Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U000466

Особливі позначки: відкрита

Дата реєстрації: 05-03-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Штанько Вадим Ігорович
2. Vadym I. Shtanko

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: Інформаційні технології

Дата захисту: 14-04-2026

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, 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 198

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, 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 університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23, 20.56, 20.56.01, 20.56.02, 20.56.03

Тема дисертації:

1. Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак
2. Information Technology for a Two-Level Intelligent Network Attack Analysis System

Реферат:

1. У дисертації досліджено методи та моделі аналізу мережевого трафіку, алгоритми машинного навчання та підходи до побудови дворівневих систем виявлення вторгнень у контексті забезпечення адаптивного кіберзахисту інформаційно-комунікаційних систем. Окреслені теоретичні засади формують методологічну основу для створення інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак, що забезпечує автоматизоване виявлення, класифікацію та інтерпретацію атипової мережевої активності у віртуалізованому середовищі. Актуальність дослідження зумовлена зростанням інтенсивності та складності кібератак, поширенням гібридних загроз, а також необхідністю переходу від сигнатурного до поведінкового аналізу мережевого трафіку із використанням методів машинного навчання. Розвиток хмарних технологій, розподілених обчислювальних середовищ і сервіс-орієнтованих архітектур обумовлює підвищення вимог до систем виявлення вторгнень щодо масштабованості, адаптивності та здатності

функціонувати в умовах змінного статистичного профілю трафіку. Традиційні сигнатурні підходи демонструють обмежену ефективність у разі появи нових або модифікованих сценаріїв атак. У зв'язку з цим обґрунтовано доцільність використання ймовірнісних та ансамблевих моделей машинного навчання як складових ієрархічної системи прийняття рішень. На основі публічного набору даних USB-IDS-1 та власноруч сформованих наборів трафіку, отриманих в ізольованому віртуальному середовищі на базі GNS3 та VirtualBox, створено емпіричну базу дослідження обсягом понад 6 млн мережевих пакетів, агрегованих у потокове представлення з використанням віконної сегментації. Це дозволило провести комплексний аналіз статистичних характеристик трафіку, сформувати навчальні та тестові вибірки для різних сценаріїв функціонування системи та дослідити вплив зсуву домену (domain shift) на якість класифікації. Встановлено, що зміна розподілів ознак істотно впливає на поведінку моделей, що підтверджує необхідність формалізованого врахування цього явища в процедурі прийняття рішень. Встановлено, що використання на першому рівні ієрархії наївного баєсівського класифікатора як бінарного фільтра забезпечує ефективне відокремлення нормативного трафіку від атак із мінімальними обчислювальними витратами. На другому рівні застосування ансамблевих методів, зокрема випадкового лісу, дозволяє здійснювати детальну багатокласову атрибуцію типів атак. У режимі узгодженого домену середнє значення accuracy для бінарної класифікації досягає 0,97, а для багатокласової – 0,89, що свідчить про високу здатність системи до розпізнавання типів вторгнень. У разі зміни статистичного профілю трафіку спостерігається закономірна деградація метрик, що підтверджує чутливість моделей до зсуву домену та необхідність адаптивного налаштування порогів прийняття рішень. Обґрунтовано математичну модель дворівневої системи класифікації як задачу мінімізації очікуваного баєсівського ризику з урахуванням асиметрії вартості помилок першого та другого роду. Аналітично виведено порогові умови прийняття рішення для кожного рівня ієрархії. Запропоновано механізм адаптивного коригування порогів на основі зваженої дивергенції Кульбака– Лейблера, що дозволяє кількісно оцінювати ступінь статистичної розбіжності між поточним та еталонним трафіком і відповідно регулювати чутливість системи без повного перенавчання моделей. Розроблено архітектуру інформаційної технології, яка реалізує замкнений цикл «генерація – детерміноване маркування – потокова класифікація» у віртуалізованому середовищі. Використання детермінованого маркування пакетів на етапі емуляції забезпечує формування верифікованих наборів даних для навчання та тестування моделей, що підвищує достовірність експериментальних результатів. Перехід від статичних інтегральних показників до синхронного віконного аналізу метрик надійності дав змогу оцінювати стабільність функціонування системи у часовому розрізі та виявляти деградацію якості класифікації в динамічних умовах. Одержані результати реалізовано у вигляді програмної системи аналізу мережевого трафіку з керованою політикою прийняття рішень, що передбачає механізм обробки невизначених станів («Unknown») та процедуру відмови від рішення у випадках підвищеної статистичної невизначеності. Запропонована модульна архітектура забезпечує можливість інтеграції з наявними засобами моніторингу мережевої безпеки та підтримує масштабування з урахуванням появи нових типів кіберзагроз. Реалізований підхід створює передумови для впровадження адаптивних систем виявлення вторгнень і підвищення стійкості інформаційно-комунікаційних систем до сучасних кібератак.

2. The dissertation investigates methods and models for network traffic analysis, machine learning algorithms, and approaches to building two-level intrusion detection systems in the context of ensuring adaptive cybersecurity of information and communication systems. The outlined theoretical foundations form the methodological basis for creating an information technology of a two-level intelligent system for network attack analysis, which provides automated detection, classification, and interpretation of anomalous network activity in a virtualized environment. The relevance of the study is conditioned by the growing intensity and complexity of cyberattacks, the spread of hybrid threats, and the need to shift from signature-based to behavioral analysis of network traffic using machine learning methods. The development of cloud technologies, distributed computing environments, and service-oriented architectures increases the requirements for intrusion detection systems in terms of scalability, adaptability, and the ability to operate under dynamically changing traffic profiles. Traditional signature-based approaches demonstrate limited effectiveness in the case of new or modified attack scenarios. In this regard, the

feasibility of using probabilistic and ensemble machine learning models as components of a hierarchical decision-making system is substantiated. Based on the public USB-IDS-1 dataset and custom traffic datasets collected in an isolated virtual environment using GNS3 and VirtualBox, an empirical research base was formed, comprising more than 6 million network packets aggregated into flowbased representations with window segmentation. This enabled a comprehensive analysis of traffic statistical characteristics, the formation of training and test datasets for various operational scenarios, and the study of the impact of domain shift on classification performance. It was established that changes in feature distributions significantly affect model behavior, confirming the necessity of formally incorporating this phenomenon into the decision-making procedure. It was found that using a Naive Bayes classifier as a binary filter at the first level of the hierarchy ensures effective separation of normal traffic from attacks with minimal computational cost. At the second level, the application of ensemble methods, particularly Random Forest, enables detailed multiclass attribution of attack types. In the in-domain setting, the average accuracy reaches 0.97 for binary classification and 0.89 for multiclass attribution, indicating a high capability of the system to identify intrusion types. When the statistical profile of traffic changes, a consistent degradation of metrics is observed, confirming model sensitivity to domain shift and the necessity of adaptive threshold adjustment. A mathematical model of the two-level classification system is substantiated as a problem of minimizing expected Bayesian risk with consideration of asymmetric costs of type I and type II errors. Threshold decision rules for each hierarchical level are derived analytically. An adaptive threshold adjustment mechanism based on weighted Kullback–Leibler divergence is proposed, allowing quantitative estimation of statistical divergence between current and reference traffic and enabling sensitivity regulation without full model retraining. An information technology architecture has been developed that implements a closed-loop cycle of “generation – deterministic labeling – flow-based classification” in a virtualized environment. The use of deterministic packet labeling at the emulation stage ensures the formation of verified datasets for model training and testing, thereby increasing the reliability of experimental results. The transition from static integral metrics to synchronous window-based reliability analysis enables the assessment of system stability over time and the detection of classification performance degradation under dynamic operating conditions. The obtained results are implemented in the form of an program system for network traffic analysis with a controlled decision-making policy, including a mechanism for handling uncertain states (“Unknown”) and a rejection option in cases of increased statistical uncertainty. The proposed modular architecture ensures integration with existing network security monitoring tools and supports scalability to accommodate new types of cyber threats. The implemented approach creates the prerequisites for deploying adaptive intrusion detection systems and enhancing the resilience of information and communication systems against modern cyberattacks.

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:

- Konyrbaev N., Nikitenko Ye., Shtanko V., Lakhno V., Baishemirov Z., Ibadulla S., Galymzhankyzy A., Myrzabek E. Evaluation and Optimization of the Naive Bayes Algorithm for Intrusion Detection Systems Using the USB-IDS-1 Dataset. Eastern-European Journal of Enterprise Technologies. 2024. Vol. 6. No. 2 (132). P. 74–82.
- Штанько В., Нікітенко Є. Проєктування та реалізація віртуального середовища для аналізу мережевого трафіку. Наука і техніка сьогодні. 2025. № 7 (48). С. 2028–2045.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація; розроблено інформаційну технологію аналізу мережевих атак у віртуалізованому середовищі, яка, на відміну від наявних, реалізує замкнений цикл «генерація – маркування – потокова класифікація» та використовує

детерміноване маркування пакетів на етапі емуляції, що забезпечує формування верифікованих наборів даних для навчання моделей без необхідності евристичної розмітки

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:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Нікітенко Євгеній Васильович
2. Yevhenii V. Nikitenko

Кваліфікація: к. ф.-м. н., доц., 01.04.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, 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. Толюпа Сергій Васильович
2. Serhii V. Toliupa

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

Ідентифікатор ORCID ID: 0000-0002-1919-9174

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Ушенко Юрій Олександрович
2. Yurii O. Ushenko

Кваліфікація: д. ф.-м. н., професор, 01.04.05

Ідентифікатор ORCID ID: 0000-0003-1767-1882

Додаткова інформація:
https://www.scopus.com/authid/detail.uri?authorId=6701840218;http://www.researcherid.com/rid/S-3308-2016;http://orcid.org/0000-0003-1767-1882;https://scholar.google.com/citations?hl=ru&user=bySBprcAAAAJ&view_op=list_works&sortby=pubdate

Повне найменування юридичної особи: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Криворучко Олена Володимирівна
2. Olena V. Kryvoruchko

Кваліфікація: д. т. н., професор, 05.13.22

Ідентифікатор ORCID ID: 0000-0002-7661-9227

Додаткова інформація:

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Сагун Андрій Вікторович

2. Andrii V. Sahun

Кваліфікація: к. т. н., доц., 01.05.02

Ідентифікатор ORCID ID: 0000-0002-5151-9203

Додаткова інформація:

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Шкарупило Вадим Вікторович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Шкарупило Вадим Вікторович
Відповідальний за підготовку облікових документів	Боярчук Сергій Васильович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна