Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U002731

Особливі позначки: відкрита

Дата реєстрації: 07-07-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Толкачов Максим Юрійович
2. Maksym Y. Tolkachov

Кваліфікація:

Ідентифікатор ORCHID ID: 0000-0001-7853-5855

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 125 Кібербезпека (12 Інформаційні технології)

Дата захисту: 28-08-2025

Спеціальність за освітою: Автоматика і телемеханіка

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 10017

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56

Тема дисертації:

1. Моделювання безпеки інтернет-трафіку як семіотичної системи
2. Modeling the Security of Internet Traffic as a Semiotic System

Реферат:

1. 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. У першому розділі проаналізовано сучасний стан захищеності інтернет-трафіку, зокрема методи захисту інформаційних ресурсів у кіберпросторі. У другому розділі запропонована модель семіотичної системи кіберпростору, що враховує взаємодію між користувачами, контентом та мережевою інфраструктурою. 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. У третьому розділі розглянуто семіотичний підхід до забезпечення кібербезпеки, який забезпечує інтеграцію технічних, семантичних, прагматичних та соціальних аспектів аналізу загроз. У четвертому розділі проведено моделювання оцінки рівня кібербезпеки власників мережі. Моделювання проведено на основі даних звіту Cisco Talos за 2023 р. 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. Вперше розроблений інтегральний показник потенційних загроз, який враховує зважене середнє показників рівнів семіотичної моделі кіберпростору: фізичного, емпіричного, синтаксичного, семантичного, прагматичного та соціального. Вперше розроблений алгоритм аналізу інформаційних ресурсів, який включає кілька основних етапів, таких як синтаксичний аналіз, кореляційний аналіз, семантичний аналіз, прагматичний аналіз, маркування рівнів доступу. Вперше розроблена модель системи динамічного аналізу та маркування захисту інформаційних ресурсів, яка враховує семіотичні рівні. Удосконалена семіотична структура "данні-інформація-знання", яка для опису інформації візуалізує зв'язки цих різних термінів. Удосконалена архітектура корпоративної мережі, яка базується на моделі зрілості CISA's Zero Trust Maturity Model. Отримані результати моделювання системи динамічного аналізу та маркування захисту інформаційних ресурсів, яка враховує семіотичні рівні, демонструють покращення показників безпеки. 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. 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%. 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.

2. The dissertation is dedicated to solving a scientific and technical problem of enhancing the security level of Internet traffic protection systems by developing and implementing mathematical models, monitoring methods, and management of security system elements, taking into account various factors, including social and perceptual aspects. The proposed approach enables the protection of mixed-content information based on semiotic analysis, which not only increases the level of information resource security but also provides flexibility in managing Internet traffic security. The aim of the dissertation is to develop Internet traffic security models in the cyber-physical space based on a multi-level semiotic model, which ensures an increased level of information protection systems' security. Object of the study: the process of creating and using models and methods for ensuring Internet

traffic protection in the cyber-physical space. Subject of the study: modeling Internet traffic security as a semiotic system. The introduction justifies the relevance of the dissertation topic, defines the research goal, and formulates scientific and applied tasks necessary to achieve it. In the first chapter, the current state of Internet traffic security is analyzed, in particular, methods for protecting information resources in cyberspace. In the second chapter, a model of the semiotic system of cyberspace is proposed, which considers the interaction between users, content, and network infrastructure. A hierarchy of reliability in cyberspace is examined, which includes physical, syntactic, semantic, pragmatic, and social levels. The use of semiotic methods for tagging and segmenting network traffic is proposed, enabling improved information flow management and the detection of anomalous behavioral patterns. The third chapter explores a semiotic approach to cybersecurity, which integrates technical, semantic, pragmatic, and social aspects of threat analysis. The fourth chapter presents the modeling of cybersecurity level assessment for network owners. The modeling is based on data from the Cisco Talos 2023 report. To perform the modeling, datasets CIC-IDS 2017/2018 and NSL-KDD 2022 were used. These datasets are based on attack detection algorithms and analysis of behavioral traffic characteristics. The conclusions of the dissertation outline the main results derived from the conducted research and present the performance indicators of the proposed solutions. For the first time, an integrated indicator of potential threats was developed, taking into account the weighted average of the levels of the semiotic model of cyberspace: physical, empirical, syntactic, semantic, pragmatic, and social. For the first time, an information resource analysis algorithm was developed, including several key stages such as syntactic analysis, correlation analysis, semantic analysis, pragmatic analysis, and access level labeling. For the first time, a model of a dynamic analysis and labeling system for protecting information resources was developed, taking into account semiotic levels. The semiotic structure of "data–information–knowledge" has been improved to visualize the relationships among these different concepts. The corporate network architecture was improved based on the CISA Zero Trust Maturity Model. The obtained results of modeling the dynamic analysis and labeling system for information resource protection, considering semiotic levels, demonstrate improved security indicators. The modeling results of cybersecurity level assessment for network owners, using the integrated indicator of potential threats, enable an objective evaluation of the cybersecurity status of actual information resource owners through a semiotic approach. The proposed approach, which uses the decomposition of mixed-content information into interrelated levels, demonstrated a probability of successful analysis for normal HTTP traffic at 0.99, which matches or exceeds similar performance metrics of known SIEM systems by 3%. The proposed models can be integrated into corporate networks to enhance access control to information resources. In the field of critical infrastructure (energy, transportation, telecommunications), the developed methods can improve protection against attacks on management and SCADA systems. The semiotic model can also be used as a semantic module in SASE architecture subsystems. Based on the research results, the practical and theoretical value of the developed methods has been confirmed. Practical recommendations for the application of the developed methods have been provided, and the feasibility of their further development has been determined.

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:

- 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.
- 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.

- 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.
- 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.
- 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 (індексується базою Scopus)
- 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 (індексується базою Scopus)
- М. Ю. Толкачов, О. В. Халецький, and О. А. Серков, "Спосіб резервування інформаційно-обчислювальної системи," Патент України № 71503А, МПК G06F 11/18, заявл. 31.12.2003; опубл. 15.11.2004, Бюл. № 11.
- 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 С2, МПК H01Q 21/06, H01Q 13/08, опубл. 26.12.2019, Бюл. № 24, заявка № а 2018 03104.
- 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.
- 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.
- Н. В. Дженюк, М. Ю. Толкачов, "Формування класифікатора загроз на основі комплексування із загрозами методів соціальної інженерії," in VII Міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології”, Кропивницький: ЦНТУ, 2023, p. 21.
- 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.
- 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.

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

Соціально-економічна спрямованість: підвищення захисту інформації в компьютерних системах і мережах

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Король Ольга Григорівна

2. Olga H. Korol

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

Ідентифікатор ORCHID ID: 0000-0002-8733-9984

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii A. Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCHID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна
2. Nadiia Kazakova

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

Ідентифікатор ORCHID ID: 0000-0003-3968-4094

Додаткова інформація:

Повне найменування юридичної особи: Одеський національний університет імені І. І. Мечникова

Код за ЄДРПОУ: 02071091

Місцезнаходження: вул. Дворянська, буд. 2, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Копп Андрій Михайлович
2. Andrii M. Kopp

Кваліфікація: д.філософ, доц., 122

Ідентифікатор ORCHID ID: 0000-0002-3189-5623

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Ткачов Андрій Михайлович
2. Andrii M. Tkachov

Кваліфікація: к. т. н., старший науковий співробітник, 20.02.12

Ідентифікатор ORCHID ID: 0000-0003-1428-0173

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Кучук Георгій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Кучук Георгій Анатолійович
Відповідальний за підготовку облікових документів	Толкачов Максим Юрійович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна