

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0222U001696

Державний реєстраційний номер: 0121U111056

Особливі позначки: відкрита

Дата реєстрації: 31-01-2022

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження сучасних методів вдосконаленого цифрового підпису на алгебраїчних решітках в постквантовий період

Початок етапу: 03.2021

Закінчення етапу: 10.2021

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: 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.): 200.000
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження сучасних методів вдосконаленого цифрового підпису на алгебраїчних решітках в постквантовий період

Назва роботи англійською:

Research of modern methods of advanced digital signature on algebraic lattices in the post-quantum period

Реферат українською:

Метою НДР є дослідження методів побудови електронного підпису на алгебраїчних решітках та обґрунтування пропозицій щодо їх застосування у постквантовий період. В результаті роботи була проведена: побудова математичної моделі алгоритму вдосконаленого цифрового підпису, що базується на перетвореннях на алгебраїчних решітках, обґрунтування вимог, щодо побудови національних стандартів вдосконаленого цифрового підпису на основі алгоритмів на алгебраїчних решітках у пост-квантовий період. Розроблена програмна реалізація базового алгоритму «Система 2021» формування вдосконаленого цифрового підпису на алгебраїчних решітках та обґрунтування застосування параметрів 256, 512, 1024 біт.

Реферат англійською:

The purpose of research of modern methods of advanced digital signature on algebraic lattices in the post-quantum period. As a result, the following work was carried out: construction of a mathematical model of advanced digital signature algorithm based on transformations on algebraic lattices, substantiation of requirements for building national standards of advanced digital signature based on algorithms on algebraic lattices in the post-quantum period. The software implementation of the basic algorithm "System 2021" of formation of the advanced digital signature on algebraic lattices and the substantiation of application of parameters 256, 512, 1024 bits is developed.

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:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

IX. Бібліографічний опис

Х. Заключні відомості

Керівник юридичної особи

Неофітний Михайло Васильович

Перелік осіб-виконавців

16. Євген'єв Андрій Михайлович

Аргунов Володимир Володимирович

Власов Андрій Володимирович

(к.т.н.)

Гапон Андрій Олександрович

Гвоздьов Роман Юрійович

Гриненко Тетяна Олексіївна

Журило Олег Дмитрович

Зубрич Артем Віталійович

Котух Євген Володимирович

(д. т. н., професор, 25.00.02)

Кохан Сергій Анатолійович

Ляшенко Олексій Сергійович

(к.т.н., доцент, 05.13.07)

Малеева Ганна Андріївна

Мартовіцький Віталій Олександрович

(к.т.н., доц.)

Марухненко Олександр Сергійович

Олешко Інна Вікторівна

(к.т.н.)

Перепада Вікторія Ігорівна

Петренко Ольга Євгенівна

(к.т.н., доц., 05.13.21)

Поддубний Вадим Олександрович

Руженцев Віктор Ігорович

(д. т. н.)

Северінов Олександр Васильович

(к.т.н., доц., 20.02.12)

Федюшин Олександр Іванович

(к. т. н.)

Шафоростов Михайло Олександрович

Щербина Денис Вадимович

Відповідальний за підготовку

Северінов Олександр Васильович

облікових документів

Телефон

+38 (057) 702-14-25

Реєстратор

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



Юрченко Тетяна Анатоліївна