НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Толкачов Максим Юрійович

УДК 004.056.53

ДИСЕРТАЦІЯ
МОДЕЛЮВАННЯ БЕЗПЕКИ ІНТЕРНЕТ-ТРАФІКУ ЯК СЕМІОТИЧНОЇ СИСТЕМИ

Спеціальність 125 – Кібербезпека та захист інформації
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

М.Ю.Толкачов

Науковий керівник:
КОРОЛЬ Ольга
Григорівна, кандідат
технічних наук, доцент

Харків – 2025

АНОТАЦІЯ

Толкачов М.Ю. Моделювання безпеки інтернет-трафіку як семіотичної системи. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії (PhD) за спеціальністю 125 – Кібербезпека та захист інформації. – Національний технічний університет "Харківський Політехнічний Інститут", Харків, 2025.

Дисертація присвячена розв'язанню науково-технічного завдання забезпечення підвищення рівня безпеки систем захисту інтернет-трафіку на основі розробки та впровадження математичних моделей, методів моніторингу та управління елементами системи безпеки з врахуванням різноманітних факторів, включно соціальних та перцептивних аспектів.

Використання запропонованого підходу забезпечує захист змішаного контенту інформації на основі семіотичного аналізу, який не тільки підвищує рівень захисту інформаційних ресурсів, але й забезпечує гнучкість управління безпеки інтернет-трафіку.

Метою дисертаційної роботи є розробка моделей безпеки інтернет-трафіку у кібефізичному просторі на основі багаторівневої семіотичної моделі, що забезпечує підвищення рівня безпеки систем захисту інформації.

Об'єкт дослідження: процес створення та використання моделей і методів забезпечення захисту інтернет-трафіку у кібефізичному просторі.

Предмет дослідження – моделювання безпеки інтернет-трафіку як семіотичної системи.

У *вступі* обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача. Подано відомості про апробацію результатів роботи, особистий внесок здобувача та його публікації.

У *першому розділі* проаналізовано сучасний стан захищеності інтернет-трафіку, зокрема методи захисту інформаційних ресурсів у кіберпросторі.

Розглянуто системні архітектури контролю та захисту мереж, а також їх відповідність сучасним загрозам. Проаналізовані моделі кібератак на різні види трафіку інфокомунікаційних систем, включаючи реальний, потоковий, еластичний і сигнальний трафік, а також визначено найбільш уразливі сегменти мережевої інфраструктури. Оцінено загрози інформаційної безпеки, зокрема ризики кібертероризму та використання цифрових технологій для маніпуляції масовою свідомістю.

Обґрунтовано необхідність підвищення рівня захисту інформаційних ресурсів у кіберпросторі шляхом інтеграції новітніх методів аналізу та контролю трафіку. Запропоновано підхід, що базується на семіотичній моделі та включає механізми шифрування, автентифікації, контролю доступу та аналізу соціальної взаємодії. Підкреслено важливість розробки універсальних моделей безпеки, що враховують як технічні характеристики трафіку, так і його змістову складову.

У *другому розділі* запропонована модель семіотичної системи кіберпростору, що враховує взаємодію між користувачами, контентом та мережевою інфраструктурою. Проаналізовано структуру Інтернет-комунікацій та визначено основні елементи їх семіотичної природи, включаючи синтаксичний, семантичний і прагматичний рівні. Розглянуто застосування семіотичної моделі для оцінки кібербезпеки, що дозволяє виявляти та нейтралізувати потенційні загрози за рахунок аналізу інформаційного контенту та його впливу на безпеку мереж.

Досліджено ієрархію надійності в кіберпросторі, яка включає фізичний, синтаксичний, семантичний, прагматичний та соціальний рівні. Запропоновано використання семіотичних методів для маркування та сегментації мережевого трафіку, що дозволяє покращити управління інформаційними потоками та виявлення аномальних поведінкових патернів.

Запропонована модель безпеки на основі концепції нульової довіри, яка передбачає комплексний підхід до автентифікації користувачів, моніторингу мережевої активності та управління ризиками. Впроваджено методологію

розподілу доступу та контролю інформаційних потоків на основі семіотичного аналізу, що забезпечує гнучкість та ефективність політик кіберзахисту.

У *третьому розділі* розглянуто семіотичний підхід до забезпечення кібербезпеки, який забезпечує інтеграцію технічних, семантичних, прагматичних та соціальних аспектів аналізу загроз.

Удосконалена семіотична модель кібербезпеки на основі семіотичного аналізу, яка дозволяє враховувати різні рівні інформації – від синтаксичного та семантичного до прагматичного і соціального. Розроблено метод цільової сегментації трафіку з використанням моделі зрілості CISA's Zero Trust Maturity Model, який забезпечує більш точний контроль доступу та мінімізацію ризиків компрометації даних.

Запропоновано дворівневе динамічне маркування даних, спрямоване на покращення аналізу інформаційних потоків і захисту ресурсів. Розроблені методи макросегментації і мікросегментації мережевого трафіку, що забезпечують розділ інформаційних потоків відповідно до вимог безпеки та ефективність управління доступом. Методи макросегментації і мікросегментації мережевого трафіку враховують комплексний аналіз інформації на основі семіотичних параметрів, який дозволяє підвищити гнучкість системи кіберзахисту та адаптувати її до поточних загроз.

Розроблений інтегральний показник захищеності мережевих ресурсів забезпечує формування інтегрованого підходу до оцінки кібербезпеки, що включає різні рівні: від фізичних аспектів (CVE Rating) до більш абстрактних, таких як вплив на соціальні аспекти (Social Level).

Розроблена методика динамічного моніторингу та управління кібербезпекою на основі семіотичного аналізу. Запропоновано метод захисту змішаного контенту в інтернет-трафіку кіберпростору, який забезпечує визначений рівень гнучкості управління системою безпеки.

Розроблені методи динамічного маркування, макро- та мікросегментації трафіку, які дозволяють підвищити контроль за доступом до даних та мінімізувати ризики компрометації.

У *четвертому розділі* проведено моделювання оцінки рівня кібербезпеки власників мережі. Моделювання проведено на основі даних звіту Cisco Talos за 2023 р. Для проведення моделювання запропоновані програмні застосунки і скріпти на мові C# і Python 3.x з використанням бібліотек Pandas, NumPy, SciPy.

Запропонований метод захисту змішаного контенту інформації інтернет-трафіку на основі семіотичного аналізу, який інтегрує стратегію нульової довіри та сучасні аналітичні технології та дає оцінку якісних та кількісних характеристик системи.

Для проведення моделювання запропонованого підходу використані набори даних CIC-IDS 2017/2018 та NSL-KDD 2022, які базуються на алгоритмах виявлення атак та аналізу поведінкових характеристик трафіку.

У *висновках* дисертаційної роботи викладено основні результати які випливають з проведених досліджень, представлено та охарактеризовано показники ефективності при використанні запропонованих рішень.

За результатами дослідження отримано такі наукові результати:

1. *Вперше* розроблений інтегральний показник потенційних загроз, який враховує зважене середнє показників рівнів семіотичної моделі кіберпростору: фізичного, емпіричного, синтаксичного, семантичного, прагматичного та соціального. Запропонований підхід з використанням розділення змішаного контенту інформації на взаємопов'язані рівні дозволяє оцінити цільові (змішані) атаки із комплексними загрозами, що відрізняє його від традиційних сучасних підходів.

2. *Вперше* розроблений алгоритм аналізу інформаційних ресурсів, який включає кілька основних етапів, таких як синтаксичний аналіз, кореляційний аналіз, семантичний аналіз, прагматичний аналіз, маркування рівнів доступу. У результаті такого поетапного аналізу створюється комплексна система захисту інформаційних потоків, що знижує рівень ентропії у кіберпросторі, підвищує точність передачі даних та забезпечує їх безпеку.

3. *Вперше* розроблена модель системи динамічного аналізу та маркування захисту інформаційних ресурсів, яка враховує семіотичні рівні. Модель включає

аспекти, такі як безпека даних, продуктивність системи, витрати ресурсів, а також вимоги до конфіденційності. В моделі розроблено методи макро і мікросегментації мережевого трафіку, що дають змогу розділяти інформаційні потоки відповідно до вимог безпеки та ефективно керувати доступом до даних.

4. *Удосконалена* семіотична структура "данні-інформація-знання", яка для опису інформації візуалізує зв'язки цих різних термінів. Вона демонструє взаємозв'язок між семіотикою та використанням знаків під час обробки інформації.

5. *Удосконалена* архітектура корпоративної мережі, яка базується на моделі зрілості CISA's Zero Trust Maturity Model. Взаємодія компонентів у цій архітектурі дотримується певного циклу, який забезпечує дворівневе динамічне маркування даних для удосконалення аналізу при захисті інформаційних ресурсів, що відрізняє її від існуючих архітектур корпоративних мереж.

Практичне значення отриманих результатів полягає в наступному:

1. Отримані результати моделювання системи динамічного аналізу та маркування захисту інформаційних ресурсів, яка враховує семіотичні рівні, демонструють покращення показників безпеки. У результаті використання семіотичних механізмів інтерпретації загроз час реагування на інциденти скоротився з 500 мс до 416 мс, що становить покращення на 16% у порівнянні з системами Snort, SEMIoTICS та іншими засобами, які переважно застосовують сигнатурний або статичний аналіз. Встановлено, що рівень відповідності політикам безпеки зріс з 87% до 95%, що на 8% вище, ніж у класичних системах, таких як Splunk ES чи Semantic SIEM, які не враховують семіотичні зв'язки між подіями та значеннями.

2. Отримані результати при моделюванні оцінки рівня кібербезпеки власників мережі з інтегральним показником потенційних загроз дозволяють сформувати об'єктивну оцінку рівня кіберзахисту реальних власників інформаційних ресурсів із застосуванням семіотичного підходу. Отримані результати моделювання розробленої моделі забезпечують рівень виявлення складних загроз (APT, соціотехнічні атаки) 55%, що на 4% (з 51% до 55%) вище

ніж у систем Suricata, Snort та аналогічних рішень. F1-міра запропонованої системи становить 0.84, що перевищує значення у Splunk ES (0.76) та Snort (0.64) на 11%, демонструючи баланс між точністю та повнотою виявлення загроз.

3. Запропонований підхід з використанням розділення змішаного контенту інформації на взаємопов'язані рівні показав ймовірність успішного аналізу для нормального трафіку HTTP на рівні 0.99, що відповідає або перевищує аналогічні показники у відомих SIEM-системах на 3%. Таких як IBM QRadar або Splunk ES, де середній рівень точності обробки нормального трафіку за даними випробувань становить близько 0.95–0.97.

4. Запропоновані моделі можуть бути інтегровані у корпоративні мережі для підвищення рівня контролю доступу до інформаційних ресурсів. У сфері критичної інфраструктури (енергетика, транспорт, телекомунікації) розроблені методи можуть підвищити захищеність від атак на управлінські та SCADA-системи. Семіотична модель може бути використана як семантичний модуль підсистеми SASE архітектури.

За результатами дослідження підтверджено практичну та теоретичну цінність розроблених методів, надано практичні рекомендації, щодо застосування розроблених методів та визначено доцільність перспективи їх подальшого розвитку.

Ключові слова: кібербезпека, машинне навчання, інформаційна безпека, семантична подібність, моделювання, засоби штучного інтелекту, кіберфізичний простір, інфокомунікаційні мережі, криптографія, інформаційна система, комп'ютерні мережі, інформаційні технології.

Список публікацій здобувача

Наукові праці, в яких опубліковано основні наукові результати:

1. S. Yevseiev, M. Tolkachov, D. Shetty, V. Khvostenko, A. Strelnikova, S. Milevskyi, and S. Golovashych, "The concept of building security of the network with elements of the semiotic approach," *ScienceRise*, no. 1, pp. 24–34, 2023, doi: 10.21303/2313-8416.2023.002828. (Закордонне видання).

2. S. Yevseiev, N. Dzheniuk, M. Tolkachov, O. Milov, T. Voitko, M. Prygara, O. Shpak, N. Voropay, A. Volkov, and O. Lezik, "Development of a multi-loop security system of information interactions in socio-cyberphysical systems," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9(125), pp. 53–74, 2023, doi: 10.15587/1729-4061.2023.289467. (Scopus).

3. O. Serkov, N. Dzheniuk, O. Kasilov, G. Sokol, M. Tolkachov, and D. Arutiunian, "Інтелектуальна безпровідна система зв'язку," *Системи управління, навігації та зв'язку*, vol. 3, no. 77, pp. 206–210, 2024, doi: 10.26906/SUNZ.2024.3.206. (Б).

4. М. Ю. Толкачов, Н. В. Дженюк, А. Г. Захаржевський, С. С. Погасій, and С. І. Глухов, "Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору," *Сучасний захист інформації*, no. 1(57), pp. 57–68, 2024, doi: 10.31673/2409-7292.2024.010007. (Б).

5. M. Tolkachov, N. Dzheniuk, S. Yevseiev, Y. Lysetskyi, V. Shulha, I. Grod, S. Faraon, I. Ivanchenko, I. Pasko, and D. Balagura, "Development of a method for protecting information resources in a corporate network by segmenting traffic," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9(131), pp. 63–78, 2024, doi: 10.15587/1729-4061.2024.313158. (Scopus).

6. М. Ю. Толкачов, "Механізми захисту трафіку в кіберпросторі," *Сучасний захист інформації*, vol. 4, no. 60, pp. 85–99, 2024, doi: 10.31673/2409-7292.2024.040009. (Б).

Інші публікації:

7. S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev, O. Korol, S. Milevskyi *et al.*, and S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev, M. Tolkachov (Eds.), *Models of socio-cyber-physical systems security*, Monograph, Kharkiv: PC TECHNOLOGY CENTER, 2023, 184 p., doi: 10.15587/978-617-7319-72-5. (Scopus).

Опубліковані праці апробаційного характеру:

8. М. Ю. Толкачов, Н. В. Дженюк, "Підхід до побудови систем безпеки корпоративної мережі," in *XI Наукова конференція «Наукові підсумки 2022 року»*, Харків, Україна, 2022, p. 18, e-ISBN 978-617-7319-62-6.

9. Н.В. Дженюк, М.Ю. Толкачов. Формування класифікатора загроз на основі комплексування із загрозами методів соціальної інженерії. *VII Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення.* 1 листопада 2023 р. Кропивницький: ЦНТУ, 2023. 135 с. (С. 21)

10. М. Ю. Толкачов, Н. В. Дженюк, "Побудова багатоконтурної системи безпеки мереж за впливу соціологічних складових навантаження," in *XII Наукова конференція «Наукові підсумки 2023 року»*, Харків: ТЕХНОЛОГІЧНИЙ ЦЕНТР, 2023, pp. 56, e-ISBN 978-617-8360-00-9.

11. М. Ю. Толкачов, "Ієрархія надійності в кіберпросторі: від фізичних рівнів до соціальних аспектів," in *XIII Наукова конференція «Наукові підсумки 2024 року»*, Харків: ТЕХНОЛОГІЧНИЙ ЦЕНТР, 2024, p. 87, e-ISBN 978-617-8360-11-5.

Авторські свідоцтва, дипломи, патенти:

12. М. Ю. Толкачов, О. В. Халецький, and О. А. Серков, "Спосіб резервування інформаційно-обчислювальної системи," Патент України № 71503A, МПК G06F 11/18, заявл. 31.12.2003; опубл. 15.11.2004, Бюл. № 11.

13. О. А. Серков, В. С. Бреславець, І. Г. Перова, М. Ю. Толкачов, and Г. І. Чурюмов, "Спосіб генерації широкосмугового імпульсного сигналу та антена для його реалізації," Патент України № 120554 C2, МПК H01Q 21/06, H01Q 13/08, опубл. 26.12.2019, Бюл. № 24, заявка № a 2018 03104.

ABSTRACT

Tolkachov M.Yu. Modeling the Security of Internet Traffic as a Semiotic System. Qualification research paper submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy (PhD) in specialty 125 – Cybersecurity and Information Protection. – National Technical University "Kharkiv Polytechnic Institute", Kharkiv, 2025.

The dissertation is devoted to solving the scientific and technical problem of increasing the security level of systems that protect Internet traffic by developing and implementing mathematical models, monitoring methods, and control mechanisms for security system elements, taking into account various factors, including social and perceptual aspects.

The proposed approach ensures the protection of mixed content information based on semiotic analysis, which not only enhances the security of information resources but also provides flexible management of Internet traffic security.

The purpose of the dissertation is to develop models for Internet traffic security in the cyber-physical space based on a multi-level semiotic model that ensures an increased level of information protection.

Object of research: the process of creating and applying models and methods to ensure Internet traffic protection in the cyber-physical space.

Subject of research: modeling the security of Internet traffic as a semiotic system.

The introduction substantiates the relevance of the dissertation topic, formulates the research goal and applied scientific tasks necessary to achieve it, shows the connection with scientific programs and topics, and presents the scientific novelty, practical significance, and the author’s contribution. Information is provided about the approbation of results, the author's contribution, and related publications.

In the first chapter, analyzes the current state of Internet traffic protection, particularly methods for securing information resources in cyberspace. It discusses system architectures for network control and protection and their alignment with

modern threats. Models of cyberattacks on various types of infocommunication system traffic are analyzed, including real-time, streaming, elastic, and signaling traffic, and the most vulnerable segments of network infrastructure are identified. The threats to information security, including cyberterrorism and the use of digital technologies for mass manipulation, are assessed.

The need to enhance information resource protection in cyberspace by integrating modern traffic analysis and control methods is justified. A semiotic model-based approach is proposed, incorporating encryption, authentication, access control, and social interaction analysis mechanisms. The importance of developing universal security models that consider both technical and content characteristics of traffic is emphasized.

In the second chapter, presents a model of a semiotic system of cyberspace that accounts for interactions among users, content, and network infrastructure. The structure of Internet communication is analyzed, and key elements of their semiotic nature are identified, including syntactic, semantic, and pragmatic levels. The application of the semiotic model for cybersecurity assessment is discussed, enabling the detection and neutralization of potential threats through content analysis and its impact on network security.

The hierarchy of trust in cyberspace is explored, which includes physical, syntactic, semantic, pragmatic, and social levels. The use of semiotic methods for labeling and segmenting network traffic is proposed to improve information flow management and detect anomalous behavior patterns.

A security model based on the zero trust concept is proposed, involving a comprehensive approach to user authentication, network activity monitoring, and risk management. A methodology for access distribution and information flow control based on semiotic analysis is introduced, ensuring flexibility and effectiveness of cybersecurity policies.

In the third section, considers a semiotic approach to cybersecurity, integrating technical, semantic, pragmatic, and social aspects of threat analysis.

The semiotic model is improved to account for different levels of information – from syntactic and semantic to pragmatic and social. A method for targeted traffic segmentation using the CISA's Zero Trust Maturity Model is developed, providing more accurate access control and minimizing data compromise risks.

A two-level dynamic data labeling technique is proposed to improve information flow analysis and resource protection. Macrosegmentation and microsegmentation methods are developed to divide information flows according to security requirements and enhance access control. These methods are based on a comprehensive analysis of semiotic parameters, increasing cybersecurity system flexibility and adaptability to current threats.

An integral security indicator of network resources is introduced, forming a holistic approach to cybersecurity assessment from physical aspects (CVE Rating) to more abstract ones such as social impact (Social Level).

A methodology for dynamic cybersecurity monitoring and management based on semiotic analysis is developed. A protection method for mixed content in Internet traffic is proposed, enabling flexible management of security systems.

The developed methods of dynamic labeling and segmentation enhance data access control and reduce compromise risks.

In the fourth chapter, presents modeling of network owner cybersecurity levels based on Cisco Talos report data (2023). Modeling is performed using software applications and scripts in C# and Python 3.x with Pandas, NumPy, and SciPy libraries.

A method for protecting mixed content in Internet traffic based on semiotic analysis is proposed, integrating the zero trust strategy and modern analytics for qualitative and quantitative system evaluation.

For modeling, datasets CIC-IDS 2017/2018 and NSL-KDD 2022 were used, employing algorithms for attack detection and behavioral traffic analysis.

The conclusions summarize the main results of the research and characterize the effectiveness indicators of the proposed solutions.

Scientific contributions:

1. For the first time, an integral indicator of potential threats was developed, considering weighted averages of the levels of the cyber semiotic model: physical, empirical, syntactic, semantic, pragmatic, and social. The use of mixed content separation into interconnected levels allows the evaluation of targeted (mixed) attacks involving complex threats, setting it apart from traditional approaches.

2. An information resource analysis algorithm was developed, including syntactic, correlation, semantic, pragmatic analyses, and access level labeling. This step-by-step process forms a comprehensive protection system that reduces entropy, increases data transfer accuracy, and ensures security.

3. A model for dynamic analysis and protection labeling of information resources was developed, considering semiotic levels. It includes data security, system performance, resource cost, and privacy requirements. Methods of macro- and microsegmentation allow the division of information flows according to security requirements and efficient access control.

4. The "data-information-knowledge" semiotic structure was improved to visualize the relationships between these elements and demonstrate the connection between semiotics and sign usage in information processing.

5. A corporate network architecture based on the CISA's Zero Trust Maturity Model was improved. It features a specific component interaction cycle enabling two-level dynamic data labeling to improve protection analysis, differentiating it from existing corporate network architectures.

Practical significance:

1. The dynamic analysis and labeling system model considering semiotic levels demonstrated improved security metrics. Using semiotic threat interpretation mechanisms reduced incident response time from 500 ms to 416 ms (a 16% improvement) compared to systems like Snort or SEMIoTICS. Security policy compliance increased from 87% to 95%, 8% higher than classical systems like Splunk ES or Semantic SIEM.

2. Modeling of network owner cybersecurity levels using the integral threat indicator enabled objective assessment of real-world cybersecurity levels using a semiotic approach. The developed model achieved 55% detection of complex threats (e.g., APT, social engineering), 4% higher than Suricata and Snort. The proposed system's F1-score reached 0.84, outperforming Splunk ES (0.76) and Snort (0.64), reflecting better balance between precision and recall.

3. The approach using mixed content decomposition showed a 0.99 success rate in analyzing normal HTTP traffic, exceeding the average accuracy of known SIEM systems (IBM QRadar, Splunk ES) by 3% (typically ~0.95–0.97).

4. The proposed models can be integrated into corporate networks to enhance access control. In critical infrastructure (energy, transport, telecom), the methods improve protection of control and SCADA systems. The semiotic model can function as a semantic module in SASE architecture subsystems.

The research confirmed both the theoretical and practical value of the developed methods, provided practical recommendations for application, and demonstrated the feasibility of future development.

Keywords: cybersecurity, machine learning, information security, semantic similarity, modeling, artificial intelligence tools, cyber-physical space, infocommunication networks, cryptography, information system, computer networks, information technology.

List of publications of the acquirer

Scientific works in which the main scientific results were published:

1. S. Yevseiev, M. Tolkachov, D. Shetty, V. Khvostenko, A. Strelnikova, S. Milevskyi, and S. Golovashych, "The concept of building security of the network with elements of the semiotic approach," *ScienceRise*, no. 1, pp. 24–34, 2023, doi: 10.21303/2313-8416.2023.002828. (Foreign publication).

2. S. Yevseiev, N. Dzheniuk, M. Tolkachov, O. Milov, T. Voitko, M. Prygara, O. Shpak, N. Voropay, A. Volkov, and O. Lezik, "Development of a multi-loop security system of information interactions in socio-cyberphysical systems," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9(125), pp. 53–74, 2023, doi: 10.15587/1729-4061.2023.289467. (Scopus).

3. O. Serkov, N. Dzheniuk, O. Kasilov, G. Sokol, M. Tolkachov, and D. Arutiunian, "Intelligent wireless communication system," *Control, Navigation and Communication Systems*, vol. 3, no. 77, pp. 206–210, 2024, doi: 10.26906/SUNZ.2024.3.206. (Category B).

4. M. Yu. Tolkachov, N. V. Dzheniuk, A. H. Zakharzhevskyi, S. S. Pohasii, and S. I. Hlukhiv, "A method for protecting information resources based on a semiotic model of cyberspace," *Modern Information Protection*, no. 1(57), pp. 57–68, 2024, doi: 10.31673/2409-7292.2024.010007. (Category B).

5. M. Tolkachov, N. Dzheniuk, S. Yevseiev, Y. Lysetskyi, V. Shulha, I. Grod, S. Faraon, I. Ivanchenko, I. Pasko, and D. Balagura, "Development of a method for protecting information resources in a corporate network by segmenting traffic," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9(131), pp. 63–78, 2024, doi: 10.15587/1729-4061.2024.313158. (Scopus).

6. M. Yu. Tolkachov, "Mechanisms for protecting traffic in cyberspace," *Modern Information Protection*, vol. 4, no. 60, pp. 85–99, 2024, doi: 10.31673/2409-7292.2024.040009. (Category B).

Other publications:

7. S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev, O. Korol, S. Milevskyi et al., and S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev, M. Tolkachov (Eds.), *Models of Socio-Cyber-Physical Systems Security*, Monograph, Kharkiv: PC TECHNOLOGY CENTER, 2023, 184 p., doi: 10.15587/978-617-7319-72-5. (Scopus).

Published works of approbation nature:

8. M. Yu. Tolkachov, N. V. Dzheniuk, "An approach to building security systems of a corporate network," in *XI Scientific Conference "Scientific Results of 2022"*, Kharkiv, Ukraine, 2022, p. 18, e-ISBN 978-617-7319-62-6.

9. N. V. Dzheniuk, M. Yu. Tolkachov, "Formation of a threat classifier based on integration with social engineering threats," *VII International Scientific and Practical Conference "Information Security and Computer Technologies"* dedicated to the 30th anniversary of the Department of Cybersecurity and Software, November 1, 2023, Kropyvnytskyi: CNTU, 2023. 135 p. (p. 21).

10. M. Yu. Tolkachov, N. V. Dzheniuk, "Building a multi-loop network security system under the influence of sociological components of the load," in *XII Scientific Conference "Scientific Results of 2023"*, Kharkiv: TECHNOLOGY CENTER, 2023, p. 56, e-ISBN 978-617-8360-00-9.

11. M. Yu. Tolkachov, "Reliability hierarchy in cyberspace: from physical levels to social aspects," in *XIII Scientific Conference "Scientific Results of 2024"*, Kharkiv: TECHNOLOGY CENTER, 2024, p. 87, e-ISBN 978-617-8360-11-5.

Patents and certificates of inventions:

12. M. Yu. Tolkachov, O. V. Khaletskyi, and O. A. Serkov, "Method of reservation of an information and computing system," Patent of Ukraine No. 71503A, IPC G06F 11/18, filed 31.12.2003; published 15.11.2004, Bulletin No. 11.

13. O. A. Serkov, V. S. Breslavets, I. H. Perova, M. Yu. Tolkachov, and H. I. Churyumov, "Method for generating a broadband pulse signal and an antenna for its

implementation," Patent of Ukraine No. 120554 C2, IPC H01Q 21/06, H01Q 13/08, published 26.12.2019, Bulletin No. 24, application No. a 2018 03104.