

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004046

Особливі позначки: відкрита

Дата реєстрації: 29-07-2026

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. МЄШКОВ Вадим Ігорович

2. Vadym I. Mieshkov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 04-08-2026

Спеціальність за освітою: захист інформації в комп'ютерних системах та мережах

Місце роботи здобувача: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, 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 15516

Повне найменування юридичної особи: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, 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: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.55.01, 20.56

Тема дисертації:

1. Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак
2. Information Technology for Intelligent Monitoring of Computer Network Traffic for Intrusion Detection Systems

Реферат/анотація:

1. Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки галузі знань 12 Інформаційні технології. – Національний технічний університет «Дніпровська політехніка», Дніпро, 2026. Метою дисертаційної роботи є розв'язання актуальної науково-прикладної задачі підвищення ефективності виявлення атак і розпізнавання їх типів у комп'ютерних мережах шляхом розроблення інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак (СВА), що базується на методах машинного навчання та забезпечує функціонування в бінарному і багатокласовому режимах аналізу. Актуальність теми зумовлена зростанням кількості та складності кіберзагроз, збільшенням обсягів мережевого трафіку, динамічністю його характеристик, а також обмеженістю традиційних сигнатурних методів під час виявлення нових, модифікованих і малопоширених атак. У зв'язку з цим

важливого значення набуває застосування методів машинного навчання, які дають змогу виявляти статистичні закономірності в мережевому трафіку та формувати рішення щодо наявності атакуючої активності і типу виявленої загрози. У вступі обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету і завдання роботи, визначено об'єкт, предмет і методи дослідження, розкрито наукову новизну та практичне значення одержаних результатів. У першому розділі проаналізовано сучасні методи та засоби моніторингу мережевого трафіку й виявлення атак, розглянуто класифікацію систем IDS/IPS, особливості сигнатурних, аномальних і гібридних методів виявлення загроз. Узагальнено особливості застосування методів машинного навчання в задачах аналізу мережевого трафіку, охарактеризовано сучасні набори даних для дослідження систем виявлення атак (СВА) та обґрунтовано вибір набору CICIDS2017 як репрезентативної основи для проведення відтворюваного експериментального дослідження. Показано, що ефективність інтелектуального виявлення атак визначається не лише вибором моделі машинного навчання, а й якістю підготовки даних, коректністю формування ознакового простору та обґрунтованістю системи оцінювання результатів. У другому розділі сформульовано постановку задачі інтелектуального виявлення атак у мережевому трафіку та визначено методичні засади її розв'язання в межах задач машинного навчання. Задачу дослідження розглянуто у двох взаємопов'язаних постановках: бінарній класифікації, спрямованій на відокремлення нормального мережевого трафіку від атакуючого, та багатокласовій класифікації, орієнтованій на розпізнавання конкретних типів атак. Охарактеризовано набір даних CIC-IDS2017 як експериментальну основу дослідження, визначено його структуру, особливості класів трафіку та підходи до формування вибірок для подальшого навчання й тестування моделей. Розроблено метод підготовки даних, класифікації та оцінювання мережевого трафіку для систем виявлення атак. У межах методу передбачено послідовне виконання процедур очищення, уніфікації та стандартизації даних, аналізу ознак і зниження розмірності простору даних, формування та балансування вибірок для бінарної і багатокласової класифікації. Обґрунтовано вибір моделей машинного навчання для задач виявлення атак і розпізнавання їх типів, а також визначено систему метрик оцінювання якості моделей і порядок організації експериментального дослідження. Запропоновано узагальнений алгоритм методу, який формалізує послідовність етапів обробки мережевого трафіку, побудови класифікаційних моделей та оцінювання їх ефективності, що створює методичну основу для подальшої розробки інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для СВА.

2. Dissertation for the degree of Doctor of Philosophy in the specialty 122 Computer Science, field of knowledge 12 Information Technology. – Dnipro University of Technology, Dnipro, 2026. The aim of this dissertation is to address a pressing scientific-applied problem of improving the efficiency of attack detection and classification in computer networks by developing an information technology for intelligent monitoring of computer network traffic for attack detection systems (ADS), based on machine learning methods and capable of operating in both binary and multi-class analysis modes. The relevance of this topic stems from the growing number and complexity of cyber threats, the increase in network traffic volumes, the dynamic nature of its characteristics, and the limitations of traditional signature-based methods in detecting new, modified, and rare attacks. In this regard, the use of machine learning methods becomes crucial, as they enable the identification of statistical patterns in network traffic and the formulation of decisions regarding the presence of attack activity and the type of detected threat. The introduction justifies the relevance of the dissertation topic, formulates the purpose and objectives of the study, defines the object, subject, and methods of the research, and highlights the scientific novelty and practical significance of the findings. The first chapter analyzes modern methods and tools for monitoring network traffic and detecting attacks, and examines the classification of IDS/IPS systems, as well as the characteristics of signature-based, anomaly-based, and hybrid threat detection methods. It summarizes the features of applying machine learning methods to network traffic analysis tasks, describes modern datasets for studying intrusion detection systems (IDS), and justifies the selection of the CIC-IDS2017 dataset as a representative basis for conducting a reproducible experimental study. It is shown that the effectiveness of intelligent attack detection is determined not only by the choice of a machine learning model, but also by the quality of data preparation, the correctness of feature space formation, and the soundness of the result evaluation system. The second chapter

formulates the problem of intelligent attack detection in network traffic and defines the methodological foundations for solving it within the framework of machine learning. The research problem is considered in two interrelated formulations: binary classification, aimed at distinguishing normal network traffic from attack traffic, and multi-class classification, focused on recognizing specific types of attacks. The CIC-IDS2017 dataset is characterized as the experimental basis of the study; its structure, the characteristics of traffic classes, and approaches to forming samples for subsequent training and testing of models are defined. A method for data preparation, classification, and evaluation of network traffic for attack detection systems has been developed. The method involves the sequential execution of procedures for data cleaning, unification, and standardization; feature analysis and dimensionality reduction of the data space; and the formation and balancing of samples for binary and multi-class classification. The selection of machine learning models for attack detection and type recognition tasks is justified, and a system of metrics for evaluating model quality and the procedure for organizing experimental research are defined. A generalized algorithm for the method is proposed, which formalizes the sequence of steps involved in processing network traffic, building classification models, and evaluating their effectiveness, thereby establishing a methodological foundation for the further development of information technology for intelligent monitoring of computer network traffic for IDS.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Не застосовується

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- Мешков, В. (2025). Методи машинного навчання для бінарної та багатокласової класифікації мережевого трафіку у системах виявлення атак. Таврійський науковий вісник. Серія: Технічні науки. Т. 1, № 4. С. 182–196.
- Мешков, В. (2025). Метод попередньої обробки даних для створення інформаційних моделей в інтелектуальних системах виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, №2. С. 108–114
- Сафаров, О., Корнієнко, В., Горєв, В., Мешков, В. (2024). Підвищення кібербезпеки електронних комунікаційних систем медичного призначення. Information Technology: Computer Science, Software Engineering and Cyber Security, № 2, С. 128–133
- Мешков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, № 1, С. 85–92

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0225U004731

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Корнієнко Валерій Іванович
2. Valerii I. Korniienko

Кваліфікація: д.т.н., доц., професор, 05.13.07

Ідентифікатор ORCID ID: 0000-0002-0800-3359

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, 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. Смірнова Тетяна Віталіївна
2. Tetiana V. Smirnova

Кваліфікація: к. т. н., доц., 05.02.01

Ідентифікатор ORCID ID: 0000-0001-6896-0612

Додаткова інформація:

Повне найменування юридичної особи: Центральнуукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Гулак Геннадій Миколайович
2. Hennadii M. Hulak

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0001-9131-9233

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:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Алексеев Михайло Олександрович

2. Mykhaylo Aleksyeyev

Кваліфікація: д.т.н., проф., 05.13.07

Ідентифікатор ORCID ID: 0000-0001-8726-7469

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Герасіна Олександра Володимирівна

2. Oleksandra V. Gerasina

Кваліфікація: к. т. н., 05.13.07

Ідентифікатор ORCID ID: 0000-0002-8196-0657

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові
голови ради

Мороз Борис Іванович

Власне Прізвище Ім'я По-батькові
головуючого на засіданні

Мороз Борис Іванович

Відповідальний за підготовку
облікових документів

Макуріна Олександра Андріївна

Реєстратор

Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності



Юрченко Тетяна Анатоліївна