

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0220U103670

Державний реєстраційний номер: 0120U100109

Особливі позначки: відкрита

Дата реєстрації: 03-11-2020

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження сучасних методів криптографічного захисту для застосування у пост-квантовий період

Початок етапу: 11.2019

Закінчення етапу: 07.2020

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, 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, 12, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Держадміністрація

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

VII. Відомості про ДіР

Назва роботи українською:

Дослідження сучасних методів криптографічного захисту для застосування у пост-квантовий період

Назва роботи англійською:

Research of modern methods of cryptographic protection for use in the post-quantum period

Реферат українською:

Метою НДР є дослідження криптографічних методів та обґрунтування пропозицій щодо їх застосування у пост-квантовий період. В результаті роботи була проведено: дослідження стійкості методів асиметричного шифрування, інкапсуляції ключів, електронного підпису на основі кодів виправлення помилок та геш-функцій щодо їх застосування у пост-квантовий період. А також розроблені та протестовані схеми асиметричного шифрування, інкапсуляції ключів та електронного підпису на основі кодів виправлення помилок та схем електронного підпису на основі геш-функцій для застосування у пост-квантовий період.

Реферат англійською:

The purpose of research is to study cryptographic methods and substantiate proposals for their use in the post-quantum period. As a result of the work, the following was performed: study of the stability of asymmetric encryption methods, key encapsulation, electronic signature based on error correction codes and hash functions for their use in the post-quantum period. As well as developed and tested schemes of asymmetric encryption, encapsulation of keys and electronic signature based on error correction codes and electronic signature schemes based on hash functions for use in the post-quantum period.

Індекс УДК: 004.7

Коди тематичних рубрик: 50.37.23

Керівники роботи

Власне Прізвище Ім'я По-батькові: Халімов Геннадій Зайдулович

Науковий ступінь: д. т. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Методи асиметричного шифрування, інкапсуляції ключів та електронного підпису на основі кодів виправлення помилок та схем електронного підпису на основі геш-функцій

Назва НТП англійською: Methods of asymmetric encryption, encapsulation of keys and electronic signature based on error correction codes and electronic signature schemes based on hash functions

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 асиметричного шифрування, інкапсуляції ключів та електронного підпису на основі кодів виправлення помилок та схем електронного підпису на основі геш-функцій та розроблені та протестовані їх програмні реалізації. Обґрунтовані вимоги, щодо побудови національних стандартів асиметричного шифрування, інкапсуляції ключів, електронного підпису на основі кодів виправлення помилок та схем електронного підпису на основі геш-функцій для застосування у пост-квантовий 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: 11.2019

Закінчення етапу: 07.2020

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

Бологова Наталя Миколаївна

Власов Андрій Володимирович

(к.т.н.)

Кузнецов Олександр Олександрович

(д. т. н., 05.13.21)

Кіян Анастасія Сергіївна

Ляшенко Олексій Сергійович

(к.т.н.)

Мартовіцький Віталій Олександрович

(к.т.н.)

Марухненко Олександр Сергійович

Перепада Вікторія Ігорівна

Романюков Микола Генріхович

Руженцев Віктор Ігорович

(д. т. н.)

Стеценко Павло Ігорович

Северінов Олександр Васильович

(к.т.н., 20.02.12)

Шипілов Дмитрій Віталійович

Відповідальний за підготовку облікових документів

Северінов Олександр Васильович

Телефон

+38 (057) 702-14-25

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

