

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0221U102101

Державний реєстраційний номер: 0118U002024

Особливі позначки: відкрита

Дата реєстрації: 28-01-2021

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: АНАЛІЗ, ДОСЛІДЖЕННЯ, РОЗРОБКА ТА СТАНДАРТИЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ПОСТ-КВАНТОВОМУ СЕРЕДОВИЩІ, В УМОВАХ ІНФОРМАЦІЙНИХ І ГІБРИДНИХ ВІЙН

Початок етапу: 01.2018

Закінчення етапу: 12.2020

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): 2201040

Фактичний обсяг фінансування (тис. грн.): 2027.606

VII. Відомості про ДіР

Назва роботи українською:

АНАЛІЗ, ДОСЛІДЖЕННЯ, РОЗРОБКА ТА СТАНДАРТИЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ПОСТ-КВАНТОВОМУ СЕРЕДОВИЩІ, В УМОВАХ ІНФОРМАЦІЙНИХ І ГІБРИДНИХ ВІЙН

Назва роботи англійською:

Analysis, investigation, development and standardization of cryptosystems for information security in post-quantum environment in conditions of information and hybrid wars

Реферат українською:

Об'єкт дослідження – процеси криптоперетворення інформації, які залишаються стійкими в умовах застосування для криптоаналізу квантових обчислень, теоретичне обґрунтування, аналіз, розробка, розвиток та стандартизація методів, механізмів, протоколів, комплексів та засобів КЗІ, які будуть застосовуватися для захисту інформації в постквантовому середовищі, в умовах інформаційних і гібридних війн. Предмет дослідження – методи, механізми, криптографічні протоколи, системи, комплекси та засоби КЗІ для застосування в постквантовому середовищі, в умовах інформаційних і гібридних війн. Мета роботи – підвищення національної безпеки держави в інформаційній сфері, забезпечення конфіденційності, цілісності та доступності державних інформаційних ресурсів, інформації з обмеженим доступом, зокрема тієї, що циркулює на об'єктах критичної інформаційної інфраструктури, забезпечення кібербезпеки в постквантовому середовищі в умовах ведення війн. Методи дослідження – методи криптоаналізу, методи математичного моделювання, методи комп'ютерного моделювання, методи експертних оцінок, асиметричні та симетричні криптографічні методи. Проект спрямовано на підвищення національної безпеки держави в інформаційній сфері, забезпечення конфіденційності, цілісності та доступності державних інформаційних ресурсів, інформації з обмеженим доступом, зокрема тієї, що циркулює на об'єктах критичної інформаційної інфраструктури, забезпечення кібербезпеки в пост-квантовому середовищі та в умовах ведення інформаційних і гібридних війн.

Реферат англійською:

The object of research is the processes of cryptotransformation of information that remain stable in terms of application of quantum computing for cryptanalysis, theoretical justification, analysis, development and standardization of methods, mechanisms, protocols, complexes and tools of comprehensive information protection, which will be used to protect information in the post-quantum environment, in terms of information and hybrid wars. The subject of research is methods, mechanisms, cryptographic protocols, systems, complexes and means of comprehensive information protection for application in the post-quantum environment. The purpose of the work is to increase the national security of the state in the information area, ensure the confidentiality, integrity and availability of state information resources, information with limited access, including that circulating in critical information infrastructure, cybersecurity in the post-quantum environment in war. Research methods are the methods of cryptanalysis, methods of mathematical modeling, methods of computer modeling, methods of expert evaluation, asymmetric and symmetric cryptographic methods. The project is aimed at improving the national security of the state in the information area, ensuring the confidentiality, integrity and accessibility of state information resources, information with limited access, including that circulating at critical information infrastructure, cybersecurity in the post-quantum environment and in the context of information and hybrid wars.

Індекс УДК: 004.7, УДК 004.056.055

Коди тематичних рубрик: 50.37.23

Керівники роботи

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

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Моделі порушника, моделі загроз та моделі безпеки стосовно криптографічних перетворень у пост-квантовий період

Назва НТП англійською: Malefactor models, threat models and security models regarding post-quantum cryptographic transformations;

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Запропоновано та досліджено моделі порушника, моделі загроз та моделі безпеки щодо криптографічних перетворень у пост-квантовий період, зокрема, асиметричних криптоперетворень (електронний підпис, направлене шифрування, інкапсуляція ключів, симетричне криптоперетворення, тощо). Розроблені моделі враховують умови та вимоги до перспективних криптоперетворень у випадку застосування зловмисниками квантових засобів криптографічного аналізу

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 01.2018

Закінчення етапу: 12.2020

Споживачі продукції: ХНУ імені В.Н.Каразіна, ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ПРАТ

Перспективні ринки: Заклади вищої освіти України

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:

Назва НТП українською: Методи та методика оцінки та порівняльного аналізу криптографічних перетворень у пост-квантовий період;

Назва НТП англійською: Methods and techniques of evaluation and comparative analysis of cryptographic transformations in the post-quantum period

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Розроблено методи та методика оцінки та порівняльного аналізу існуючих та пост-квантових криптографічних перетворень (електронного підпису, направлено шифрування, протоколів інкапсуляції ключів, симетричних криптоперетворень, тощо) у пост-квантовий період. Отримано та узагальнено результати аналізу стійкості існуючих методів та механізмів криптографічного захисту інформації у постквантовий період, обґрунтовано напрямки розвитку квантово-стійких криптографічних перетворень; досліджено питання розробки, аналізу та застосування різних сімейств квантово-стійких асиметричних та симетричних криптоперетворень.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 01.2018

Закінчення етапу: 12.2020

Споживачі продукції: ХНУ імені В.Н.Каразіна, ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ПРАТ

Перспективні ринки: Заклади вищої освіти України

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:

Назва НТП українською: Спеціальне математичне забезпечення стосовно оцінки криптографічної стійкості існуючих методів та механізмів криптографічного захисту інформації у пост-квантовий період;

Назва НТП англійською: Special mathematical support for assessing the cryptographic stability of existing methods and mechanisms of cryptographic information protection in the post-quantum period;

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Розроблено спеціальне математичне забезпечення стосовно оцінки криптографічної стійкості існуючих методів та механізмів криптографічного захисту інформації у пост-квантовий період. Практичне застосування отриманої продукції дозволило обґрунтувати суттєві переваги квантово-стійких криптоперетворень, побудованих, зокрема, на алгебраїчних решітках; на основі збиткових кодів; на мультіваріативних квадратичних перетвореннях; із застосуванням геш-функцій; на ізогеніях еліптичних кривих, на симетричних криптоалгоритмах.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 01.2018

Закінчення етапу: 12.2020

Споживачі продукції: ХНУ імені В.Н.Каразіна

Перспективні ринки:

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

Kuznetsov, O.O., Gorbenko, Y.I., Bilozertsev, I.M., Andrushkevych, A.V., Narizhnyi, O.P., 2018. ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. Telecommunications and Radio Engineering, vol. 77. <https://doi.org/10.1615/TelecomRadEng.v77.i4.30>

Gorbenko, I.D., Kachko, O.G., Yesina, M.V., 2018. ANALYSIS OF ASYMMETRIC NTRU PRIME IIT UKRAINE ENCRYPTION ALGORITHM WITH REGARDS TO KNOWN ATTACKS. Telecommunications and Radio Engineering, vol. 77. <https://doi.org/10.1615/TelecomRadEng.v77.i9.50>

Gorbenko, Y.I., Melnik, T.V., Gorbenko, I.D., 2018. ANALYSIS OF POTENTIAL POST-QUANTUM SCHEMES OF HASH-BASED DIGITAL SIGNATUR. Telecommunications and Radio Engineering, vol. 77. <https://doi.org/10.1615/TelecomRadEng.v77.i7.40>

Kuznetsov O. O. Algebraic immunity of non-linear blocks of symmetric ciphers / Kuznetsov O. O., Gorbenko Y. I., Bilozertsev I. M., Andrushkevych A. V., Narizhnyi O. P. //, 2018. Vol. 77. – Режим доступу: <https://doi.org/10.1615/TelecomRadEng.v77.i4.30>.

Горбенко І. Д. Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки / І. Д. Горбенко, С. О. Кандій, М. В. Єсіна, Є. В. Остряньська // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 57–63.

Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / Ю.І. Горбенко, М.В. Єсіна, В.В. Онопрієнко, Г.А. Малєєва // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 72–78

Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 5–28.

Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. G. Kachko, M. V. Yesina, I. V. Stelnik, S. O. Kandy, V. A. Bobukh, V. A. Ponomar // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 4 – P. 327-340. DOI: 10.1615/TelecomRadEng.v78.i4.40

Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Yesina // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 7 – P. 579–594. DOI: 10.1615/TelecomRadEng.v78.i7.30

Gorbenko I. D. Analysis of asymmetric NTRU Prime IIT Ukraine encryption algorithm with regards to known attacks / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Telecommunications and Radio Engineering, 2018. – Volume 77, Issue 9 – P. 799–816. DOI: 10.1615/TelecomRadEng.v77.i9.50.

Х. Заключні відомості

Керівник юридичної особи

Катрич Віктор Олександрович

Перелік осіб-виконавців

Єсіна Марина Віталіївна

(к. т. н.)

Ісірова Катерина Володимирівна

Гальцева Ірина Михайлівна

Горбенко Іван Дмитрович

(д. т. н.)

Горбенко Юрій Іванович

(к. т. н.)

Долгов Віктор Іванович

(д.т.н., 20.00.16)

Д'яченко Андрій Сергійович

Качко Олена Григорівна

(к. т. н.)

Колгатін Андрій Олександрович

Кошман Сергій Олександрович

(д. т. н.)

Краснобаєв Віктор Анатолійович

(д. т. н.)

Кіян Анастасія Сергіївна

Олешко Олег Іванович

(к.т.н.)

Полуяненко Микола Олександрович

(к.т.н.)

Пономар Володимир Андрійович

(к.т.н.)

Потій Олександр Володимирович

(д. т. н.)

Рассомахін Сергій Геннадійович

(д. т. н., 05.13.06)

Скриннік Володимир Андрійович

Седова Крістіна Володимирівна

Шевцов Олексій Володимирович

(к. т. н.)

Відповідальний за підготовку

Майстренко Людмила Олексіївна

облікових документів

Телефон

+38 (057) 707-55-23

Реєстратор

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

