

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0225U005087

Державний реєстраційний номер: 0121U114705

Особливі позначки: відкрита

Дата реєстрації: 25-12-2025

II. Етап виконання ДіР

Номер етапу: 5

Назва етапу: Розробка методів обробки інформації в різних теоретико-числових базисах, інформаційних моделей та компонентів кіберфізичних систем

Початок етапу: 01.2025

Закінчення етапу: 12.2025

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, буд. 11, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46009, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380352475051

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: проспект Перемоги, буд. 10, м. Київ, 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: 2.7 - інше

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2201390

Фактичний обсяг фінансування (тис. грн.): 344.700
--

VII. Відомості про ДіР

Назва роботи українською:

Виконання завдань Перспективного плану розвитку наукового напрямку "Технічні науки" Західноукраїнського національного університету

Назва роботи англійською:

Fulfillment of tasks of the Perspective plan of development of the scientific direction "Technical Sciences" of the West Ukrainian National University

Реферат українською:

Етап зосереджено на створенні постквантових криптосистем. Вперше розроблено асиметричний метод шифрування на основі криптосистеми МакЕліса та коригуючих кодів СЗК, який забезпечує значно менший розмір відкритого ключа (приблизно в 5 разів) при збереженні високої криптостійкості та можливості виправлення помилок під час розшифрування. Проведено теоретичну оцінку стійкості до відомих атак. Отримані результати вирізняються науковою новизною завдяки розробці оригінальних методів та алгоритмів. Вони мають важливе практичне значення, сприяючи підвищенню безпеки зберігання й обробки даних, зростанню ефективності систем підтримки прийняття рішень та прискоренню реагування на надзвичайні ситуації. Отримані результати можуть бути впроваджені в інформаційних системах державних установ і приватного сектору, а також у роботі служб надзвичайних ситуацій а також слугувати основою для подальших досліджень у галузі захищених інформаційних систем та штучного інтелекту.

Реферат англійською:

Stage concentrated on developing post-quantum cryptosystems. For the first time, an asymmetric encryption method based on the McEliece cryptosystem and error-correcting codes in the residue number system was developed. It features a substantially smaller public key (approximately five times smaller) compared to the classical McEliece system, while preserving high cryptographic strength and supporting error correction during decryption. A theoretical evaluation of resistance to known attacks was conducted. The obtained results exhibit scientific novelty through the development of original methods and algorithms and hold significant practical value by improving data security, enhancing the efficiency of decision-support systems, and accelerating emergency responses. These achievements can be implemented in information systems of public institutions and the private sector, as well as in emergency services operations, and serve as a solid foundation for further research in secure information technologies and artificial intelligence.

Індекс УДК: 004

Коди тематичних рубрик: 20.54

Керівники роботи

Власне Прізвище Ім'я По-батькові: Яцків Василь Васильович

Науковий ступінь: д. т. н.

Вчене звання: проф.

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Асиметричний метод шифрування

Назва НТП англійською: Asymmetric encryption method

НТП, яку передбачалося створити: Створено

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії, гіпотези, Методичні документи, Аналітичні матеріали

Галузь застосування: М 72 Наукові дослідження та розробки. КВЕД: 72.19 (для природничих та технічних наук)

Реєстраційний номер картки технології:

Опис НТП: Розроблено асиметричний метод шифрування на основі криптосистеми МакЕліса та коригуючих кодів СЗК, який забезпечує значно менший розмір відкритого ключа (приблизно в 5 разів) при збереженні високої криптостійкості та можливості виправлення помилок під час розшифрування. Проведено теоретичну оцінку стійкості до відомих атак.

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: 03.2025

Закінчення етапу: 12.2025

Споживачі продукції: Підприємства, установи та організації

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

Yatskiv, V., Kulyna, S., & Ivasiev, S. (2025). Data Encryption Method Based on the McEliece Cryptosystem and the Redundant Residue Number System. *Advances in Cyber-Physical Systems*. Vol. 10, No. 2, 2025, pp. 214-222.

<https://doi.org/10.23939/acps2025.02.214>

Yakymenko I., Kasianchuk, M., Martyniuk, O., & Martyniuk, S. (2025). A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing, 24(1), pp. 92-101.

<https://doi.org/10.47839/ijc.24.1.3880>

Kasianchuk, M., Shevchuk, R., Adamyk, B., Benson, V., Shylinska, I., & HOLEMBIOVSKYI, M. (2025). Affine Cipher Encryption Technique Using Residue Number System. Cryptography, 9(2), 26.

<https://doi.org/10.3390/cryptography9020026>

Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S., Martyniuk A., Yakymenko Y. A Symmetric Cryptoalgorithm in a Polynomial Hierarchical Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT., 2025, pp. 501-504. DOI: 10.1109/ACIT65614.2025.111858

T. Tsavolyk, P. Kasprowski, V. Yatskiv, A. Sachenko, I. Novosad. Zero-knowledge Proof Protocol based on the RRNS. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2025), 4-6 September, 2025, Gliwice, Poland, (Vol. 2, pp. 993-997)

Яцків В., Івас'єв С., Яцків Н. Криптосистема McEliece на основі коригуючих кодів системи залишкових класів. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. – С. 229 -231.

Х. Заключні відомості

Керівник юридичної особи

Крисоватий Андрій Ігорович
д. е. н., 08.00.08

Перелік осіб-виконавців

Давлетова Аліна Ярославівна

Комар Мирослав Петрович
(д. т. н., професор, 05.13.06)

Кіт Іван Романович

Тимчишин Василь Степанович

Цаволик Тарас Григорович
(к. т. н.)

Шпак Володимир Богданович

Відповідальний за підготовку облікових документів

Семанюк Віта Зеновіївна

Телефон

+380988340338

Реєстратор

Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Тетяна Анатоліївна