НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ШАРОВ ВЛАДИСЛАВ ОЛЕГОВИЧ

УДК 519.72, 004.4:004.7, 004.9

ДИСЕРТАЦІЯ
МОДЕЛІ, МЕТОДИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДВИЩЕННЯ НАДІЙНОСТІ Й ЗАХИЩЕНОСТІ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖАХ

Спеціальність 122 – Комп’ютерні науки

Галузь знань 12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.О. Шаров

Науковий керівник:
Нікуліна Олена Миколаївна
доктор технічних наук, професор

Харків – 2026

АНОТАЦІЯ

Шаров В.О. Моделі, методи та інформаційна технологія підвищення надійності й захищеності передачі даних у мережах – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Національний технічний університет «Харківський політехнічний інститут», Харків, 2026.

Дисертаційну роботу присвячено вирішенню актуальної науково-технічної задачі підвищення надійності та захищеності передавання даних у комп'ютерних мережах в умовах дії завад і кіберзагроз шляхом розроблення інтегрованих моделей, методів та інформаційної технології, що поєднують механізми завадостійкого кодування та захищеного тунелювання.

Об'єкт дослідження – процес передавання даних у комп'ютерних мережах за наявності завад і кіберзагроз.

Предмет дослідження – моделі, методи та інформаційна технологія забезпечення надійності й захищеності передавання даних на основі інтеграції завадостійкого кодування та оверлейних технологій.

Метою роботи є підвищення ефективності, надійності та захищеності передавання даних шляхом розроблення та впровадження інтегрованого підходу до забезпечення їх надійності та захищеності.

У *вступі* обґрунтовано актуальність теми, визначено наукову проблему недостатньої ефективності ізольованого застосування засобів захисту та завадостійкості, що не дозволяє забезпечити необхідний рівень стабільності передачі даних у сучасних мережах.

У *першому розділі* проаналізовано сучасний стан методів забезпечення ефективності, надійності та захищеності передавання даних, визначено їх обмеження та сформульовано наукову задачу інтеграції відповідних механізмів.

У *другому розділі* обґрунтовано систему показників оцінювання ефективності, розроблено концептуальну модель гібридного захищеного каналу передавання даних та методи синтезу та формування його параметрів.

У *третьому розділі* розроблено моделі та методи інтеграції завадостійкого кодування та оверлейних технологій, удосконалено метод адаптивного керування параметрами системи та запропоновано інформаційну технологію багаторівневого захисту.

У *четвертому розділі* проведено імітаційне моделювання та експериментальні дослідження ефективності запропонованих рішень із використанням профілів VPN (зокрема IPsec, OpenVPN, WireGuard) та каскадних кодів. Отримані результати підтвердили підвищення стійкості до помилок, зменшення втрат пакетів і покращення стабільності передачі даних порівняно з базовими підходами.

У *висновках* дисертаційної роботи узагальнено результати проведених досліджень та підтверджено досягнення поставленої мети. У роботі розроблено гібридну модель захищеного каналу передавання даних, методи синтезу профілю каналу та адаптивного керування параметрами системи, а також реалізовано інформаційну технологію інтеграції завадостійкого кодування та VPN-протоколів. Доведено ефективність інтегрованого підходу до забезпечення надійності й захищеності передавання даних в умовах завад, втрат пакетів і кіберзагроз. Встановлено, що спільне використання механізмів FEC-кодування та VPN-тунелювання забезпечує підвищення стійкості до помилок, зменшення втрат пакетів і стабілізацію процесу передавання даних у складних умовах функціонування мереж.

За результатами дослідження отримано такі наукові результати:

– удосконалено гібридну модель захищеного каналу передавання даних, побудовану на поєднанні механізмів завадостійкого кодування та VPN-тунелювання з урахуванням впливу завад і кіберзагроз різної природи, яка, на відміну від існуючих підходів до окремого використання зазначених механізмів,

забезпечує їх комплексну взаємодію та дозволяє підвищити стійкість системи до помилок і атак, а також забезпечити стабільність передавання даних у складних умовах функціонування мереж;

– удосконалено метод адаптивного налаштування параметрів завадостійкого кодування та оверлейних протоколів на основі оцінювання стану мережі й показників ефективності передавання даних, який, на відміну від існуючих методів із фіксованими або частково змінними параметрами, забезпечує узгоджене коригування конфігурації системи та дозволяє підвищити ефективність використання мережевих ресурсів і якість обслуговування трафіку;

– отримали подальший розвиток методи формування профілю каналу передавання даних і побудови інформаційної технології багаторівневого захисту на основі комплексного врахування параметрів кодування та характеристик VPN-протоколів, які, на відміну від існуючих рішень, забезпечують інтегроване налаштування параметрів системи та дозволяють реалізувати адаптивне конфігурування захищених каналів зв’язку відповідно до умов функціонування й вимог до надійності та інформаційної безпеки.

Практичне значення отриманих результатів полягає у безпосередньому використанні запропонованих моделей, методів та інформаційної технології при побудові захищених комп’ютерних мереж і каналів передавання даних, завдяки чому досягається підвищення ефективності, надійності та захищеності обміну інформацією в умовах дії завад, втрат пакетів і кіберзагроз різної природи. Запропоновані рішення дозволяють забезпечити адаптивне налаштування параметрів завадостійкого кодування та VPN-протоколів, зменшити рівень помилок передавання даних і підвищити стабільність функціонування мережевих систем.

Практична цінність отриманих результатів дослідження полягає у можливості їх впровадження у таких важливих галузях української економіки:

– безпека та оборона, де інтеграція механізмів завадостійкого кодування та VPN-тунелювання дозволяє забезпечити захищене й стабільне передавання даних

у системах зв’язку, управління, моніторингу та взаємодії безпілотних платформ в умовах активного впливу завад і кіберзагроз;

– інформаційно-телекомунікаційні системи та цифрова інфраструктура, де розроблені моделі й методи можуть бути використані для підвищення надійності функціонування корпоративних мереж, дата-центрів, хмарних сервісів та розподілених інформаційних систем;

– промисловість та автоматизовані системи управління, де застосування адаптивного керування параметрами передавання даних дозволяє забезпечити стабільність обміну інформацією між компонентами автоматизованих і кіберфізичних систем у режимі реального часу;

– транспорт і логістика, де використання запропонованих підходів забезпечує підвищення стійкості телекомунікаційних каналів до помилок і втрат пакетів у системах навігації, диспетчеризації та моніторингу транспортних потоків;

– цифровізація економіки та інформаційна безпека, де запропоновані рішення дозволяють реалізувати гнучке налаштування захищених каналів зв’язку відповідно до вимог користувачів, характеристик мережі та умов функціонування інформаційних систем.За результатами дослідження підтверджено теоретичну обґрунтованість і практичну ефективність запропонованих рішень, що свідчить про завершеність роботи та можливість їх подальшого застосування і розвитку.

Ключові слова: VPN, захищене передавання даних, комп’ютерні мережі, імітаційне моделювання, каскадні коди, адаптивне керування, інформаційна безпека, модель, завадостійкість, безпека даних, кібербезпека, канали передачі даних, цілісність даних, моделювання помилок, якісна пе-редача даних

ABSTRACT

Sharov V.O. Models and methods for ensuring the reliability and security of data transmission in computer networks based on the integration of noise-resistant coding and overlay technologies. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 122 – Computer Science. – National Technical University "Kharkiv Polytechnic Institute", Kharkiv, 2026.

The dissertation is devoted to solving the current scientific and technical problem of increasing the reliability and security of data transmission in computer networks under conditions of interference and cyber threats by developing integrated models, methods and information technology that combine the mechanisms of noise-resistant coding and secure tunneling.

The object of research is the process of data transmission in computer networks in the presence of interference and cyber threats.

The subject of the research is models, methods and information technology for ensuring the reliability and security of data transmission based on the integration of noise-resistant coding and overlay technologies.

The purpose of the research is to increase the efficiency, reliability and security of data transmission by developing and implementing an integrated approach to ensuring their reliability and security.

The introduction substantiates the relevance of the topic, identifies the scientific problem of insufficient effectiveness of the isolated use of protection and noise-resistant means, which does not allow ensuring the required level of data transmission stability in modern networks.

The first section analyzes the current state of methods for ensuring the efficiency, reliability and security of data transmission, identifies their limitations and formulates the scientific task of integrating the relevant mechanisms.

The second section substantiates the system of performance evaluation indicators, develops a conceptual model of a hybrid protected data transmission channel and methods for synthesizing and forming its parameters.

In the third section, models and methods for integrating noise-tolerant coding and overlay technologies are developed, a method for adaptive control of system parameters is improved, and an information technology for multi-level protection is proposed.

In the fourth section, simulation modeling and experimental studies of the effectiveness of the proposed solutions using VPN profiles (in particular, IPsec, OpenVPN, WireGuard) and cascading codes are carried out. The results obtained confirmed the increase in error resistance, reduction of packet loss, and improvement of data transmission stability compared to basic approaches.

The conclusions of the dissertation summarize the results of the research and confirm the achievement of the set goal. The work develops a hybrid model of a secure data transmission channel, methods for channel profile synthesis and adaptive control of system parameters, and also implements information technology for integrating noise-tolerant coding and VPN protocols. The effectiveness of the integrated approach to ensuring the reliability and security of data transmission in conditions of interference, packet loss, and cyber threats is proven. It was established that the joint use of FEC coding and VPN tunneling mechanisms provides increased error resistance, reduced packet loss and stabilization of the data transmission process in difficult network operating conditions.

The research yielded the following scientific results:

– a hybrid model of a secure data transmission channel was enhanced, built on a combination of noise-tolerant coding and VPN tunneling mechanisms, taking into account the impact of interference and cyber threats of various nature, which, unlike existing approaches to the separate use of these mechanisms, ensures their complex interaction and allows to increase the system's resistance to errors and attacks, as well as ensure the stability of data transmission in difficult network operating conditions;

– the method of adaptive adjustment of noise-tolerant coding parameters and overlay protocols based on assessing the network state and data transmission efficiency indicators was improved, which, unlike existing methods with fixed or partially variable parameters, provides coordinated adjustment of the system configuration and allows to increase the efficiency of using network resources and the quality of traffic service;

– the methods for forming a data transmission channel profile and building multi-level protection information technology based on comprehensive consideration of encoding parameters and characteristics of VPN protocols have been further developed, which, unlike existing solutions, provide integrated configuration of system parameters and allow for adaptive configuration of protected communication channels in accordance with operating conditions and requirements for reliability and information security.

The practical significance of the results obtained lies in the direct use of the proposed models, methods and information technology in the construction of secure computer networks and data transmission channels, which results in increased efficiency, reliability and security of information exchange under conditions of interference, packet loss and cyber threats of various nature. The proposed solutions allow for adaptive adjustment of parameters of noise-resistant coding and VPN protocols, reduce the level of data transmission errors and increase the stability of network systems.

The practical value of the obtained research results lies in the possibility of their implementation in the following important sectors of the Ukrainian economy:

– security and defense, where the integration of noise-resistant coding and VPN tunneling mechanisms allows for secure and stable data transmission in communication systems, control, monitoring and interaction of unmanned platforms under conditions of active interference and cyber threats;

– information and telecommunication systems and digital infrastructure, where the developed models and methods can be used to increase the reliability of corporate networks, data centers, cloud services and distributed information systems;

– industry and automated control systems, where the use of adaptive control of data transmission parameters allows to ensure the stability of information exchange between components of automated and cyber-physical systems in real time;

– transport and logistics, where the use of the proposed approaches ensures increased stability of telecommunication channels to errors and packet loss in navigation, dispatching and monitoring systems of transport flows;

– digitalization of the economy and information security, where the proposed solutions allow to implement flexible configuration of protected communication channels in accordance with user requirements, network characteristics and operating conditions of information systems. The results of the study confirmed the theoretical validity and practical effectiveness of the proposed solutions, which indicates the completion of the work and the possibility of their further application and development.

Keywords: VPN, secure data transmission, computer networks, simulation modeling, cascading codes, adaptive control, information security, model, noise immunity, data security, cybersecurity, data transmission channels, data integrity, error modeling, high-quality data transmission

Список публікацій здобувача:

Публікації здобувача за темою дисертації, в яких опубліковані основні наукові результати

1. Шаров В.О., Нікуліна О.М., Северин В.П. Розробка моделі завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами. Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (8), 2022, с. 57–62.

2. Шаров В.О., Нікуліна О.М., Северин В.П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (9)*, 2023, с. 64–69.

3. Шаров В.О., Нікуліна О.М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (11)*, 2024, с. 70–75.

4. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (12)*, 2024, с. 92–97.

5. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (13)*, 2025, с. 112–116.

Опубліковані праці апробаційного характеру:

6. Шаров В.О., Бердніков А.Г. Модель завадостійкого каналу передачі даних. *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2020)*, Харків: ХНУ ім. В.Н. Каразіна, 2020. 4 с.

7. Шаров В.О., Бердніков А.Г. Моделювання коригувального каскадного коду в каналах передачі даних системи управління. *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021)*, Харків: ХНУ ім. В.Н. Каразіна, 2021. 5 с.

8. Шаров В.О., Нікуліна О.М., Лошкарьова С.Є. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: Тези*

доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023, 17-20 травня 2023 р., Харків, НТУ «ХПІ», с. 1048.

9. Шаров В.О., Нікуліна О.М. Модель завадостійкої системи управління з урахуванням штучних перешкод вищого рівня. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: Тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-24 травня* 2024 р., Харків, НТУ «ХПІ», с. 1270.

10. Sharov V.O., Nikulina O.M. The model control system resistant to interference from higher-level artificial sources. *XVIII Міжнар. наук.-практ. конф. магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених», 19–22 листопада* 2024 р., Харків: НТУ «ХПІ», с. 56–57.