

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0223U000934

Державний реєстраційний номер: 0121U109939

Особливі позначки: відкрита

Дата реєстрації: 22-01-2023

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Розробка та дослідження моделей, методів та протоколів КЗІ для пост-квантового середовища. Аналіз та дослідження квантових криптографічних технологій для ЕДП в умовах пост-квантового середовища. Впровадження результатів досліджень.

Початок етапу: 01.2022

Закінчення етапу: 12.2022

Вид звітнього документа: Остаточний 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)

Напрямок 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.): 1449.065

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:

Проект прикладного дослідження в інтересах національної безпеки держави в інформаційній сфері (практична значимість підтверджена Державною службою спеціального зв'язку та захисту інформації України). Дослідження спрямовано на отримання нових фундаментальних та прикладних знань у галузі інформаційної та кібербезпеки в частині створення надійних та безпечних технологій криптографічного захисту інформації (КЗІ), придатних для практичного застосування в нових умовах пост-квантового середовища, тобто коли зломисникам доступні квантові засоби обчислення для проведення криптоаналізу. Також в проекті досліджується побудова квантових криптоалгоритмів, тобто криптографічних перетворень із використанням квантово-механічних властивостей. Ці алгоритми будуть застосовані на заміну традиційним при наявності універсальних квантових обчислювачів, для реалізації на нових фізичних принципах механізмів захисту інформації, як для традиційних застосувань, так і для нових прикладних додатків. Проект безпосередньо пов'язаний із проведенням відкритого конкурсу пост-квантової криптографії національного інституту стандартів і технологій (NIST) США з розробки, дослідження та стандартизації у найближчі роки низки нових стандартів пост-квантового КЗІ.

Реферат англійською:

Project of applied research in the interests of national security of the state in the information sphere (practical significance confirmed by the State Service of Special Communications and Information Protection of Ukraine). The research is aimed at obtaining new fundamental and applied knowledge in the field of information and cybersecurity in terms of creating reliable and secure technologies for cryptographic protection of information (CPI), suitable for practical application in the new conditions of the post-quantum environment, that is, when attackers have access to quantum computers for cryptanalysis. The project also investigates the construction of quantum cryptoalgorithms, that is, cryptographic transformations using quantum mechanical properties. These algorithms will be used to replace traditional ones in the presence of universal quantum computers, to implement on new physical principles of information security mechanisms, both for traditional applications and for new applications. The project is directly related to the open competition of post-quantum cryptography of the National Institute of Standards and Technology (NIST) of the United States to develop, research and standardize in the coming years a number of new standards of post-quantum CPI.

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)

Назва НТП українською: Моделі, методи та механізми криптографічного захисту інформації для пост-квантового середовища

Назва НТП англійською: Models, methods and mechanisms of cryptographic protection of information for the post-quantum environment

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії, Нормативні документи, Методичні документи, Програмні продукти, Аналітичні матеріали

Галузь застосування: Інформаційні технології

Реєстраційний номер картки технології:

Опис НТП: При виконанні проекту отримано нові науково-обґрунтовані знання та положення з актуальних проблем КЗІ з урахуванням вимог пост-квантового середовища, зокрема: моделей загроз, порушника та безпеки; критеріїв та показників ефективності механізмів КЗІ; методик оцінки та порівняльних досліджень; результатів порівняння та оцінки ефективності криптографічних примітивів (ЕП, НШ, ІК та ін.); квантового криптографічного аналізу, порівняльних досліджень та класифікації моделей, методів та алгоритмів КЗІ, вимог та умов їх практичного застосування; математичних моделей, методів, обчислювальних алгоритмів та протоколів КЗІ із використанням різних класів математичних перетворень (у кільцях зрізаних поліномів; завадостійких кодів; мультіваріативних перетворень; геш-функцій; алгоритмів симетричної криптографії), практичних рекомендацій з їх впровадження; основних підходів, моделей, методів та обчислювальних алгоритмів, що застосовують явища квантової механіки для передачі та обробки даних в квантових обчислювачах; квантових криптографічних алгоритмів та пропозицій з їх практичної реалізації як для традиційних застосувань так і для нових додатків; аналізу національних та міжнародних нормативно-правових документів, які регулюють систему стандартизації криптографічних перетворень; рекомендацій стосовно прийняття національних та/або гармонізації міжнародних стандартів пост-квантової криптографії; рекомендацій стосовно імплементації розроблених криптоперетворень в діючих інформаційних системах та мережах.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту, Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих, Підвищення автоматизації виробничих процесів, 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: розробники (різних форм власності) засобів КЗІ, комплексів та систем кібербезпеки, інформаційних та телекомунікаційних систем і технологій в інтересах національної безпеки та оборони держави

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

A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Analysis of Stream Modes for Block Symmetric Ciphers, vol. 375. Springer Science and Business Media Deutschland GmbH, 2022, p. 98. doi: 10.1007/978-3-030-79770-6_5

A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Analysis of Synchronous Stream Cryptoconversions, vol. 375. Springer Science and Business Media Deutschland GmbH, 2022, p. 64. doi: 10.1007/978-3-030-79770-6_4.

A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Requirements for Feedback Coefficients, What Should the M-Nlfsr Respond to?, vol. 375. Springer Science and Business Media Deutschland GmbH, 2022, p. 377. doi: 10.1007/978-3-030-79770-6_13

A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Research of Second-Order Properties of NLFSR. Comparative Analysis of M-NLFSR and M-LFSR, vol. 375. Springer Science and Business Media Deutschland GmbH, 2022, p. 465. doi: 10.1007/978-3-030-79770-6_15

A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Stream Symmetric Cipher "Strumok," vol. 375. Springer Science and Business Media Deutschland GmbH, 2022, p. 516. doi: 10.1007/978-3-030-79770-6_16.

R. Oliynykov, O. Kuznetsov, O. Lemeshko, and T. Radivilova, Preface, vol. 115. Springer Science and Business Media Deutschland GmbH, 2022, p. x. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85127975895&partnerID=40&md5=07065b7413740d9d95aea36d9dd19ac6>

Х. Заключні відомості

Керівник юридичної особи

Бакіров Віль Савбанович

д. соц. н.

Перелік осіб-виконавців

Єсін Віталій Іванович

(д. т. н., 05.13.06)

Єсіна Марина Віталіївна

(к. т. н.)

Івко Тетяна Вікторівна

Багмут Михайло Олександрович

(аспірант)

Бобух Всеволод Анатолійович

(к. т. н.)

Горбенко Іван Дмитрович

(д.т.н., 20.01.09)

Горбенко Юрій Іванович

(к. т. н.)

Гостев Олександр Леонтійович

Кандій Сергій Олегович

(аспірант)

Качко Олена Григорівна

(к. т. н.)

Кошман Сергій Олександрович

(к. т. н., 05.13.05)

Краснобаєв Віктор Анатолійович

(д.т.н., 20.02.14)

Олійников Роман Васильович

(д. т. н., 05.13.05)

Полуяненко Микола Олександрович

(к. т. н.)

Пономар Володимир Андрійович

(к.т.н.)

Скриннік Володимир Андрійович

Седова Крістіна Володимирівна

Швайко Олександр Дмитрович

Відповідальний за підготовку облікових документів

Козир О.В.

Телефон

+38 (057) 707-52-96

Реєстратор

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

