Власов Андрій Володимирович
(к.т.н.)

Гапон Андрій Олександрович

Журило Олег Дмитрович

Колгатін Андрій Олександрович

Коптева Марія Володимирівна

Кохан Сергій Анатолійович

Лисицкий Костянтин Євгенійович

Луценко Марія Сергіївна

Ляшенко Олексій Сергійович
(к.т.н.)

Малеева Ганна Андріївна

Марухненко Олександр Сергійович

Перепада Вікторія Ігорівна

Петренко Ольга Євгенівна
(к.т.н., 05.13.21)

Родінко Марія Юріївна

Руженцев Віктор Ігорович
(Д. Т. Н.)

Сергійчук Юрій Олександрович

Скрябін Богдан Борисович

Стеценко Павло Ігорович

Северінов Олександр Васильович
(к.т.н., 20.02.12)

Тимченко Владислав Анатолійович

Федюшин Олександр Іванович
(К. Т. Н.)

Халімов Геннадій Зайдулович
(Д. Т. Н.)

Шипілов Дмитрій Віталійович

Відповідальний за підготовку облікових документів

Малеева Ганна Андріївна

Телефон

+38 (057) 702-14-25

Реєстратор

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

