# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0425U000034

**Особливі позначки:** відкрита

**Дата реєстрації:** 12-02-2025

**Статус:** Запланована

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Жолубак Іван Михайлович

2. Ivan M. Zholubak

**Кваліфікація:**

**Ідентифікатор ORCID ID:** 0000-0001-8871-7222

**Вид дисертації:** кандидат наук

**Аспірантура/Докторантура:** так

**Шифр наукової спеціальності:** 05.13.05

**Назва наукової спеціальності:** Комп'ютерні системи та компоненти

**Галузь / галузі знань:** Не застосовується

**Освітньо-наукова програма зі спеціальності:** Не застосовується

**Дата захисту:** 28-03-2025

**Спеціальність за освітою:** комп’ютерна інженерія

**Місце роботи здобувача:** Національний університет "Львівська політехніка"

**Код за ЄДРПОУ:** 02071010

**Місцезнаходження:** вул. Степана Бандери, буд. 12, Львів, 79013, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## III. Відомості про організацію, де відбувся захист

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** Д 35.052.18

**Повне найменування юридичної особи:** Національний університет "Львівська політехніка"

**Код за ЄДРПОУ:** 02071010

**Місцезнаходження:** вул. Степана Бандери, буд. 12, Львів, 79013, 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 університет "Львівська політехніка"

**Код за ЄДРПОУ:** 02071010

**Місцезнаходження:** вул. Степана Бандери, буд. 12, Львів, 79013, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## V. Відомості про дисертацію

**Мова дисертації:** Українська

**Коди тематичних рубрик:** 50.33.33, 50.09, 27.17.27

### Тема дисертації:

1. Методи та засоби створення реконфігурованих вузлів криптографічного захисту інформації для кібер-фізичних систем

2. The methods and tools for creating reconfigurable units for cryptographic data protection in cyber-physical systems

### Реферат:

1. У дисертації розв'язується важливе науково-технічне завдання створення реконфігурованих вузлів КЗІ на основі ЕК, які оперують у КФС елементами розширених полів Галуа GF(p^n), де p > 2 – просте число, конфігурована характеристика поля, та n – порядок утворюючого поле полінома, степінь поля над його простим підполем. Проаналізовано апаратні витрати при реалізації таких систем у розширених полях Галуа GF(p^n) з різною характеристикою p та порядком n утворюючого поле полінома. Запропоновано помножувач елементів таких полів Галуа на основі модифікованої комірки Гілда (МКГ). Запропоновано 3 структури створення МКГ. Наведено порівняння їх апаратних витрат. Програмне виконання операцій над елементами розширених полів Галуа GF(p^n) має більшу трудоємність, у порівнянні з GF(2^m) та забезпечує більшу стійкість до злому. Апаратна реалізація реконфігурованих вузлів КЗІ забезпечує ще більшу криптографічну стійкість засобів КЗІ. За елементну базу для створення вузлів КЗІ у складі КФС у роботі було

обрано програмовані логічні інтегральні схеми (ПЛІС). Для генерації VHDL-описів вузлів КЗІ, що працюють з використанням розширених полів Галуа GF(p^n), для їхньої наступної реалізації у ПЛІС було розроблено мовою С++ програми-генератори ядер помножувачів елементів розширених полів Галуа. У роботі розглянуто сучасний стан та перспективи розвитку засобів та методів створення реконфігурованих вузлів КЗІ, методи створення реконфігурованих вузлів КЗІ для КФС, загальну методику проведення дисертаційних досліджень, описано вимоги до створення реконфігурованих вузлів КЗІ, обгрунтовано доцільність створення паралельних помножувачів елементів розширених полів Галуа GF(p^n) та запропоновано методи створення таких помножувачів. Вдосконалено методи оцінки часової та апаратної складностей та запропоновано метод тестування генераторів ядер таких помножувачів. Також описано процес розробки засобів створення (генераторів ядер) помножувачів елементів розширених полів Галуа GF(p^n) для вузлів КЗІ КФС, проведено дослідження створених в ході виконання роботи операційних вузлів (помножувачів) для полів Галуа, які застосовуються у криптографічних засобах захисту інформації на базі ЕК. Отримані, під час виконання дисертаційної роботи, наукові результати створюють методологічну базу для розробки вузлів КЗІ, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ, які працюють з використанням ЕК та розширених полів Галуа.

2. In the dissertation, an important scientific and technical task of creating reconfigurable units for cryptographic information security (CIS) systems based on elliptic curves, which operate in cyber-physical systems with elements of extended Galois fields GF(p^n), where p > 2 is a prime number, the configured characteristic of the field, and n is the order of the field-generating polynomial, the degree of the field over its prime subfield, is addressed. The hardware costs of implementing such systems in extended Galois fields GF(p^n) with various characteristics p and orders n of the field-generating polynomial are analyzed. A multiplier of elements for such Galois fields based on a modified Guild cell (MGC) is proposed. Three structures for creating MGC are proposed. A comparison of their hardware costs is provided. Software execution of operations over elements of extended Galois fields GF(p^n) is more labor-intensive compared to GF(2^m) and provides greater resistance to cracking. The hardware implementation of reconfigurable units provides even greater cryptographic robustness of CIS devices. FPGA were chosen as the elemental base for creating units in cyber-physical systems in the study. For generating VHDL descriptions of units that operate using extended Galois fields GF(p^n) for their subsequent implementation in FPGA, C++ programs-generators of multiplier cores of elements of extended Galois fields were developed. The paper examines the current state and prospects for the development of tools and methods for creating reconfigurable units for CIS systems, considers methods for creating reconfigurable units for CIS systems, the general methodology for conducting dissertation research, the requirements for creating reconfigurable units, the rationale for creating parallel multipliers of elements of extended Galois fields GF(p^n), and methods for creating such multipliers. Methods for assessing time and hardware complexities were improved, and a method for testing the generators of cores of such multipliers was proposed. The process of developing tools (core generators) for multipliers of extended Galois field elements GF(p^n) for cryptographic system units (CIS) is also described. Research has been conducted on the operational units (multipliers) for Galois fields developed during the work, which are used in cryptographic information protection tools based on elliptic curves. The scientific results obtained during the dissertation work create a methodological base for developing CIS units, which allow enhancing the reliability, authenticity, and security of modern hardware CIS devices that operate using elliptical curves and extended Galois fields.

### Державний реєстраційний номер ДіР:

**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:

- В.С. Глухов, І.М. Жолубак, Мохаммед Кадім Рахма Рахма. Принципи побудови та проектування операційних вузлів для полів Галуа, що використовуються в задачах криптографічного захисту інформації на основі еліптичних кривих. Кіберфізичні системи: багаторівнева організація та проектування [Текст]: монографія – А.О. Мельник та інші. За редакцією професора А. О. Мельника. Львів: «Магнолія 2006», 2019. 238 с. С. 58- 131.
- Elias, R., Hlukhov, V., Rahma, M., Zholubak, I. Hardware Components for Post-Quantum Elliptic Curves Cryptography // Advanced Computer Information Technologies (ACIT 2018), Ceske Budejovice, Czech Republic, June 1–3, 2018. P. 236–239. (Scopus).
- Zholubak, I., Rahma, M. K., Hlukhov, V. Automation System for Configuration of Cryptographic Data Protection Unit Model // Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018), in frameworks of the 14th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2018), Kyiv, Ukraine, May 14–17, 2018. С. 700–707. (Scopus).
- Zholubak, I.M., Hlukhov, V.S. Galua Field Multipliers Core Generator. International Journal of Computer Network and Information Security, 2023. – Vol. 3. – Pp. 1–14. DOI: 10.5815/ijcnis.2023.03.01, (Scopus).
- Rahma, M., Zholubak, I., Hlukhov, V. Devices for multiplicative inverse calculation in binary Galois fields // The 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2018), Kyiv, Ukraine, 24–27 May 2018. P. 275–278. (Scopus).
- Zholubak, I.M., Hlukhov, V.S. Comparison of hardware complexity of multipliers GF(pm). In Proceedings of the 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2023. – Pp. 812–816. Dortmund, Germany. DOI: 10.1109/IDAACS-SWS50031.2020.9297059, (Scopus).
- Zholubak, I.M., Hlukhov, V.S. Verification of Synthesized by the IP-core Generator Multipliers of Extended Galois Fields GF(pn) Elements. In Proceedings of the 13th International Conference Dependable Systems, Services and Technologies (DESSERT), 2023. – Athens, Greece, (Scopus).
- Zholubak, I.M., Hlukhov, V.S. Validation of Multipliers for Elements of Extended Galois Fields GF(pn) and Multipliers IP-core Generator. In Proceedings of the 18th IEEE International Conference on Computer Science and Information Technologies (CSIT), 2023. – Lviv, Ukraine, (Scopus).
- В.С. Глухов, І.М. Жолубак, А.Т. Костик. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі. Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі", № 830. Львів, 2015. С. 33 – 39.
- Жолубак І. М., Глухов В.С. Визначення розширеного поля Галуа GF(dm) з найменшою апаратною складністю помножувача. Вісник Національного університету «Львівська політехніка» "Інформаційні системи та мережі", № 854. Львів, 2016. С. 63 – 69.
- Жолубак І. М., Глухов В. С. Апаратні витрати помножувачів полів Галуа GF(dm) з великою основою. Вісник Національного університету «Львівська політехніка» "Комп'ютерні науки та інформаційні технології", № 864. Львів, 2017. С. 77 – 82.
- Жолубак І. М., Глухов В. С. Реалізація у ПЛІС помножувачів елементів полів Галуа високих порядків. Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 881. Львів, 2017. С. 41 – 47.
- Hlukhov, V., Kostyk, A., Zholubak, I., Rahma, M. Galois Fields Elements Processing Units for Cryptographic Data Protection in Cyber-Physical Systems // Advances in Cyber-Physical Systems. 2017. V. 2. № 2. P. 47–53.
- Родріг Еліас, Валерій Глухов, Мохаммед Рахма, Іван Жолубак. Ємнісна складність та вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа. Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 29(105), с. 95 – 102.

- Р.М. Еліас, В.С. Глухов, М. Рахма, І.М. Жолубак. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа. Вісник Національного університету «Львівська політехніка» “Комп’ютерні системи та мережі”, № 905. Львів, 2018. С. 64 – 72.
- Жолубак І. М., Курман П. В. Система безконтактних платежів на основі технології NFC. Науковий журнал «Комп’ютерні системи та мережі», № 1. Львів, 2022. С. 28 – 37, DOI: https://doi.org/10.23939/csn2022.01.028
- Жолубак І. М., Матвієць В. Ю. Трекер для сонячних електростанцій. Науковий журнал «Комп’ютерні системи та мережі», № 1. Львів, 2022. С. 37 – 46, DOI: https://doi.org/10.23939/csn2022.01.037
- Bohdan Marii, Ivan Zholubak. Features of Development and Analysis of REST Systems. Advances in Cyber-Physical Systems. Volume 7. Number 2. Lviv Polytechnic National University. 2022. pp. 121 – 129, DOI: https://doi.org/10.23939/acps2022.02.121
- Жолубак І. М., Аналіз алгоритмів множення в полях Галуа для криптографічного захисту інформації. Вісник Національного університету «Львівська політехніка» “Інформаційні системи та мережі”, № 13. Львів, 2023. С. 338 – 349, DOI: https://doi.org/10.23939/sisn2023.13.338
- Kostyk, A., Zholubak, I. Features of multiplication execution of operations in binary and ternary Galois fields // 5th International Youth Science Forum LITTERIS ET ARTIBUS 2015, Lviv, Ukraine, November 26–28, 2015.
- В.С. Глухов, І.М. Жолубак. Порівняння апаратних витрат помножувачів елементів розширених полів Галуа. 17-а міжнародно науково-практична конференція «Сучасні інформаційні та електронні технології» Одеса, Україна, 23—27 травня 2016 р. С. 133 – 134.
- І.М. Жолубак, В.С. Глухов. Визначення розширеного поля Галуа GF(dm) з найменшою апаратною складністю помножувача. Інформаційні технології та комп’ютерне моделювання: матеріали статей Міжнародної науково-практичної конференції, 23 – 28 травня 2016 року. - Івано-Франківськ. 2016. С. 80 - 81.
- Глухов В.С., Жолубак І.М. Дослідження апаратної складності помножувачів елементів розширених полів Галуа GF(dm). Другий науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р. Матеріали Другого наукового семінару, с. 98 – 105.
- Kostyk, A., Zholubak, I. The research of the binary codes program complication and application in cyber-physical systems // 6th International Youth Science Forum LITTERIS ET ARTIBUS 2016, Computer Science & Engineering (CSE-2016), Lviv, Ukraine, November 24–26, 2016.
- Zholubak, I., Hlukhov, V. Research Hardware Complexity of Multipliers of Extended Galois Field GF(dm) // 6th International Youth Science Forum LITTERIS ET ARTIBUS 2016, Computer Science & Engineering (CSE-2016), Lviv, Ukraine, November 24–26, 2016.
- Zholubak, I., Hlukhov, V. Hardware complexity of multipliers of extended Galois field in FPGA // 7th International Youth Science Forum LITTERIS ET ARTIBUS 2017, Computer Science & Engineering (CSE-2017), Lviv, Ukraine, November 23–25, 2017. P. 420–421.
- Zholubak, I., Rahma, M., Hlukhov, V. Automation system program models configuration of cryptography cells in cyber-physical systems // 14th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2018), Kyiv, Ukraine, May 14–17, 2018. P. 669–679.
- Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. FPGA Cores for Fast Multiplicative Inverse Calculation in Galois Fields. Міжнародна науково-практична конференція «Електротехнічні та комп’ютерні системи: Теорія та практика» ЕЛТЕКС – 2018. м. Одеса, 29 травня - 1 червня 2018. Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 27(103), с. 227-233.

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

**Соціально-економічна спрямованість:** забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг; створення реконфігурованих вузлів криптографічного захисту

інформації

**Охоронні документи на ОПІВ:**

**Впровадження результатів дисертації:** Впроваджено

**Зв'язок з науковими темами:** 0115U000446

## VI. Відомості про наукового керівника/керівників (консультанта)

**Власне Прізвище Ім'я По-батькові:**

1. Глухов Валерій Сергійович

2. Valeriy Hlukhov

**Кваліфікація:** д.т.н., професор, 05.13.05

**Ідентифікатор ORCID ID:** 0000-0002-0542-7447

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний університет "Львівська політехніка"

**Код за ЄДРПОУ:** 02071010

**Місцезнаходження:** вул. Степана Бандери, буд. 12, Львів, 79013, 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. Возна Наталія Ярославівна

2. Nataliia Vozna

**Кваліфікація:** д.т.н., професор, 05.13.05

**Ідентифікатор ORCID ID:** 0000-0002-8856-1720

**Додаткова інформація:**

**Повне найменування юридичної особи:** Західноукраїнський національний університет

**Код за ЄДРПОУ:** 33680120

**Місцезнаходження:** вул. Львівська, буд. 11, Тернопіль, Тернопільський р-н., 46009, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Власне Прізвище Ім'я По-батькові:**

1. Кльоц Юрій Павлович

2. Yuri Clots

**Кваліфікація:** к.т.н., доц., 05.13.13

**Ідентифікатор ORCID ID:** 0000-0002-3914-0989

**Додаткова інформація:**

**Повне найменування юридичної особи:** Хмельницький національний університет

**Код за ЄДРПОУ:** 02071234

**Місцезнаходження:** вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Рецензенти**

## VIII. Заключні відомості

| | |
|---|---|
| **Власне Прізвище Ім'я По-батькові голови ради** | Дудикевич Валерій Богданович |
| **Власне Прізвище Ім'я По-батькові головуючого на засіданні** | Дудикевич Валерій Богданович |
| **Відповідальний за підготовку облікових документів** | Мичуда Леся Зиновіївна |
| **Реєстратор** | УкрІНТЕІ |
| **Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності** | Юрченко Тетяна Анатоліївна |