Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U002589

Особливі позначки: відкрита

Дата реєстрації: 02-07-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Панчук Богдан Олександрович
2. Bogdan O. Panchuk

Кваліфікація:

Ідентифікатор ORCHID 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: 26-06-2025

Спеціальність за освітою: Комп'ютерні науки

Місце роботи здобувача: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 8756

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

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

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.23.37, 20.54.06, 20.56.01

Тема дисертації:

1. Виявлення мережевих атак алгоритмами штучного інтелекту
2. Detection of Network Attacks Using Artificial Intelligence Algorithms

Реферат:

1. Дисертаційна робота присвячена дослідженню методів оцінюванню та підвищенню стійкості систем виявлення шкідливого мережевого трафіку на основі штучного інтелекту, до змагальних впливів з урахуванням семантики можливих дій зловмисника. Основним завданням дисертаційної роботи є створення системи виявлення зразків трафіку ботнетів та спорідненого зловмисного програмного забезпечення з підвищеною стійкістю до спроб навмисного ухилення від виявлення та формально верифікованими оцінками показників стійкості. На відміну від споріднених робіт в області аналізу мережевих даних моделями ШІ, де увага зосереджується лише на проблемі підвищення точності класифікації, в цьому

досліджені вирішується актуальна науково-прикладна задача - підвищення стійкості систем виявлення до можливих «змагальних атак» направлених супроти моделі з ціллю приховування зловмисної мережевої активності. Також надаються оцінки стійкості класифікатора потоків мережевих даних до атак такого роду, перевірені за допомогою формальних методів верифікації. В роботі вперше формалізовано критерій локальної стійкості класифікатора мережевого трафіка та здійснено його верифікацію шляхом автоматичного доведення (чи спростування) виконуваності накладених на модель обмежень за допомогою SMT-розв'язувача, що дозволило достовірно оцінити стійкість створеної системи виявлення загроз до можливих збурень у вхідних даних. Також вперше розроблено універсальний метод формальної верифікації властивостей глибоких нейронних мереж з кусково-лінійними функціями активації, який базується на представленні обчислювального графу нейромережі у формі спрощеної SMT-формули, побудованої інкрементально шляхом розв’язування локальних SMT-задач сформованих для функцій активації нейронів та перевірки можливості їх тотожної заміни на лінійні функції. Для підвищення точності та стійкості моделей класифікації в роботі було розвинено метод генерації штучних прикладів та доповнення наборів даних шляхом адаптації швидкого методу знаку градієнту до простору ознак мережевих потоків, з метою оцінки та підвищення стійкості систем виявлення шкідливого трафіку до можливих змагальних атак. В ході роботи було здійснено навчання класифікаторів мережевого трафіку на базі алгоритмів машинного навчання та нейронних мереж з використанням різних наборів мережевих даних. Для навчання та тестування було створено розширену вибірку даних на основі комбінації різних відкритих наборів. На основі отриманих моделей класифікації був створений прототип багатоцільового аналізатора мережевого трафіку. Його вихідний код та детальні інструкцій до використання опубліковані на ресурсі Github. Екземпляр прототипу було впроваджено в експлуатацію у ролі системи виявлення мережевих загроз у компанії ТОВ «НВП «Радікс», що спеціалізується на розробці апаратного забезпечення для АЕС.

2. The dissertation is dedicated to the study of methods for assessing and improving the robustness of artificial intelligence-based systems for detecting malicious network traffic against adversarial influences, taking into account the semantics of potential attacker actions. The main objective of the dissertation is to develop a detection system for traffic samples of botnets and other related types of malicious software with enhanced resistance to deliberate evasion attempts and formally verified robustness metrics. Unlike related works in the field of network data analysis using AI models, which primarily focus on improving classification accuracy, this research addresses a pressing scientific and practical challenge—enhancing the resilience of detection systems against potential adversarial attacks aimed at concealing malicious network activity. The study also provides robustness evaluations of network flow classifiers against such attacks, validated using formal verification methods. For the first time, the criterion of local robustness for network traffic classifiers has been formalized and verified through automated proofs (or refutations) of the satisfiability of model constraints using an SMT solver. This approach enabled a reliable assessment of the threat detection system's resilience to perturbations in input data. Additionally, a universal method for formal verification of deep neural networks with piecewise-linear activation functions was developed for the first time. It is based on representing the computational graph of the neural network as a simplified SMT formula constructed incrementally by solving local SMT problems for activation functions and verifying the possibility of their identical substitution with linear functions. To enhance both the accuracy and robustness of classification models, the work advances a method for generating artificial examples and augmenting datasets by adapting the Fast Gradient Sign Method (FGSM) to the feature space of network flows. This technique aims to evaluate and improve the resilience of malicious traffic detection systems against adversarial attacks. During the research, traffic classifiers based on machine learning algorithms and neural networks were trained using various network datasets. An extended dataset was constructed by combining multiple public datasets for training and testing purposes. Using the resulting classification models, a prototype of a multi-purpose network traffic analyzer was developed. Its source code and detailed usage instructions have been published on GitHub. A prototype instance has been deployed as a network threat detection system at Radics LLC, a company specializing in hardware development for nuclear power plants.

Державний реєстраційний номер ДіР: 0122U001164

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- Панчук Б. Виявлення ботнет-трафіку на основі потоків, використовуючи ШІ. Проблеми програмування. 2022. №3-4. С. 376-386.
- Панчук Б.О. Генерація та використання змагальної вибірки для протидії ухиленню ботнетів від виявлення нейронними мережами (до 100-річчя з дня народження академіка В.М. Глушкова). Проблеми керування та інформатики. 2023. 68(5). С. 71–85.
- Панчук Б. Формальна верифікація нейронних мереж глибокого навчання. Проблеми програмування. 2024. №2-3. С. 253-262.
- Летичевський О., Панчук Б. Проблема точності в системах протидії кібератакам та верифікація нейронних мереж на прикладі задачі виявлення ботнетів. Кібернетика та системний аналіз. 2025. 61(2). С. 3–12.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: посилення інформаційної безпеки мережевих технологій

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U001164

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Летичевський Олександр Олександрович

2. Oleksandr O. Letychevsky

Кваліфікація: д. ф.-м. н., старший науковий співробітник, 01.05.03

Ідентифікатор ORCHID ID: 0000-0003-0856-9771

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=55557358400

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Ізонін Іван Вікторович
2. Ivan V. Izonin

Кваліфікація: к. т. н., 05.13.23

Ідентифікатор ORCHID ID: 0000-0002-9761-0096

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=38461225700

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Гордєєв Олександр Олександрович
2. Oleksandr O. Gordieiev

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

Ідентифікатор ORCHID ID: 0000-0003-2517-9388

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=56447150300

Повне найменування юридичної особи: Луцький національний технічний університет

Код за ЄДРПОУ: 05477296

Місцезнаходження: вул. Львівська, буд. 75, Луцьк, Луцький р-н., 43018, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Пепеляєв Володимир Анатолійович
2. Volodymyr A. Pepeliaiev

Кваліфікація: д.ф.-м.н., с.н.с., 01.05.02

Ідентифікатор ORCHID ID: 0009-0009-3169-1776

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=8967548400

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

Власне Прізвище Ім'я По-батькові:

1. Горбачук Василь Михайлович
2. Vasyl M. Gorbachuk

Кваліфікація: д. ф.-м. н., професор, 01.05.01

Ідентифікатор ORCHID ID: 0000-0001-5619-6979

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=55646075900

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Сектор науки: Академічний

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Будник Микола Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Будник Микола Миколайович
Відповідальний за підготовку облікових документів	Стовба Віктор Олександрович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна