Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U003113

Особливі позначки: відкрита

Дата реєстрації: 23-07-2025

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ від 29.08.2025 №1592/ст

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Петляк Наталія Сергіївна

2. Nataliia Petliak

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

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: Кібербезпека

Дата захисту: 14-08-2025

Спеціальність за освітою: 123 - «Комп'ютерна інженерія»

Місце роботи здобувача: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, 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 9612

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, 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: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 49.33.35, 50.37.23, 50.39.21, 50.41.27

Тема дисертації:

1. Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах
2. Models and methods for detecting abnormal traffic in information and communication systems

Реферат:

1. В умовах цифровізації інформаційна безпека (ІБ) стає важливою для організацій різного масштабу. Одним із напрямів є виявлення аномалій у мережевому трафіку, що дає змогу фіксувати загрози, які не відповідають відомим шаблонам атак. Хоча системи виявлення вторгнень широко застосовуються і аналізують трафік у реальному часі, більшість з них усе ще базуються на сигнатурному аналізі, ефективність якого обмежена. Такий підхід не справляється з новими, прихованими або розподіленими у часі атаками. Тому актуальним є розвиток інтелектуальних систем, що орієнтуються на виявлення аномальної активності. У вступі обґрунтовано актуальність дисертаційної роботи, сформульовано мету та основні завдання дослідження, наведено відомості щодо зв'язку роботи з науковим темами. У першому розділі представлено комплексний огляд сучасного стану ІБ в контексті зростаючих загроз для інформаційно-комунікаційних систем (ІКС). Зроблено акцент на особливості виявлення аномалій саме у вихідному трафіку, який часто не охоплюється

традиційними системами захисту. У другому розділі представлено моделі процесів, що описують поведінку користувачів і потенційних зловмисників у мережі, а також моделей класифікації мережевого трафіку з метою виявлення аномалій. Розроблено модель поведінки порушника та сформовано модель сигнатури пакету. Впроваджено концепцію нечіткої класифікації, формалізовано моделі, які у подальшому використовуються як складові частини при розробці методів виявлення аномалій. У третьому розділі здійснено розробку та вдосконалення методів виявлення аномального трафіку. Покращено метод класифікації трафіку за ознаками. Вдосконалено метод класифікації на основі самоподібності, який аналізує мережевий трафік у часових вікнах, дозволяючи виявити відхилення від звичних моделей поведінки у мережі. Запропоновано нечіткий метод виявлення аномалій, який оперує правилами нечіткої логіки для оцінки рівня загрози. Створено гібридний метод, що об'єднує метод класифікації трафіку за ознаками, на основі самоподібності та нечіткий метод, в єдину систему. У четвертому розділі дисертації реалізовано структурну модель системи виявлення аномального трафіку на основі розробленого гібридного методу. Описано особливості реалізації кожного з етапів функціонування системи — від захоплення та попередньої обробки трафіку до прийняття рішення щодо безпечності з'єднання. Окрему увагу приділено реалізації модулів на практиці, зокрема у тестовому середовищі. Проведено низку експериментів, що включали різні сценарії роботи мережі, типи атак і варіації навантаження. Результати оцінки достовірності свідчать про підвищення точності виявлення аномалій при використанні гібридного підходу порівняно з окремими методами. У висновках узагальнено результати виконаного дослідження, обґрунтовано наукову новизну розроблених моделей та методів, а також доведено їхню практичну ефективність. На підставі теоретичних і практичних досліджень, виконаних у дисертаційній роботі, отримано такі нові результати: □ Вдосконалено модель сигнатури пакету для пошуку аномального трафіку, що за рахунок виключення з параметрів сигнатури розміру заголовка, контрольної суми заголовку, корисного розміру пакета, мітки потоку, пріоритету пакету, контрольної суми пакету за принципом Парето, забезпечило зменшення часу аналізу трафіку. □ Вдосконалено модель процесу нечіткого виявлення аномального трафіку, в якій за рахунок використання експертного підходу сформована множина правил та набір відповідних лінгвістичних змінних, що дозволило розробити нові підходи до виявлення аномального трафіку в ІКС. □ Вперше розроблено гібридний метод виявлення аномального трафіку в ІКС в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та розробленої моделі процесу нечіткого виявлення дозволило динамічно формувати множини сигнатур при класифікації трафіку за ознаками та підвищити показники виявлення аномального трафіку. □ Удосконалено структурну модель системи виявлення аномального трафіку в ІКС, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в ІКС та динамічного варіювання множиною дозволених та заборонених з'єднань у режимі реального часу дозволило зменшити навантаження на процесор. Одержані в дисертаційній роботі результати стали підґрунтям для забезпечення зменшення обсягів аномального трафіку в ІКС. Практично вагомими вважаються такі результати: розроблено алгоритмічне забезпечення системи виявлення аномального трафіку в ІКС, що реалізує гібридний метод, його складові метод класифікації трафіку за ознаками, метод самоподібності, нечіткий метод та моделі, що в них використовуються; на основі алгоритму розроблено програмний застосунок, що дозволяє проводити аналіз трафіку в ІКС; можливість практичного використання розробленого програмного застосунку сумісно з маршрутизаторами в ІКС.

2. In the context of digitalization, information security (IS) is becoming important for organizations of all sizes. One of the areas of focus is detecting anomalies in network traffic, which allows you to detect threats that do not match known attack patterns. Although intrusion detection systems are widely used and analyze traffic in real time, most of them are still based on signature analysis, which is limited in its effectiveness. This approach cannot cope with new, hidden or time-distributed attacks. Therefore, the development of intelligent systems focused on detecting anomalous activity is relevant. The introduction substantiates the relevance of the dissertation, formulates the purpose and main objectives of the study, and provides information on the relationship of the work to scientific topics. The first chapter provides a comprehensive overview of the current state of IS in the context of growing threats to information and communication systems (ICS). The emphasis is placed on the peculiarities of

detecting anomalies in outbound traffic, which is often not covered by traditional security systems. The second section presents models of processes that describe the behavior of users and potential attackers in the network, as well as models for classifying network traffic to detect anomalies. A model of intruder behavior is developed and a packet signature model is formed. The concept of fuzzy classification is introduced, and models are formalized, which are further used as components in the development of anomaly detection methods. In the third chapter, we develop and improve methods for detecting anomalous traffic. The method of traffic classification by features has been improved. The self-similarity-based classification method, which analyzes network traffic in time windows, has been improved, allowing to detect deviations from the usual patterns of behavior in the network. A fuzzy anomaly detection method is proposed, which operates on fuzzy logic rules to assess the level of threat. A hybrid method has been created that combines the method of traffic classification by features based on self-similarity and the fuzzy method into a single system. The fourth chapter of the thesis presents a structural model of the anomalous traffic detection system based on the developed hybrid method. It outlines the implementation of each system stage—from traffic capture and preprocessing to deciding on connection security. Particular attention is given to practical implementation in a test environment. Several experiments were conducted, involving various network scenarios, attack types, and load levels. Reliability assessment results show improved anomaly detection accuracy using the hybrid method compared to individual approaches. The conclusions summarize the results of the study, substantiate the scientific novelty of the developed models and methods, and prove their practical effectiveness. Based on the theoretical and practical research carried out in this thesis, the following new results were obtained: □ A packet signature model for detecting anomalous traffic has been improved, which, by excluding header size, header checksum, payload size, flow label, packet priority, and Pareto checksum from the signature parameters, has reduced the time for traffic analysis. □ The model of the process of fuzzy detection of anomalous traffic was improved, in which a set of rules and a set of relevant linguistic variables were formed using an expert approach, which allowed to develop new approaches to detecting anomalous traffic in ICS. □ For the first time, a hybrid method for detecting anomalous traffic in ICS has been developed, which, by integrating the method of traffic classification by features, the method of self-similarity and the developed model of the fuzzy detection process, allowed to dynamically form sets of signatures when classifying traffic by features and increase the detection rate of anomalous traffic. □ The structural model of the system for detecting anomalous traffic in ICS was improved, which, by integrating the developed hybrid method for detecting anomalous traffic in ICS and dynamically varying the set of allowed and prohibited connections in real time, reduced the load on the processor. The results obtained in this dissertation became the basis for reducing the volume of anomalous traffic in the ICS. The following results are considered practically significant: algorithmic support for the system for detecting anomalous traffic in the ICS, which implements a hybrid method, its components: a method for classifying traffic by features, a self-similarity method, a fuzzy method and the models used in them; based on the algorithm, a software application was developed that allows analyzing traffic in the ICS; the possibility of practical use of the developed software application in conjunction with routers in the ICS.

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. Тітова В.Ю., Кльоц Ю.П., Петляк Н.С., Капустян М.В.. Fuzzy inference subsystem for classifying threats to computer information. Вимірювальна та обчислювальна техніка в технологічних процесах. 2022. № 1. С. 57-61

- 2. Кльоц Ю.П., Петляк Н.С.. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2022. № 3. С. 79-86. DOI: 10.31891/2219-9365-2022-71-3-9
- 3. Мостовий С.В., Петляк Н.С., Голота І.О.. Дослідження ефективності інструментів виявлення і запобігання вторгнень на вузли в корпоративних мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2023. № 2. С. 5-8. DOI: 10.31891/2219-9365-2023-74-1
- 4. Nataliia Petliak, Yuliia Khokhlachova. Method of analysis of outgoing traffic package signatures. Захист інформації. 2024. № 1. С. 179-187. DOI: 10.18372/2410-7840.26.18841
- 5. Петляк Н.С. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2025. № 1. С. 180-186. DOI: 10.31891/2219-9365-2025-81-21
- 6. Петляк Н.С.. Гібридний метод та система виявлення аномального трафіку в інформаційно-комунікаційних системах. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025. №2. С. 561-569. DOI: 10.31891/2307-5732-2025-349-82.
- 7. Klots Y., Titova V., Petliak N., Cheshun V., Salem A.-B.M.. Research of the Neural Network Module for Detecting Anomalies in Network Traffic. 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS 2022), Khmelnytskyi, 23-25 March 2022. Vol. 3156, P. 378 - 389. ISSN 16130073
- 8. Petliak N., Klots Y., Titova V., Cheshun V., Boyarchuk A.. Signature-based Approach to Detecting Malicious Outgoing Traffic. 4th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntellTSIS 2023), Khmelnytskyi, 22-23 March 2023. Vol. 3373. P. 486 - 506. ISSN 16130073
- 9. Klots Y., Petliak N., Titova V.. Evaluation of the efficiency of the system for detecting malicious outgoing traffic in public networks. 13th International Conference on Dependable Systems, Services and Technologies (DESSERT 2023), Athens, 13-15 October 2023. DOI: 10.1109/DESSERT61349.2023.10416502
- 10. Klots Y., Petliak N., Martsenko S., Tymoshchuk V., Bondarenko I.. Machine Learning system for detecting malicious traffic generated by IoT devices. nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024), Ternopil, 12 June 2024. Vol. 3742. P. 97 - 110. ISSN 16130073
- 11. Titova V., Klots Y., Petliak N., Cheshun V., Salem A.-B.M.. Detection of network attacks in cyber-physical systems using a rule-based logical neural network. 1st International Workshop on Intelligent and CyberPhysical Systems (ICyberPhyS 2024), Khmelnytskyi, 28 June 2024. Vol. 3736. P. 255 - 268. ISSN 16130073
- 12. Petliak N., Klots Y., Titova V., Salem A.-B.M.. Attack detection system based on network traffic analysis by means of fuzzy inference. 1st International Workshop on Advanced Applied Information Technologies (AdvAIT 2024), Khmelnytskyi, 5 December 2024. Vol. 3899. P. 201-213.ISSN 16130073
- 13. Петляк Н.С., Кльоц Ю.П., Хохлачова Ю.Є.. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. Інформаційна, функційна і кібербезпека: тези доп. II студ. наук.-техн. к. (м. Харків, 30 листопада – 1 грудня 2022 р.) Х., 2022. С. 45-46
- 14. Петляк Н.С., Кльоц Ю.П.. Підхід до аналізу вихідного трафіку на основі сигнатур. Інформаційна безпека та комп'ютерні технології: тези доп. VI міжнар. наук.-пр. конф. (м. Кропивницький, 20-21 квітня 2023 р.) Кр., 2023. С. 3-4
- 15. Петляк Н.С., Кльоц Ю.П., Хохлачова Ю.Є.. Підхід до аналізу вихідного трафіку. Безпека інформаційних технологій: тези доп. XII міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). К., 2023. С. 97-99
- 16. Петляк Н.С., Кльоц Ю.П., Тітова В.Ю., Чешун В.М. Виявлення зловмисного вихідного трафіку мережі на основі нечіткого логічного висновку. Захист інформації і безпека інформаційних систем: тези доп. IX міжнар. наук.-техн. конф. (м. Львів, 25-26 травня 2023 р.) Л., 2023. С. 33-35
- 17. Петляк Н.С., Кльоц Ю.П.. Метод ідентифікації вторгнень на основі алгоритму визначення самоподібності трафіку та алгоритмів нечіткої логіки. Безпека інформаційних технологій: тези доп. XIII міжнар. наук.-техн. конф. (м. Львів, 9-11 травня 2024 р.) Л., 2024. С. 117-119.

Наукова (науково-технічна) продукція: технології

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

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U201817

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Лазаренко Сергій Володимирович
2. Serhii Lazarenko

Кваліфікація: д. т. н., професор, 21.02.03

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Кльоц Юрій Павлович
2. Yuriy Klots Yuriy

Кваліфікація: к.т.н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0002-3914-0989

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, 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. Корченко Анна Олександрівна

2. Anna Korchenko

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

Ідентифікатор ORCID ID: 0000-0003-0016-1966

Додаткова інформація:

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

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, буд. 19, 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. Казмірчук Світлана Володимирівна

2. Svitlana Kazmirchuk

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

Ідентифікатор ORCID ID: 0000-0001-6083-251X

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Одарченко Роман Сергійович

2. Roman Odarchenko

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-7130-1375

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Ільєнко Анна Вадимівна

2. Anna Ilienko

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

Ідентифікатор ORCID ID: 0000-0001-8565-1117

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Гнатюк Сергій Олександрович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Гнатюк Сергій Олександрович
Відповідальний за підготовку облікових документів	Довженко Олена Андріївна
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна