

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004432

Особливі позначки: відкрита

Дата реєстрації: 07-08-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кисюк Дмитро Васильович

2. Dmytro Kysiuk

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0003-8514-2007

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп'ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерна інженерія

Дата захисту: 02-09-2026

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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): PhD 15380

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.23.17, 50.37.23, 50.39, 50.41.23

Тема дисертації:

1. Методи та засоби організації роботи з даними у приватних хмарних сервісах на основі байтпорієнтованого гешування
2. Methods and means of organizing data processing in private cloud services based on byte-oriented hashing

Реферат/анотація:

1. Дисертаційна робота присвячена розв'язанню актуального науково-прикладного завдання підвищення ефективності захисту даних у приватних хмарних сервісах шляхом удосконалення методів байт-орієнтованого гешування та розроблення спеціалізованої апаратно-програмної архітектури криптографічного процесора. Загальний обсяг роботи становить 174 сторінки, з яких основний зміст викладено на 158 сторінках. Дисертація містить 32 рисунки та 21 таблицю. Робота виконувалась відповідно до тематичних планів наукових досліджень кафедр обчислювальної техніки та захисту інформації Вінницького національного технічного університету. Основні наукові результати та висновки дисертаційної роботи отримані автором самостійно та викладені у 5 наукових працях та 19 тезах доповідей на конференціях. Актуальність дослідження зумовлена стрімким розвитком хмарних технологій, зростанням обсягів даних, необхідністю забезпечення їх цілісності, автентичності та ефективної обробки в умовах обмежених обчислювальних ресурсів, а також підвищеними вимогами до продуктивності сучасних кіберфізичних

систем, IoT-пристроїв та edge-обчислень. Об'єктом дослідження є процеси забезпечення цілісності даних у приватних хмарних сервісах. Предметом дослідження виступають методи, моделі та засоби байт-орієнтованого гешування, а також архітектурні рішення для їх апаратної реалізації. Метою дисертаційної роботи є підвищення продуктивності процесів контролю цілісності даних у приватних хмарних сервісах шляхом розроблення методів байт-орієнтованого гешування та спеціалізованої архітектури криптографічного процесора, що забезпечують зменшення часу обробки повідомлень при збереженні необхідного рівня криптографічної стійкості. У роботі проведено аналіз сучасних методів криптографічного гешування, визначено їх переваги та обмеження щодо використання в ресурсно-обмежених інформаційних системах. Запропоновано нові методи байт-орієнтованого гешування, засновані на попередньому формуванні характеристичних структур повідомлення та їх подальшому ущільненні, що дозволяє зменшити обсяг проміжних обчислень і підвищити швидкість алгоритму. Удосконалено математичну модель процесу гешування, яка враховує особливості організації байтових потоків даних та забезпечує ефективну паралельну обробку. Розроблено багатопланову апаратно-програмну архітектуру криптографічного процесора, адаптовану до реалізації на FPGA, яка забезпечує конвеєризацію операцій, паралельне виконання окремих етапів обробки та масштабованість залежно від вимог прикладної системи. Запропоновані архітектурні рішення дозволяють зменшити затримки при обчисленні геш-значень, підвищити пропускну здатність системи та забезпечити ефективне використання апаратних ресурсів. У процесі дослідження розроблено структурні та функціональні моделі криптографічного процесора, виконано їх програмне моделювання та апаратну реалізацію на FPGA. Проведено експериментальні дослідження продуктивності, які підтвердили працездатність запропонованих методів і архітектурних рішень. Отримані результати демонструють скорочення часу обробки даних та підвищення продуктивності порівняно з програмною реалізацією криптографічних алгоритмів загального призначення при раціональному використанні логічних ресурсів програмованої логіки. Наукова новизна одержаних результатів полягає у розробленні нових методів байт-орієнтованого гешування, удосконаленні моделей організації процесу обробки даних та створенні спеціалізованої багатопланової архітектури криптографічного процесора для забезпечення контролю цілісності інформації у приватних хмарних сервісах. Подальшого розвитку набули підходи до апаратного прискорення криптографічних перетворень на основі FPGA із застосуванням конвеєрної та паралельної обробки даних. Практичне значення отриманих результатів полягає у можливості використання розроблених методів та архітектурних рішень під час створення високопродуктивних засобів контролю цілісності інформації у приватних хмарних інфраструктурах, центрах обробки даних, системах резервування та дедуплікації інформації, кіберфізичних системах, IoT- та edge-пристроях і спеціалізованих інформаційно-комунікаційних комплексах. Результати дослідження можуть бути використані при проектуванні апаратних криптографічних модулів, а також у навчальному процесі закладів вищої освіти під час викладання дисциплін, пов'язаних із криптографією, комп'ютерною інженерією та інформаційною безпекою. Основні положення дисертаційної роботи апробовано на міжнародних та всеукраїнських науково-практичних конференціях. Результати дослідження опубліковано у наукових працях, зокрема у фахових виданнях України та виданнях, що індексуються міжнародними наукометричними базами даних.

2. The dissertation is devoted to solving the relevant scientific and applied problem of improving data protection efficiency in private cloud services by enhancing byte-oriented hashing methods and developing a specialized hardware-software architecture of a cryptographic processor. The dissertation comprises 174 pages, including 158 pages of the main text. It contains 32 figures and 21 tables. The research was carried out in accordance with the scientific research plans of the Departments of Computer Engineering and Information Protection of Vinnytsia National Technical University. The main scientific results and conclusions of the dissertation were obtained independently by the author and are presented in 5 scientific publications and 19 conference proceedings. The relevance of the research is determined by the rapid development of cloud technologies, the continuous growth of data volumes, the need to ensure data integrity, authenticity, and efficient processing under limited computing resources, as well as the increasing performance requirements of modern cyber-physical systems, Internet of Things (IoT) devices, and edge computing. The object of the research is the processes of ensuring data integrity in

private cloud services. The subject of the research comprises methods, models, and tools of byte-oriented hashing, as well as architectural solutions for their hardware implementation. The aim of the dissertation is to improve the performance of data integrity control processes in private cloud services through the development of byte-oriented hashing methods and a specialized cryptographic processor architecture that reduces message processing time while maintaining the required level of cryptographic strength. The dissertation includes an analysis of modern cryptographic hashing methods and identifies their advantages and limitations for application in resource-constrained information systems. New byte-oriented hashing methods based on the preliminary formation of message characteristic structures followed by their compression are proposed, making it possible to reduce the amount of intermediate computations and improve algorithm performance. A mathematical model of the hashing process has been improved, taking into account the specific features of byte-stream organization and providing efficient parallel data processing. A multilayer hardware-software architecture of a cryptographic processor adapted for FPGA implementation has been developed. The proposed architecture provides operation pipelining, parallel execution of individual processing stages, and scalability according to the requirements of a target application. The proposed architectural solutions reduce hash computation latency, increase system throughput, and ensure efficient utilization of FPGA hardware resources. During the research, structural and functional models of the cryptographic processor were developed, software simulation was performed, and hardware implementation on an FPGA platform was carried out. Experimental performance evaluation confirmed the efficiency of the proposed methods and architectural solutions. The obtained results demonstrate reduced data processing time and improved performance compared with software implementations of general-purpose cryptographic algorithms while ensuring rational utilization of programmable logic resources. The scientific novelty of the obtained results lies in the development of new byte-oriented hashing methods, the improvement of data processing organization models, and the creation of a specialized multilayer cryptographic processor architecture intended for ensuring information integrity in private cloud services. The approaches to FPGA-based hardware acceleration of cryptographic transformations using pipelined and parallel data processing have been further developed. The practical significance of the obtained results lies in the possibility of applying the developed methods and architectural solutions to create high-performance information integrity control tools for private cloud infrastructures, data centers, backup and data deduplication systems, cyber-physical systems, IoT and edge devices, and specialized information and communication systems. The research results can also be used in the design of hardware cryptographic modules and in the educational process of higher education institutions when teaching courses related to cryptography, computer engineering, and information security. The main provisions of the dissertation have been presented at international and national scientific and practical conferences. The research results have been published in scientific papers, including articles in Ukrainian peer-reviewed journals and publications indexed in international scientometric databases.

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:

- 1. Кисюк Д. В. Аналітичний огляд постачальників хмарних послуг. Вимірювальна та обчислювальна техніка в технологічних процесах. 2025, №3, С. 105–111.
- 2. Кисюк Д. В. Актуальність проблеми впровадження хмарних сервісів для організації роботи з даними. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025, Т.356, № 5.
- 3. Кисюк Д. В., Захарченко С. М. Оптимізація застосування хмарних сервісів для розподіленої обробки даних в системах колективного доступу. Наукові праці ВНТУ. 2025, Вип. №2, С. 66–72.

- 4. Лужецький В. А., Кисюк Д. В. Новий підхід до побудови байт-орієнтованих криптографічних геш-функцій. Вимірювальна техніка та метрологія. 2026, Випуск 87(1), ISTCMTM, Львів, Номер 1, С. 51-58
- 5. Лужецький В. А., Захарченко С. М., Кисюк Д. В. Метод байт-орієнтованого гешування з підвищеним рівнем дифузії та спеціалізований МНпроцесор для приватних хмарних інфраструктур. Вимірювальна та обчислювальна техніка в технологічних процесах. 2026, № 85(1), С. 134-141.
- 6. Лужецький В. А., Савицька Л. А., Кисюк Д. В. Спеціалізований процесор для ущільнення даних. Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації». 2016, Вінниця : ВНТУ, С.108-110
- 7. Лужецький В. А., Кисюк Д. В., Савицька Л. А. Метод байт-орієнтованого хешування. Тези доповідей V Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації». 2016, Вінниця-Немирів
- 8. Лужецький В. А., Кисюк Д. В. Новий підхід до побудови криптографічних хеш-функцій. Матеріали статей П'ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». 2015, Івано-Франківськ : ФОП Голіней О. М., С.149-150
- 9. Кисюк Д. В., Захарченко С. М. Аналіз переваг використання хмарних сервісів для обробки даних у сучасних системах управління базами даних. Матеріали LII Науково-технічної конференції підрозділів ВНТУ. 2023, Вінниця.
- 10. Кисюк Д. В., Лужецький В. А. Програмний засіб для побудови хеш-значення за допомогою байт-орієнтованої обробки даних для мобільних пристроїв. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2023)». 2023, Вінниця.
- 11. Мазур Б. С., Кисюк Д. В. Хмарні сервіси. Обробка та збереження даних за допомогою хмарних сховищ. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)». 2024, Вінниця
- 12. Кисюк Д. В., Шулдик С. С. Хмарні сервіси як інструмент управління проектами у системах забезпечення ресурсами підприємства SAP ERP. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2025)». 2025, Вінниця
- 13. Лужецький В. А., Кисюк Д. В. Узагальнений метод хешування байтової форми представлення інформації. Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». 2014, Вінниця : ВНТУ, С. 184-186
- 14. Лужецький В. А., Кисюк Д. В. Метод хешування даних на основі їх характеристичних ознак. Тези доповідей II Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації». 2014, Київ : Європейський університет, С. 100-102.
- 15. Лужецький В. А., Кисюк Д. В., Савицька Л. А. Метод байт-орієнтованого хешування. Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації». 2016, Вінниця : ВНТУ, С. 37-38.
- 16. Лужецький В. А., Кисюк Д. В., Комаров А. О. Метод та спеціалізований процесор для байт-орієнтованого хешування даних. Тези доповідей Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерне моделювання (ITCM)». 2016, Івано-Франківськ : ПНУ ім. В. Стефаника, С. 123-125.
- 17. Кисюк Д. В., Заруцький М. В. Перспективи впровадження штучного інтелекту в хмарних обчисленнях. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2025)». 2025, Вінниця
- 18. Кисюк Д. В., Червінський В. О. Архітектура приватних хмарних сервісів для зберігання та обробки даних. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2025)». 2025, Вінниця
- 19. Кисюк Д. В., Сірак В. О. Методи підвищення ефективності зберігання та обробки великих обсягів даних у приватних хмарних сервісах. Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2026)». 2026, Вінниця

Наукова (науково-технічна) продукція: технології; методи, теорії, гіпотези

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

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Лужецький Володимир Андрійович

2. Volodymyr A. Luzhetskyi

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

Ідентифікатор ORCID ID: 0000-0001-7466-7738

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Захарченко Сергій Михайлович

2. Serhii Zakharchenko

Кваліфікація: к.т.н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0003-3977-2908

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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. Коршун Наталія Володимирівна
2. Nataliia V. Korshun

Кваліфікація: д. т. н., професор, 05.12.13

Ідентифікатор ORCID ID: 0000-0003-2908-970X

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 45307965

Місцезнаходження: вул. Бульварно-Кудрявська, Київ, 04053, Україна

Форма власності: Комунальна

Сфера управління: Держадміністрація

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій Олексійович
2. Andrii O. Fesenko

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: 0000-0001-5154-5324

Додаткова інформація:

Повне найменування юридичної особи: Національний університет «Київський авіаційний інститут»

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Іванченко Євгенія Вікторівна
2. Yevheniia V. Ivanchenko

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

Ідентифікатор ORCID ID: 0000-0003-3017-5752

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Баришев Юрій Володимирович

2. Yurii V. Baryshev

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0001-8324-8869

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові
голови ради

Ковтун В'ячеслав Васильович

Власне Прізвище Ім'я По-батькові
головуючого на засіданні

Ковтун В'ячеслав Васильович

Відповідальний за підготовку
облікових документів

Іванчук Ярослав Володимирович

Реєстратор

Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності



Юрченко Тетяна Анатоліївна