Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U005625

Особливі позначки: відкрита

Дата реєстрації: 11-11-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Стеценко Вадим Олегович
2. Vadym O. Stetsenko

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0008-5315-5539

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 17-12-2026

Спеціальність за освітою: Кібербезпека та захист інформації

Місце роботи здобувача: Стеценко Вадим Олегович

Код за ЄДРПОУ: 3367205917

Місцезнаходження: вул.Михайлівська б.7, Харків, Харківський р-н., 61019, Україна

Форма власності: Державна

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 17409

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56

Тема дисертації:

1. Метод підвищення автентичності даних в смарт технологіях

2. Smart technologies data authenticity increasing method

Реферат/анотація:

1. Стеценко В. О. Метод підвищення автентичності даних в смарт технологіях. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації (12 – Інформаційні технології). – Національний технічний університет “Харківський Політехнічний Інститут”, Харків, 2026. На підставі проведеного аналізу, результатів вивчення наукових публікацій за темою дослідження дисертацій, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об’єктивне протиріччя між криптосистемами на основі кодів / еліптичних кривих які не забезпечують необхідного рівня безпеки при коротких ключах та необхідністю розробки нових стійких гібридних криптосистем, що поєднують різні алгебраїчні підходи для уникнення вразливостей відомих класів атак. Вирішенню цього наукового завдання і присвячена дисертаційна робота. Об’єкт дослідження п процес забезпечення захисту

даних в смарт технологіях. Предмет дослідження – моделі та методи захисту даних в смарт технологіях за рахунок підвищення криптографічної стійкості системи. Метою дисертаційної роботи є підвищення криптографічної стійкості системи шляхом запобігання редукції системи до класичних задач (декодування кодів або дискретного логарифмування) та мінімізації витоку інформації про внутрішню організацію криптосхеми за рахунок розробки нової архітектури несиметричної криптосистеми, що поєднує алгебраїчні властивості лінійних блокових кодів та еліптичних кривих в єдину структуру зі спільним математичним фундаментом. Отримані результати дозволяють використання m-кодів як узагальненої основи для криптосистеми Мак-Еліса, що дозволяє гнучко адаптувати кодову структуру під різні вимоги безпеки, зберігаючи при цьому високий рівень обфускації та стійкості до статистичного аналізу, навіть у спрощених демонстраційних реалізаціях. Поєднання постквантової стійкості кодової криптографії з ефективністю симетричного шифрування (наприклад, AES) у гібридній архітектурі є перспективним напрямком для побудови криптографічних протоколів майбутнього, особливо в умовах загрози від квантових атак. Проведені експериментальні дослідження статистичної безпеки крипто-кодових конструкцій, побудованих на еліптичних кодах показали, що всі 189 статистичних тестів (згідно з методикою тестування NIST SP 800-22) несиметричні теоретико-кодові схеми, побудовані за еліптичним кривим успішно пройшли з критерієм 6 > 0. Крім того, 74 % тестів успішно пройшли за критерієм Pi > 0,99, що є найкращим результатом, порівняно з генератором BBS та алгоритмом блочного шифрування FIPS 197. У висновках дисертаційної роботи викладено основні результати які випливають із проведених досліджень, представлено та охарактеризовано показники ефективності при використанні запропонованих рішень. За результатами дослідження отримано такі наукові результати: – вперше запропоновано модель криптосистеми на основі комбінації лінійного блокового коду та еліптичної кривої, де параметри кривої та коду формуються через спільну алгебраїчну структуру, що ускладнює застосування стандартних методів криптоаналізу (наприклад, атак на основі декодування довільного коду або дискретного логарифмування). У роботі запропоновано формалізоване рівняння кривої у вигляді y2+a1xy+a3y=x3+a2x2+a4x+a6 та описано механізм її інтеграції з кодовою матрицею [n, k, d]; – набув подальшого розвитку алгоритм уніфікованого кодування / декодування криптограм, який одночасно використовує властивості еліптичної кривої та лінійного коду для забезпечення додаткового рівня приховування інформації. Це дозволяє зменшити ймовірність успішного аналізу шляхом розкладання системи на окремі компоненти, оскільки секретний ключ формується як комбінація матриці маскування X, перестановки P та діагональної матриці D, що відповідає принципу мінімального розголошення інформації про внутрішню структуру системи. – удосконалено механізм уніфікованого кодування / декодування криптограм, який реалізує принцип мінімального розголошення внутрішньої структури криптосистеми шляхом формування секретного ключа як композиції нетривіальних лінійних перетворень – маскування, перестановки та діагонального масштабування. Цей механізм не передбачає окремого виділення криптографічного та кодового шарів під час обробки даних, що суттєво ускладнює проведення атак на основі аналізу окремих компонент системи. Експериментальна верифікація підтвердила, що запропонований підхід забезпечує на 10–12 % вищу ефективність захисту цілісності, конфіденційності та автентичності даних порівняно з існуючими гібридними криптосхемами, що робить його перспективним для застосування в IoT-пристроях, розумних містах та інших смарт-середовищах;– вперше запропоновано постквантово стійку Challenge-Response автентифікаційну схему, засновану на гібридній крипто-кодовій конструкції, що поєднує алгеброгеометричний код над скінченним полем із механізмом формування інформаційної послід

2. Based on the analysis conducted, the results of the study of scientific publications on the topic of the study of theses, patents, monographs and practical developments, it was established that at the current stage of development of progressive information technologies there is an objective contradiction between cryptosystems based on codes / elliptic curves that do not provide the required level of security with short keys and the need to develop new stable hybrid cryptosystems that combine various algebraic approaches to avoid vulnerabilities of known classes of attacks. The dissertation is dedicated to solving this scientific problem. The object of research is the process of ensuring data protection in smart technologies. The subject of research is models and methods of data protection in smart technologies by increasing the cryptographic stability of the system. The goal of the

dissertation is to increase the cryptographic stability of the system by preventing the reduction of the system to classical tasks (decoding codes or discrete logarithmization) and minimizing the leakage of information about the internal organization of the cryptographic scheme by developing a new architecture of an asymmetric cryptosystem that combines the algebraic properties of linear block codes and elliptic curves into a single structure with a common mathematical foundation. The obtained results allow the use of m-codes as a generalized basis for the McAlice cryptosystem, which allows for flexible adaptation of the code structure to various security requirements, while maintaining a high level of obfuscation and resistance to statistical analysis, even in simplified demonstration implementations. The combination of post-quantum stability of code cryptography with the efficiency of symmetric encryption (e.g., AES) in a hybrid architecture is a promising direction for building cryptographic protocols of the future, especially in conditions of threat from quantum attacks. Experimental studies of the statistical security of crypto-code structures based on elliptic codes have shown that all 189 statistical tests (according to the NIST testing methodology) SP 800-22) asymmetric code-theoretic schemes built on an elliptic curve successfully passed with the criterion 6>0. In addition, 74 % of tests successfully passed according to the Pi>0.99, which is the best result compared to the BBS generator and FIPS block cipher algorithm 197. The practical implementation of the results obtained in the work consists in scientifically and methodologically ensuring data security in networks through unified encoding / decoding of cryptograms, which simultaneously uses the properties of an elliptic curve and a linear code to provide an additional level of information concealment. The presented scientifically based practical recommendations confirm the reliability of the proposed method of assessing stability and demonstrate an increase in protection efficiency by 10–12 % compared to existing approaches, which is a significant achievement in the context of resource -limited environments. Therefore, the research topic not only meets modern scientific and practical challenges, but also offers ways to systematically solve them through the integration of fundamental algebraic methods into a single stable cryptographic architecture. The lack of similar solutions in our country and abroad makes research results a priority. The directions of future research are to further improve the proposed methods for detecting external influences on data storage environments in smart technologies, which will reduce the overall impact of destabilizing factors of various kinds during the operation of such systems. Results works implemented in the curriculum process departments cybersecurity of NTU “KhPI” in the disciplines “Design and development of web applications” and “Development of web application interfaces”. Keywords: cryptosystem, computer system, information security, storage data, experimental research, defense data, information technologies, cybersecurity, cyber threats, cryptography, privacy, cryptanalysis, method, mathematical model, prediction, internet of things, network bandwidth, information system.

Державний реєстраційний номер ДіР: 0123U101018, 0123U10102, 0126U002562

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Стеценко В. О. Розробка методів автентифікації на основі модифікованих теоретико-кодових схем / Стеценко В. О. // Сучасний захист інформації, 2025. № 4(64). С. 155–164. (Б)
- Стеценко В. О. Метод побудови криптосистеми Нідеррайтера на основі m-кодів / Лаптєв О. А., Стеценко В. О. // Сучасний захист інформації, 2025. № 3(63). С. 83–90. (Б)
- Стеценко В. О. Метод виявлення небезпечних цифрових радіосигналів / Лаптєв О. А., Хохлачова Ю. Є., Лаптєва Т. О., Стеценко В. О., Лаптєв С. О. // Кібербезпека: освіта, наука, техніка, 2025. № 3(31). С. 620–634. (Б)

- Стеценко В. О. Метод побудови системи автентифікації в постквантових мережах на основі кодових криптосистем / Лаптєв О. А., Стеценко В. О. // Сучасний захист інформації, 2026. № 3(67). С. 156–163. (Б)
- Stetsenko V. Application of zero trust architecture (zero trust) to ensure the security of smart systems / Holdobin S., Milevskyi S., Kudriavtseva A., Zhyhalov M., Stetsenko V. // ScienceRise: innovative technologies in industry, 2025. Vol. 2, P. 29–38.
- Стеценко В. О. Метод побудови криптосистеми Мак-Еліса на основі m-кодів / Лаптєв О. А., Стеценко В. О. // Міжнар. наук.-техн. конф. “SMICS: Безпека сучасних інформаційно-комунікаційних систем”: матеріали збірка тез допов. учасник. Україна. – Львів: ЛНУ ім. І. Франка, 2025. – С. 260–266.
- Stetsenko V. Hardware Security Evaluation of IoT Microcontrollers: Threats and Countermeasures / Pohasii S., Tkach M., Holdobin S., Brynza N., Stetsenko V. // “2025 IEEE 6th KhPI Week on Advanced Technology, KhPIWeek 2025”: Conference Proceedings, Ukraine. – Kharkiv, 2025. – P. 1 – 6. (Scopus, Ukraine).
- Стеценко В. О. Метод підвищення автентичності данних в смарт технологіях / Стеценко В. О. // V Міжнар. наук.-практ. конф. “Інформаційна безпека та інформаційні технології”: матеріали збірка тез допов. учасник. Україна. – Харків – Одеса – Луцьк: НТУ “ХПІ”, 2025. – С. 49–50.
- Stetsenko V. Crypto Code Constructions in Post-Quantum Cryptography / Tkachov A., Korol O., Voropay N., Dunaiev S., Stetsenko V., Tomashevsky B. // 7th International Congress Human-Computer Interaction, Optimization and Robotic Applications (ICHORA): Conference Proceedings, Turkey. – Ankara, 2025. – P. 1 – 6. (Scopus, Turkey).
- Stetsenko V. Post-Quantum Authentication and Authorization Using the Niederreiter Code-Theoretic Scheme / Korolov R., Milevskyi S., Dunaiev S., Stetsenko V., Korol O., Voropay N. // 2025 9th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT): Conference Proceedings, Turkiye. – Ankara, 2025. – P. 1 – 4. (Scopus, Turkey).
- Stetsenko V. Development of the authentication method based on lightweight ciphers / Korolov R., Yevseiev S., Stetsenko V., Milevska T. // 8th International congress on 3D printing (additive manufacturing) “Technologies and digital industry”: Conference Proceedings, Turkey. – Antalya, 2024. – P. 505 – 524. (Scopus, Turkey).
- Stetsenko V. Method for reducing the frequency spectrum overlaying error in digital narrow-band filtration / Herasymov S., Soroka V., Milevskyi S., Korol O., Aksonova I., Stetsenko V. // 6th International Congress “Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)”: Conference Proceedings, Turkey. – Istanbul, 2024. – P. 1 – 5. (Scopus, Turkey).
- . Стеценко В. О. Розробка алгоритму автентифікації на основі крипто-кодової конструкції Мак-Еліса. / Дунаєв С. В., Стеценко В. О. // XIII Міжнар. наук.-техн. конф. “ITSec: Безпека інформаційних технологій”: збірка тез допов. учасник. Україна. – Львів: ЛНУ ім. І. Франка, 2024. – С. 90–91.

Наукова (науково-технічна) продукція: технології; методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U101018, 0123U10102, 0126U002562

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Мілевський Станіслав Валерійович

2. STANISLAV V. MILEVSKYI

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0001-5087-7036

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Лаптєв Олександр Анатолійович

2. Oleksandr Laptiev

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-4194-402X

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович

2. Oleksii A. Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація: https://scholar.google.com.ua/citations?user=-eNGlFoAAAAJ&hl

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна

2. Nadiia Kazakova

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3968-4094

Додаткова інформація:

Повне найменування юридичної особи: Одеський національний економічний університет

Код за ЄДРПОУ: 02071079

Місцезнаходження: вул. Преображенська, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Заковоротний Олександр Юрійович

2. Oleksandr Y. Zakovorotniy

Кваліфікація: д. т. н., професор, 05.13.07

Ідентифікатор ORCID ID: 0000-0003-4415-838X

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57201613700; https://www.webofscience.com/wos/author/record/812476; https://scholar.google.com.ua/citations?user=4ZtccWsAAAAJ&hl=ua

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Шматко Олександр Віталійович

2. Oleksandr Shmatko

Кваліфікація: к. т. н., доц., 01.05.02

Ідентифікатор ORCID ID: 0000-0002-2426-900X

Додаткова інформація: Профіль у Scopus: https://www.scopus.com/authid/detail.uri?authorId=6602623478; Профіль у Google Scholar: https://scholar.google.com.ua/citations?user=Wyv6ESUAAAAJ&hl; Профіль у WoS: https://www.webofscience.com/wos/author/record/M-7366-2017

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Кучук Георгій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Кучук Георгій Анатолійович
Відповідальний за підготовку облікових документів	Гаврилова Алла Андріївна
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна