ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації
НАУМЕНКА СЕРГІЯ ВАСИЛЬОВИЧА
на тему: «Метод та моделі захисту інформації для кіберфізичних систем з обмеженими ресурсами»
для здобуття ступеня доктора філософії
за спеціальністю 123 – Комп'ютерна інженерія

Публічна презентація наукових результатів дисертації Науменка Сергія Васильовича відбулася на засіданні кафедри інформаційної безпеки та комп'ютерної інженерії (далі – ІБКІ) Черкаського державного технологічного університету (далі – ЧДТУ) 7 квітня 2026 року, протокол № 16.

ПРИСУТНІ:
Лавданський А.О., завідувач кафедри ІБКІ, к.т.н., доцент;
Бабенко В.Г., професор кафедри ІБКІ, д.т.н., професор;
Гресько С.О., ст. викладач кафедри ІБКІ;
Миронець І.В., доцент кафедри ІБКІ, к.т.н., доцент;
Миронюк Т.В., доцент кафедри ІБКІ, к.т.н., доцент;
Нечипоренко О.В., доцент кафедри ІБКІ, к.т.н., доцент;
Розломій І.О., доцент кафедри ІБКІ, к.т.н., доцент;
Скуцький А.Б., старший викладач кафедри ІБКІ, доктор філософії;
Тазетдінов В.А., доцент кафедри ІБКІ, к.т.н., доцент;
Фауре Е.В., професор кафедри ІБКІ, д.т.н., професор;
Федоров Є.Є., професор кафедри ІБКІ, д.т.н., професор;
Чепинога А.В., доцент кафедри ІБКІ, к.т.н., доцент;
Рудаков К.С., доцент кафедри ІБКІ, к.т.н., доцент;
Бондар В.В., асистент кафедри ІБКІ;
Коробейник Ю.О., асистент кафедри ІБКІ;
Трембовецький Р.С., асистент кафедри ІБКІ;
Науменко С.В., здобувач ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» 4-го року навчання.

Тему дисертації «Метод та моделі захисту інформації для кіберфізичних систем з обмеженими ресурсами» затверджено на засіданні вченої ради факультету інформаційних технологій і систем 31 березня 2026 року (протокол № 11). Науковий керівник: к.т.н., доцент Розломій Інна Олександрівна –

призначений наказом Черкаського державного технологічного університету від 21 березня 2026 року № 70/03-03.

1. Актуальність теми дослідження.

Актуальність дослідження зумовлена стрімким розвитком кіберфізичних систем (КФС) та Інтернету речей, які широко впроваджуються у промисловості, медицині, енергетиці, транспорті та інших критично важливих сферах. Зростання кількості взаємопов'язаних вбудованих пристроїв і сенсорних вузлів супроводжується підвищенням рівня кіберзагроз, що спрямовані на порушення конфіденційності, цілісності та доступності даних.

Особливістю таких систем є функціонування їх компонентів в умовах обмежених обчислювальних ресурсів, пам'яті та енергоспоживання, а також необхідність забезпечення обробки даних у реальному часі. Це суттєво ускладнює використання традиційних криптографічних механізмів, які не враховують специфіку вбудованих середовищ та можуть призводити до зниження продуктивності системи або перевищення допустимих енергетичних витрат.

Крім того, сучасні кіберфізичні системи характеризуються динамічною топологією, розподіленою архітектурою та активним використанням edge/fog-обчислень, що потребує побудови комплексних підходів до захисту інформації на різних рівнях – від сенсорних модулів і вбудованих пристроїв до мережевої взаємодії між компонентами. Існуючі рішення не забезпечують достатньої адаптивності до змін умов функціонування та ресурсних обмежень, що зумовлює необхідність розробки нових методів і моделей криптографічного захисту.

Дисертаційне дослідження спрямоване на розв'язання науково-прикладної задачі підвищення ефективності захисту інформації в кіберфізичних системах та IoT-середовищах в умовах обмежених обчислювальних ресурсів. Досягнення цього забезпечується шляхом розробки методу та моделей, що враховують особливості обміну даними, динамічність архітектур типу edge/fog та використання механізмів захищеного завантаження, що у сукупності сприяє підвищенню рівня захищеності сучасних інформаційних технологій.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, результати яких представлено в дисертаційній роботі, відповідають пріоритетному напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології» та його тематичному напряму «Кіберфізичні системи. Інтернет речей. Робототехніка» і виконувалися відповідно до програм і планів науково-дослідних робіт Черкаського національного університету імені Богдана Хмельницького, у тому числі в рамках науково-дослідної теми «Технічне і програмне забезпечення новітніх

комп'ютерних інформаційних систем» (номер державної реєстрації 0126U001916), у якій автор брав участь як виконавець.

Метою дисертаційної роботи є підвищення ефективності захисту інформації у компонентах кіберфізичних систем шляхом розробки методу та моделей, адаптованих до умов обмежених обчислювальних ресурсів, з урахуванням особливостей обміну даними та захищеного завантаження в архітектурах типу edge/fog.

Досягнення означеної мети передбачає виконання наступних завдань:

1. Удосконалити модель захисту інформації на рівні вбудованих пристроїв та сенсорних модулів, яка включає механізми захищеного завантаження, вибору та інтеграції криптографічних алгоритмів, а також управління ключами.
2. Побудувати модель захисту інформаційного обміну між компонентами КФС, включаючи протидію атакам на канали передавання, механізми шифрування, автентифікації та захисту від повторної передачі.
3. Удосконалити модель динамічного розподілу криптографічного навантаження між компонентами кіберфізичної системи та периферійними обчисленнями (edge/fog) з урахуванням стану ресурсів, характеристик каналів зв'язку та вимог до безпеки інформаційного обміну.
4. Розвинути метод побудови комплексної системи криптографічного захисту інформації у компонентах кіберфізичних систем на основі інтеграції механізмів захищеного завантаження, адаптивного вибору полегшених криптографічних алгоритмів та організації захищеного інформаційного обміну з урахуванням обмежених обчислювальних ресурсів.
5. Оцінити ефективність запропонованого методу у програмно-апаратному середовищі з використанням мікроконтролера STM32 за визначеними метриками та порівняння з існуючими криптографічними рішеннями.

Для аналізу архітектур КФС і класифікації загроз застосовано методи теорії інформації, теорії систем, системного аналізу та ризик-орієнтованого моделювання. Для розробки моделей захисту на рівні сенсорних вузлів і вбудованих пристроїв із забезпеченням захищеного завантаження використано методи дискретної математики, теорії графів, математичної логіки, формальних мов і автоматів, а також апаратно-програмного моделювання. Для побудови моделі захищеного інформаційного обміну застосовано методи криптографічного аналізу, теорії мережевої безпеки, протоколів автентифікації та аналізу атак. Для формування комплексного методу захисту використано методи комбінаторної оптимізації, математичного моделювання, теорії алгоритмів і аналізу енергоспоживання. Для оцінювання ефективності

запропонованих рішень і їх реалізації у середовищі FreeRTOS на платформі STM32 застосовано методи експериментального дослідження, статистичного аналізу, теорії ймовірності і математичної статистики та об'єктно-орієнтованого програмування.

Об'єктом дослідження є процеси криптографічного захисту інформації у компонентах кіберфізичних систем, функціонування яких відбувається в умовах обмежених обчислювальних ресурсів.

Предмет дослідження – методи, моделі та алгоритми криптографічного захисту інформації, що реалізуються на рівні сенсорних модулів, вбудованих пристроїв та каналів взаємодії між компонентами кіберфізичних систем.

2. Формулювання наукового завдання, нове розв'язання якого отримано в дисертації.

У дисертаційній роботі вирішено науково-технічну задачу підвищення ефективності криптографічного захисту інформації у компонентах кіберфізичних систем та IoT-середовищ з обмеженими обчислювальними ресурсами шляхом розробки сукупності взаємопов'язаних моделей і узагальненого методу їх інтеграції. Зокрема, розроблено модель захисту інформації на рівні сенсорних вузлів і вбудованих пристроїв, що забезпечує перевірку цілісності та автентичності програмного коду і реалізацію механізмів захищеного завантаження; модель захищеного інформаційного обміну між компонентами системи, орієнтовану на протидію атакам у мережевому середовищі та забезпечення конфіденційності і цілісності даних; а також модель динамічного розподілу криптографічного навантаження, яка дозволяє адаптивно обирати місце виконання криптографічних операцій залежно від ресурсного стану вузлів. На основі зазначених моделей сформовано метод побудови комплексної системи криптографічного захисту, який передбачає їх узгоджену інтеграцію та адаптивний вибір криптографічних механізмів з урахуванням обмежень продуктивності, енергоспоживання та вимог до часу обробки даних.

3. Наукові положення, розроблені особисто дисертантом, їхня новизна.

Дисертаційне дослідження містить у собі наступні наукові положення, розроблені особисто дисертантом:

– *вперше побудовано* модель криптографічного захисту інформаційного обміну між компонентами кіберфізичних систем, яка базується на використанні ресурсоощадних криптографічних механізмів встановлення захищеного каналу зв'язку та засобів протидії атакам повторної передачі, що забезпечує конфіденційність і цілісність даних у децентралізованих архітектурах типу edge/fog з урахуванням динамічної топології та обмежених ресурсів вузлів;

– *удосконалено* модель захисту інформації на рівні сенсорних модулів і вбудованих пристроїв, яка, на відміну від існуючих підходів, поєднує механізми захищеного завантаження, контролю цілісності програмного коду та керування криптографічними ключами з урахуванням обмежень обчислювальних ресурсів, що підвищує стійкість до атак на етапі ініціалізації системи;

– *удосконалено* модель динамічного розподілу криптографічного навантаження між компонентами КФС та периферійними обчисленнями, яка на основі узагальненої функції вартості та обмежень за енергоспоживанням, затримками й доступними ресурсами забезпечує адаптивний вибір між локальним і делегованим виконанням криптографічних операцій;

– *набув подальшого розвитку* метод побудови комплексної системи криптографічного захисту інформації у компонентах КФС, який передбачає інтеграцію механізмів захищеного завантаження, адаптивного вибору полегшених криптографічних алгоритмів та організації захищеного інформаційного обміну, що забезпечує ефективне функціонування систем в умовах обмежених обчислювальних ресурсів.

4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Наукові положення, висновки та рекомендації дисертаційної роботи є достатньо обґрунтованими. Обґрунтованість отриманих теоретичних результатів базується на використанні методів теорії інформації, теорії систем, криптографічного аналізу, теорії алгоритмів, дискретної математики, теорії ймовірності та математичної статистики, а також методів моделювання складних систем.

Для підтвердження сформульованих наукових положень здобувачем проведено експериментальні дослідження у програмно-апаратному середовищі з використанням мікроконтролерної платформи STM32. Реалізацію алгоритмів здійснено в середовищі FreeRTOS та в автономному режимі виконання програм без застосування операційної системи.

Експериментальні результати підтвердили працездатність і ефективність розробленої моделі захисту на рівні вбудованих пристроїв, зокрема забезпечення перевірки цілісності та автентичності програмного коду при обмежених ресурсах. Для моделі захищеного інформаційного обміну підтверджено забезпечення стабільної передачі даних із низькими затримками та стійкістю до атак у динамічних мережевих умовах. Для моделі динамічного розподілу криптографічного навантаження доведено можливість зниження обчислювального навантаження та оптимізації використання ресурсів за рахунок адаптивного вибору місця виконання криптографічних операцій.

Отримані результати в цілому підтверджують ефективність запропонованого методу інтеграції моделей, що забезпечує зменшення енергоспоживання, підвищення продуктивності та стабільності функціонування кіберфізичних систем в умовах обмежених ресурсів.

5. Рівень теоретичної підготовки здобувача, його особистий внесок у розв'язання конкретного наукового завдання. Рівень обізнаності здобувача з результатами наукових досліджень інших учених.

Дисертантом виконано ґрунтовне дослідження предметної області захисту інформації в кіберфізичних системах та IoT-середовищах. У роботі проаналізовано сучасні підходи до забезпечення конфіденційності, цілісності та автентичності даних у вбудованих пристроях і розподілених системах, а також особливості організації захищеного інформаційного обміну між компонентами, функціонування edge/fog-архітектур і механізмів розподілу та делегування криптографічного навантаження.

На основі опрацювання значної кількості наукових джерел, зокрема публікацій, індексованих у міжнародних наукометричних базах, автором враховано сучасні досягнення у сфері полегшеної криптографії, мережевої безпеки, вбудованих систем та розподілених обчислень. Отримані результати свідчать про високий рівень теоретичної підготовки здобувача в галузі інформаційних технологій, комп'ютерної інженерії, криптографії та математичного моделювання, а також про його вагомий особистий внесок у розв'язання поставленого наукового завдання.

6. Наукове та практичне значення роботи.

Наукове значення роботи полягає у подальшому розвитку методів і моделей криптографічного захисту інформації в кіберфізичних системах за рахунок урахування обмежених обчислювальних ресурсів, енергоспоживання та динамічної топології. Запропоновано комплекс взаємопов'язаних моделей захисту на рівні вбудованих пристроїв, інформаційного обміну та розподілу криптографічного навантаження, а також узагальнений метод їх інтеграції в єдину систему, орієнтовану на багаторівневу архітектуру з використанням edge/fog-обчислень.

Практичне значення одержаних результатів полягає у можливості їх застосування при проєктуванні систем захисту інформації у вбудованих пристроях, сенсорних мережах та IoT-системах. Експериментальні дослідження показали, що застосування запропонованих підходів дозволяє зменшити енергоспоживання криптографічних операцій у середньому на 23%, знизити обчислювальне навантаження на 35–40% та підвищити продуктивність системи на 20–25% порівняно з традиційними рішеннями. При цьому забезпечується перевірка цілісності програмного коду за час до 120 мс для прошивок обсягом

до 128 КБ із використанням не більше 5 КБ оперативної пам'яті, а також організація захищеного обміну даними із затримкою до 1,4 мс у мережах із динамічною топологією.

7. Використання результатів роботи.

Результати дисертаційного дослідження можуть бути використані у процесі проєктування та впровадження систем криптографічного захисту інформації в кіберфізичних системах та IoT-пристроях, зокрема у медичних вбудованих системах, промислових контролерах та периферійних обчислювальних платформах. Отримані результати доцільно застосовувати в освітньому процесі закладів вищої освіти при викладанні дисциплін з кібербезпеки, криптографії та комп'ютерної інженерії, а також при розробці нових і вдосконаленні існуючих програмно-апаратних рішень для захисту інформації в умовах обмежених ресурсів.

8. Повнота викладу матеріалів дисертації.

За матеріалами дисертаційного дослідження опубліковано 44 наукові праці, в тому числі 19 наукові статті, що входять до наукометричних баз даних Scopus та/або Web of Science, 10 статей у наукових виданнях, що входять до переліку фахових видань України, 3 розділах колективних монографій, 12 доповідях на науково-практичних конференціях.

Повний перелік наукових публікацій:

1. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. *Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023)*. 2023. P. 145–146. URL: https://ceur-ws.org/Vol-3609/paper12.pdf **(Scopus)**
2. Rozlomii I., Yarmilko A., Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. *Proceedings of the 4th Edge Computing Workshop (DOORS 2024)*. 2024. Vol. 3666. P. 85–96. URL: https://ceur-ws.org/Vol-3666/paper13.pdf **(Scopus)**
3. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. The role of encryption in information protection for cloud computing. *IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)*. 2024. P. 70–75. URL: https://doi.org/10.1109/SIST61555.2024.10629501 **(Scopus)**
4. Yarmilko A., Rozlomii I., Naumenko S. Dependability of embedded systems in the Industrial Internet of Things: Information security and reliability of the communication cluster. *Information Technology for Education, Science, and Technics*. 2024. Vol. 222. P. 235–249. URL: https://doi.org/10.1007/978-3-031-71804-5_16 **(Scopus)**

5. Rozlomii I., Naumenko S., Mykhailovskyi P., Monarkh V. Resource-saving cryptography for microcontrollers in biomedical devices. *IEEE 5th KhPI Week on Advanced Technology (KhPIWeek)*. 2024. P. 1–5. URL: https://doi.org/10.1109/KhPIWeek61434.2024.10877958 **(Scopus)**

6. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. Hardware encryptors and cryptographic libraries for optimizing security in IoT. *Proceedings of the 12th International Conference Information Control Systems & Technologies (ICST 2024)*. 2024. Vol. 3790. P. 99–109. URL: https://ceur-ws.org/Vol-3790/paper09.pdf **(Scopus)**

7. Rozlomii I., Yarmilko A., Naumenko S. Security and efficiency models for cyber-physical systems in medical devices. *IEEE 19th International Conference on Computer Science and Information Technologies (CSIT)*. 2024. P. 1–4. URL: https://doi.org/10.1109/CSIT65290.2024.10982678 **(Scopus)**

8. Rozlomii I., Yarmilko A., Naumenko S. Innovative resource-saving security strategies for IoT devices. *Journal of Edge Computing*. 2025. Vol. 4, no. 1. P. 35–56. URL: https://doi.org/10.55056/jec.748 **(Scopus)**

9. Rozlomii I., Yarmilko A., Naumenko S. Vulnerability modeling in cybersecurity of intelligent infrastructure networks. *International Scientific-Practical Conference*. 2024. P. 234–248. URL: https://doi.org/10.1007/978-3-031-90735-7_19 **(Scopus)**

10. Rozlomii I., Yarmilko A., Naumenko S. Resource-efficient solutions for data security at the network level of the Medical Internet of Things. *Proceedings of the 7th International Conference on Informatics & Data-Driven Medicine (IDDM'2024)*. 2024. P. 171–182. URL: https://ceur-ws.org/Vol-3892/paper13.pdf **(Scopus)**

11. Faure E., Rozlomii I., Yarmilko A., Naumenko S. Protection of IoT networks: cryptographic solutions for cybersecurity management. *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024)*. 2024. P. 24–34. URL: https://ceur-ws.org/Vol-3925/paper03.pdf **(Scopus)**

12. Rozlomii I., Yarmilko A., Naumenko S. Integration of lightweight cryptography and artificial intelligence methods to increase the dependability of precision medicine systems. *Proceedings of the International Workshop on Computational Intelligence (IWSCI 2025), co-located with the IV International Scientific Symposium "Intelligent Solutions" (IntSol 2025), Kyiv–Uzhhorod, May 01–05, 2025*. 2025. P. 201–212. URL: https://ceur-ws.org/Vol-4035/Paper17.pdf **(Scopus)**

13. Faure E., Rozlomii I., Naumenko S. Cryptographic load sharing method in critical infrastructure sensor networks. *Proceedings of the Fourth International*

Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN-25). 2025. P. 24–34. URL: https://ceur-ws.org/Vol-4024/paper01.pdf **(Scopus)**

14. Rozlomii I., Naumenko S., Mykhailovskyi P., Lishchuk R. Methodology for selecting the protection strategy in IoT environments based on the device resource profile. *IEEE 6th KhPI Week on Advanced Technology (KhPIWeek).* 2025. P. 1–5. URL: https://doi.org/10.1109/KhPIWeek61436.2025.11288556 **(Scopus)**

15. Danchenko O., Rozlomii I., Yarmilko A., Naumenko S. A lightweight Secure Boot mechanism for protecting the firmware of IoT devices. *Proceedings of the 13-th International Conference Information Control Systems & Technologies (ICST 2025), Odesa, Ukraine, September 24–26, 2025. CEUR Workshop Proceedings,* Vol. 4048. 2025. P. 240-250. URL: https://ceur-ws.org/Vol-4048/paper19.pdf **(Scopus)**

16. Rozlomii I., Faure E., Yarmilko A., Naumenko S. The method for verifying firmware integrity in IoT devices for secure boot using lightweight hash functions. *Proceedings of the Cyber Security and Data Protection (CSDP 2025), Lviv, Ukraine, July 31, 2025. CEUR Workshop Proceedings,* Vol. 4042. 2025. P. 105-116. URL: https://ceur-ws.org/Vol-4042/paper8.pdf **(Scopus)**

17. Rozlomii I., Naumenko S., Trembovetskyi R. Method for rotating cryptographic keys based on time tokens for radio-electronic medical modules with limited resources. *Visnyk NTUU KPI Seriia-Radiotekhnika Radioaparatobuduvannia.* 2025. No. 102. P. 58–65. URL: https://doi.org/10.64915/RADAP.2025.102.58-65 **(Scopus)**

18. Zabolotnii S., Rozlomii I., Yarmilko A., Naumenko S. Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska.* 2025. Vol. 15, no. 4. P. 164–169. URL: https://doi.org/10.35784/iapgos.7782 **(Scopus)**

19. Faure E., Rozlomii I., Naumenko S. Hybrid digital twin-driven anomaly detection in IoT telemetry using LSTM autoencoder. *Proceedings of the 2nd International Workshop on Data Analytics (WDA 2026), Kyiv, Ukraine, January 26, 2026.* CEUR Workshop Proceedings, Vol. 4155. 2025. P. 76–89. URL: https://ceur-ws.org/Vol-4155/paper06.pdf **(Scopus)**

20. Розломій І. О., Косенюк Г. В., Науменко С. В., Михайловський П. В. Моделювання системи датчиків на базі мікроконтролера в ігровій симуляції «Смарт-будинок» з використанням шифрування. *Computer-Integrated Technologies: Education, Science, Production.* 2023. Вип. 53. С. 292–299. URL: https://doi.org/10.36910/6775-2524-0560-2023-53-43

21. Розломій І. О., Симонюк В. П., Науменко С. В., Михайловський П. В. Адаптивна криптографія для енергоефективного захисту пристроїв IoT. *Проблеми моделювання та автоматизації проектування.* 2024. № 1(19). С. 77–83. URL: https://doi.org/10.31474/2074-7888-2024-1-19-77-83

22. Розломій І. О., Симонюк В. П., Науменко С. В., Михайловський П. В. Модель безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. *Computer-Integrated Technologies: Education, Science, Production.* 2024. Вип. 55. С. 191–198. URL: https://doi.org/10.36910/6775-2524-0560-2024-55-24

23. Rozlomii O., Yarmilko A., Naumenko S. The intelligent approaches to organizing secure information exchange in dynamic swarms of unmanned platforms. *Artificial Intelligence.* 2024. Vol. 29, no. 4. P. 151–158. URL: https://doi.org/10.15407/jai2024.04.151

24. Розломій І. О., Науменко С. В. Моделювання взаємовпливу інформаційної безпеки та обчислювальних витрат у вбудованих пристроях. *Computer-Integrated Technologies: Education, Science, Production.* 2024. Вип. 57. С. 139–145. URL: https://doi.org/10.36910/6775-2524-0560-2024-57-16

25. Розломій І. О., Фауре Е. В., Науменко С. В. Методи аутентифікації у вбудованих системах з обмеженими обчислювальними ресурсами. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2025. Вип. 81. С. 29–35. URL: https://doi.org/10.31891/2219-9365-2025-81-4

26. Розломій І. О., Науменко С. В. Архітектура та функціональні особливості захищених систем керування базами даних нового покоління з підтримкою serverless та edge-обчислень. *Systems and Technologies.* 2025. №1 (69), С. 7–15. URL: https://doi.org/10.32782/2521-6643-2025-1-69.16

27. Розломій І. О., Науменко С. В., Симонюк В. В., Птащенчук В. О., Зажома В. В. Полегшена криптографія для безпеки параметрів вібрації в постобробці 3D-друкованих деталей. *Інформаційні технології та суспільство.* 2025. № 2(17). С. 175–182. URL: https://doi.org/10.32689/maup.it.2025.2.25

28. Rozlomii I., Koseniuk G., Naumenko S. Mechanisms for cryptographic code authentication control in sensor nodes with limited computing resources. *Computer-Integrated Technologies: Education, Science, Production.* 2025. No. 61. P. 193–198. URL: https://doi.org/10.36910/6775-2524-0560-2025-61-27

29. Розломій І., Науменко С., Ковтюх В. Модель захищеного зберігання даних у розподілених базах даних на основі атрибутного шифрування для критичних інформаційно-комунікаційних систем. *Measuring and Computing Devices in Technological Processes.* 2026. № 1. С. 215–220. URL: https://doi.org/10.31891/2219-9365-2026-85-27

30. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. Modern encryption methods in IoT: hardware solutions and cryptographic libraries for data. *Розвитки інформаційно-керуючих систем та технологій: монографія / за ред. В. Вичужаніна. Львів-Торунь: Liha-Pres,* 2024. P. 28–44. URL: https://doi.org/10.36059/978-966-397-422-4

31. Розломій І. О., Ярмілко А. В., Науменко С. В. Ресурсоощадний підхід до побудови secure boot у вбудованих системах інтернету речей. *Системи контролю інформації та інтелектуальні технології. Досягнення та застосування: монографія / за ред. В. Вичужаніна. Львів-Торунь: Liha-Pres,* 2025. С. 102–122. URL: https://doi.org/10.36059/978-966-397-538-2-6

32. Rozlomii I., Yarmilko A., Naumenko S. Towards distributed anomaly detection in smart networks: a power-efficient node-level approach. *Методи та засоби обчислювального інтелекту в управлінні смарт-системами: колективна монографія / за ред. В. М. Теслюка.* Львів, 2025. С. 109–118.

33. Yarmilko A., Rozlomii I., Naumenko S. Robust communication clusters: Secure information exchange and redundant hashing for third-party inclusions localization. *КЗЯТПС-2023:* тези доп. Чернігів, 2023. P. 224–225.

34. Науменко С. В., Розломій І. О. Information protection strategies in Industry 4.0: Encryption and cybersecurity for industrial systems. *Theoretical and Experimental Research in Materials Science and Mechanical Engineering:* матеріали IX Міжнар. наук.-практ. конф., Луцьк, 2023. Луцьк: Вежа-Друк, 2023. С. 191–193.

35. Науменко С. В., Розломій І. О., Михайловський П. В. Забезпечення кібербезпеки в Smart-імплантах: роль полегшеної криптографії. *Інформаційна безпека та комп'ютерні технології:* матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 1 листоп. 2023 р. Кропивницький, 2023. С. 17–18.

36. Rozlomii I. O., Yarmilko A., Naumenko S. Optimized hash functions for integrity control and data recovery in embedded systems. *Information-Management Systems and Technologies:* матеріали XI Міжнар. наук. конф. 2023. С. 31–34.

37. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. The comprehensive IoT security strategy using hardware and software encryption methods. *Information-Management Systems and Technologies:* матеріали XII Міжнар. наук. конф., Одеса, 23 – 25 верес. 2024 р. Одеса, 2024. С. 63–65.

38. Розломій І. О., Ярмілко А. В., Науменко С. В. Інтелектуальні підходи до організації інформаційного обміну в динамічних зграях безпілотних платформ. *Штучний інтелект та інтелектуальні системи (AIIS'2024):* матеріали XXIV Міжнар. наук.-техн. конф. 2024. С. 144–149.

39. Науменко С. В., Михайловський П. В., Стабецька Т. А. Сучасні технології захисту даних у вбудованих пристроях з обмеженими ресурсами.

Free and Open Source Software: матеріали Міжнар. наук.-практ. конф., Харків, 13 – 14 лют. 2025 р. Харків, 2025. С. 63–64.

40. Розломій І. О., Науменко С. В. Конфігурований ARX-примітив для енергоефективного хешування у пристроях IoT. *Інформаційні системи та технології: результати і перспективи (IST 2025):* матеріали II Міжнар. наук.-практ. конф. 2025. С. 269–271.

41. Чікін Д. М., Науменко С. В., Розломій І. О. Захист персональних даних в IoT-пристроях із застосуванням штучного інтелекту. *Інформаційна безпека та комп'ютерні технології:* тези доп. VIII Міжнар. наук.-практ. конф., м. Кропивницький, 24 – 25 квіт. 2025 р. Кропивницький: ЦНТУ, 2025. С. 12–13.

42. Розломій І. О., Науменко С. В., Михайловський П. В. Формування сеансових ключів у сенсорних пристроях з обмеженим обсягом пам'яті на основі часових токенів. *Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2025):* матеріали XV Міжнар. наук.-практ. конф., Чернігів, 22 – 23 трав. 2025 р. Чернігів: НУ «Чернігівська політехніка», 2025. Вип. 2. С. 248–249.

43. Розломій І. О., Науменко С. В. Метод розподілу криптографічного навантаження між мікроконтролерами в edge-архітектурах на основі енергетичної моделі. *Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем:* матеріали II Міжнар. наук.-практ. конф., Луцьк, 2025. Луцьк: ЛНТУ, 2025. С. 112–115.

44. Розломій І. О., Науменко С. В. Модель адаптивної побудови довірчих IoT-мереж із динамічною ротацією вузлів. *Програмне та апаратне забезпечення в інформаційних технологіях:* матеріали Міжнар. наук.-практ. конф. молодих вчених та студентів, Луцьк, 6 трав. 2025 р. / відп. ред. Т. В. Терлецький. Луцьк: ЛНТУ, 2025. Вип. 1. С. 136–139.

У роботах, опублікованих у співавторстві, здобувачем: [1], [5], [11], [15], [16], [21], [25], [28], [36], [39] – розроблено та обґрунтовано методи використання полегшених криптографічних і хеш-функцій для забезпечення цілісності, автентичності та конфіденційності даних у вбудованих пристроях і сенсорних вузлах з обмеженими ресурсами; виконано аналіз ефективності запропонованих рішень для мікроконтролерних платформ; [2], [4], [7], [8], [12], [14], [22], [24], [30], [32], [34], [35] – виконано дослідження архітектур кіберфізичних та IoT-систем, сформульовано вимоги до полегшених криптографічних механізмів, запропоновано моделі захисту інформації з урахуванням енергоспоживання, обчислювальних витрат і ролі пристрою в системі; [8], [13], [14], [21], [22], [24], [43], [44] – запропоновано та узагальнено моделі динамічного вибору й розподілу криптографічного навантаження між компонентами кіберфізичних систем, edge- та fog-вузлами; розроблено критерії

ефективності та функції вартості для адаптивного прийняття рішень; [6], [18], [27], [36], [40] – здобувачем виконано модифікацію та аналіз криптографічних примітивів і блокових перетворень, орієнтованих на реалізацію в середовищі з обмеженими апаратними ресурсами; оцінено їх вплив на швидкодію, пам'ять і стійкість до атак; [15], [16], [28], [31], [36] – розроблено методи захищеного завантаження (Secure Boot) та контролю цілісності програмного коду для вбудованих пристроїв; визначено структуру алгоритмів, механізми перевірки автентичності та сценарії їх практичного застосування; [17], [42] – запропоновано методи формування та ротації криптографічних ключів у сенсорних і радіоелектронних модулях на основі часових токенів, адаптовані до умов обмеженої пам'яті та нестабільного живлення; [23], [33], [37], [38], [44] – розроблено підходи до організації захищеного інформаційного обміну в динамічних децентралізованих кіберфізичних середовищах, зокрема у зграях безпілотних платформ, із урахуванням змінної топології та автономності вузлів; [3], [9], [12], [19], [26], [29], [32], [41] – виконано дослідження суміжних аспектів підвищення надійності та безпеки кіберфізичних і хмарних систем, зокрема із застосуванням інтелектуальних та адаптивних підходів; отримані результати використано для розширення та узагальнення моделей, запропонованих у дисертації.

Результати аналізу роботи, в тому числі за допомогою перевірки тексту дисертації з використанням системи TURNITIN на пошук та аналіз текстових збігів, свідчать про відповідність дисертації принципам академічної доброчесності.

9. Апробація матеріалів дисертації відбувалась на наступних міжнародних наукових конференціях: XIII міжнародній науково-практичній конференції «Комплексне забезпечення якості технологічних процесів та систем» (м. Чернігів, 26 травня 2023 р.); 11-th International Conference «Information Control Systems & Technologies» (Odesa, Ukraine, September 21–23, 2023); VII міжнародній науково-практичній конференції «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 1 листопада 2023); 8th International Conference «Mathematical Modeling and Simulation Systems» (MODS2023) (Chernihiv, Ukraine, November 13–15, 2023); 6th International Conference on Informatics & Data-Driven Medicine (Bratislava, Slovakia, November 17–19, 2023); 3rd International Workshop on Information Technologies: Theoretical and Applied Problems (Ternopil, Ukraine, Opole, Poland, November 22–24, 2023); 4th Edge Computing Workshop (Zhytomyr, Ukraine, April 5, 2024); 4th IEEE International Conference on Smart Information Systems and Technologies (Astana, Kazakhstan, May 15–17, 2024); 14th International Conference on Advanced Computer Information Technologies (České Budějovice, September 19–21 2024);

XII International Scientific Conference «Information-Management Systems and Technologies» (Odesa, 23–25 September 2024); 5th KhPI Week on Advanced Technology (Kharkiv, Ukraine, October 7–11, 2024); 14th International Conference on Dependable Systems, Services and Technologies (Athens, Greece, October 11–13, 2024); XXIV міжнародній науково-технічній конференції «Штучний інтелект та інтелектуальні системи- AIIS'2024» (м. Київ, 18–19 жовтня 2024 р.); 19th International Conference on Computer Science and Information Technologies (Lviv, Ukraine, 16–19 October 2024); 3-rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024) (Kyiv, Ukraine, January 24–27, 2024); XVI міжнародній науково-практичній конференції «Free and Open Source Software» (м. Харків, 13–14 лютого 2025 р.); VIII міжнародній науково-практичній конференції «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 24–25 квітня 2025 р.); II міжнародній науково-практичній конференції «Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем» (м. Луцьк, 9–11 червня 2025 р.); міжнародній науково-практичній конференції «Програмне та апаратне забезпечення в інформаційних технологіях» (м. Луцьк, 6 травня 2025 р.); 2nd International Workshop on Data Analytics (Kyiv, Ukraine, January 26, 2026).

10. Оцінка мови та стилю дисертації.

Дисертацію написано з дотриманням норм і правил граматики, а стиль викладу в ній матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття.

Дисертація повною мірою відповідає пунктам 6–8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради про присудження ступеня доктора філософії в Черкаському державному технологічному університеті», затверджений вченою радою ЧДТУ, протокол №14 від 18.04.2022 року зі змінами та доповненнями. Робота містить нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання, що має істотне значення для галузі знань 12 Інформаційні технології.

Дисертацію виконано державною мовою та відповідно до наявних вимог щодо оформлення.

11. Відповідність змісту дисертації освітньо-науковій програмі, з якої вона подається до захисту.

Зміст дисертації повністю відповідає спеціальності 123 Комп'ютерна інженерія освітньо-наукової програми «Комп'ютерні системи та мережі».

12. Рекомендація дисертації до захисту.

Враховуючи рівень наукових досліджень, актуальність теми роботи та наукову новизну отриманих результатів, учасники фахового семінару кафедри

інформаційної безпеки та комп'ютерної інженерії одноголосно ухвалили рішення затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Науменка Сергія Васильовича на тему «Метод та моделі захисту інформації для кіберфізичних систем з обмеженими ресурсами» для здобуття ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології та рекомендувати до захисту у разовій спеціалізованій вченій раді Черкаського державного технологічного університету для здобуття ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

У голосуванні брали участь 16 осіб. Результати голосування:
«ЗА» – 16,
«ПРОТИ» – немає,
УТРИМАЛИСЬ – немає.

Головуюча:
професор кафедри інформаційної безпеки
та комп'ютерної інженерії,
д.т.н, професор Віра БАБЕНКО