Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0222U001420

Державний реєстраційний номер: 0121U109939

Особливі позначки: відкрита

Дата реєстрації: 27-01-2022

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження проблем КЗІ в пост-квантовому середовищі. Обґрунтування критеріїв та показників ефективності, методики оцінки та порівняльних досліджень. Дослідження методів квантового криптографічного аналізу.

Початок етапу: 04.2021

Закінчення етапу: 12.2021

Вид звітного документа: Проміжний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577051247

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Міністерство освіти і науки України

Код за ЄДРПОУ: 38621185

Місцезнаходження: просп. Перемоги, буд. 10, м. Київ, Київська обл., 01135, Україна

Форма власності:

Сфера управління: Кабінет Міністрів України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380444813221

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)

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2021040

Фактичний обсяг фінансування (тис. грн.): 2225.903

VII. Відомості про ДіР

Назва роботи українською:

Математичні та програмні моделі, методи та механізми криптографічного захисту інформації для пост-квантового середовища в інтересах національної безпеки держави

Назва роботи англійською:

Mathematical and software models, methods and mechanisms of cryptographic information protection for the post-quantum environment for the interests of national security

Реферат українською:

Об'єкт дослідження – процеси обґрунтування вимог та перспектив надання електронних довірчих послуг в перехідний та постквантовий періоди на основі стандартизованих асиметричних криптографічних перетворень. Предмет досліджень – методи та засоби асиметричних криптоперетворень на основі існуючих та нових алгебраїчних структур для перехідного та постквантового періодів. Метою НДР є підвищення національної безпеки держави в інформаційній сфері шляхом розробки та впровадження математичних та програмних моделей, методів та механізмів криптографічного захисту інформації (КЗІ) з урахуванням вимог постквантового середовища; отримання нових фундаментальних та прикладних знань та положень у галузі інформаційної та кібербезпеки з побудови квантових криптографічних технологій; інтеграція української криптографічної науки до світового наукового простору через участь в міжнародних конкурсах постквантової криптографії. НДР призначено для вирішення таких завдань: дослідження сучасних проблем КЗІ з урахуванням вимог постквантового середовища; обґрунтування критеріїв та показників ефективності, розробка методики оцінки та порівняльних досліджень криптопримітивів; розробка та дослідження моделей, методів та протоколів КЗІ із використанням методів сучасної криптографії; Методи дослідження – методи криптології, математичні методи експертного оцінювання та порівняння ЕП, методи математичного та програмного моделювання асиметричних криптоперетворень, методи аналізу та синтезу існуючих та перспективних асиметричних криптопримітивів.

Реферат англійською:

Mathematical and software models, methods and mechanisms of cryptographic informatio

Індекс УДК: 65.012.8; 003.26; 004.56.5

Коди тематичних рубрик: 20.53.37

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)

IX. Бібліографічний опис

1. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022s. Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing. https://doi.org/10.1007/978-3-030-79770-6

2. Kuznetsov, A., Gorbenko, Y., Kolovanova, I., Smirnov, S., Perevozova, I., Kuznetsova, T., 2021d. Output Feedback Encryption Mode: Periodic Features of Output Blocks Sequence, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 621–648. https://doi.org/10.1007/978-3-030-43070-2_27

3. Kuznetsov, A., Kononchenko, A., 2021. Software Implementation of Data Hiding in Vector Images, in: 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON). Presented at the 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 572–577. https://doi.org/10.1109/UKRCON53503.2021.9575240

4. Kuznetsov, A., Fedotov, S., Bagmut, M., 2021c. Convolutional Neural Networks to Protect Against Spoofing Attacks on Biometric Face Authentication, in: Wrycza, S., Maślankowski, J. (Eds.), Digital Transformation, Lecture Notes in Business Information Processing. Springer International Publishing, Cham, pp. 123–146. https://doi.org/10.1007/978-3-030-85893-3_9

5. Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., Kolhatin, A., 2021h. Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain. IJCNIS 13, 1–15. https://doi.org/10.5815/ijcnis.2021.02.01

6. Kuznetsov, A., Pushkar'ov, A., Serhiienko, R., Smirnov, O., Babenko, V., Kuznetsova, T., 2021j. Representation of Cascade Codes in the Frequency Domain, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 557–587. https://doi.org/10.1007/978-3-030-43070-2_25

X. Заключні відомості

Керівник юридичної особи Бакіров Віль Савбанович

д. соц. н.

Перелік осіб-виконавців

Горбенко Іван Дмитрович
(д.т.н., 21.01.09)

Кузнецов Олександр Олександрович
(д. т. н., 05.13.21)

Полуяненко Микола Олександрович
(к. т. н.)

Відповідальний за підготовку облікових документів Майстренко Людмила Олексіївна

Телефон +38 (057) 707-55-23

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

