Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U000678

Особливі позначки: відкрита

Дата реєстрації: 27-02-2025

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ №35-ас/ВС від 26.05.2025

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Міщенко Максим Валерійович
2. Maksym Mishchenko

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0001-9769-9759

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: 05-05-2025

Спеціальність за освітою: Інженерія програмного забезпечення

Місце роботи здобувача: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, 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 7847

Повне найменування юридичної особи: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, 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 "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54, 20.56, 20.56.02

Тема дисертації:

1. Прогнозування та виявлення загроз для корпоративних комп’ютерних мереж засобами експертних систем
2. Forecasting and detection of threats to corporate computer networks using expert systems

Реферат:

1. В роботі вирішено актуальне наукове завдання з розробки моделей та методів виявлення та прогнозування загроз для корпоративних комп’ютерних мереж засобами експертних систем для підвищення точності виявлень та оперативності прийняття рішень щодо реагування на наявні та можливі загрози. Об’єктом дослідження є інформаційні процеси захисту корпоративних комп’ютерних мереж від кіберзагроз. Предметом дослідження є методи, моделі та елементи інформаційної технології виявлення та прогнозування кіберзагроз для корпоративних комп’ютерних мереж засобами експертних систем. Метою дисертаційного дослідження є підвищення оперативності виявлення загроз та забезпечення підтримки прийняття рішень щодо реагування на наявні та можливі вразливості корпоративних комп’ютерних мереж. Завдання дослідження полягає у створенні методів виявлення та прогнозування загроз для корпоративних комп'ютерних мереж, а також створення моделі інформаційної технології, що враховує комплексне використання запропонованих методів та засобів експертних систем для підтримки прийняття рішень. У першому розділі проведено аналіз основних типів загроз інформаційній безпеці корпоративних

комп'ютерних мереж, шляхів їх потрапляння до корпоративної мережі та механізмів їх дії. Було визначено модель загрози для корпоративної комп'ютерної мережі та змодельовано процес виявлення загроз. Представлено порівняльний аналіз існуючих систем та підходів виявлення загроз для корпоративних мереж. У другому розділі запропоновано модель комплексної інформаційної технології виявлення загроз з використанням експертних оцінок для подальшого прогнозування ймовірності реалізації визначених векторів вразливостей та формування рекомендацій з протидії загрозам на основі Теорії Ігор. Також розроблено методи виявлення загроз, результати яких використовуються для наповнення бази знань експертної системи. Серед методів виявлення загроз запропоновано метод визначення та класифікації секції Linux ELF файлу для ідентифікації шкідливого ПЗ та обґрунтовано актуальність виявлення загроз для UNIX-подібних систем. В порівнянні з існуючим дослідженим методом ідентифікації шкідливого ПЗ для UNIX-подібних систем, запропонований метод показав статистично значуще покращення точності та F1-міри. Досліджено застосування моделей NLP до виявлення загроз, в результаті чого запропоновано метод ідентифікації шкідливих Windows PE файлі з використанням моделі word2vec. Для виявлення мережевих аномалій запропоновано метод, що здатний виявляти DDoS атаки з урахуванням часового контексту рядів спостережень мережевих параметрів. У якості методу прогнозування загроз запропоновано використання мереж Баєса для формування ймовірності настання загрози на основі аналізу мережевого трафіку. Також було проаналізовано систему кількісної оцінки загроз CVSS, яка стала основою для побудови рушія висновків інформаційної технології підтримки прийняття рішень щодо захисту корпоративних комп'ютерних мереж. У третьому розділі представлено загальну функціональну модель інформаційної системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж, що визначає основні вхідні та вихідні параметри, обмеження та механізми виконання з трьома рівнями деталізації. Проведено моделювання інформаційної системи з використанням UML діаграм, що дозволило виділити основні варіанти використання інформаційної технології. Четвертий розділ містить розроблені модулі інформаційної системи виявлення та прогнозування загроз для корпоративних комп'ютерних мереж. Наведені результати експериментів, які підтверджують ефективність запропонованих методів та моделей. Основні результати дослідження та наукова новизна роботи полягають в розробці та удосконаленні методів та моделей виявлення та прогнозування загроз для корпоративних комп'ютерних мереж з використанням статистичних моделей, методів машинного навчання та засобів експертних систем. Визначено основні сутності, що в сукупності являють собою модель кіберзагрози та аналізуються в процесі її виявлення, що дозволило сформувати набір методів для забезпечення захисту корпоративних комп'ютерних мереж. Представлені методи підвищують ефективність процесу виявлення загроз за рахунок зменшення часу на їх ідентифікацію та підвищення точності. В роботі запропоновано поєднання засобів експертних систем з запропонованими методами виявлення та прогнозування загроз, що забезпечує процес підтримки прийняття рішень щодо реагування на існуючі та прогнозовані вразливості. Створена функціональна модель інформаційної системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж, що містить інформацію про основні вхідні та вихідні параметри, обмеження, ресурси, деталізацію процесів виявлення та прогнозування загроз та може бути основою для проектування систем захисту корпоративних комп'ютерних мереж.

2. The thesis solves a current scientific task of developing models and methods for detecting and predicting threats to corporate computer networks using expert systems to increase the accuracy of detection and the efficiency of decision-making regarding response to existing and potential threats. The object of the research is the information processes for protecting corporate computer networks from cyber threats. The subject of the research is methods, models, and elements of information technology for detecting and predicting cyber threats for corporate computer networks using expert systems. The purpose of the research is to increase the efficiency of threat detection and provide decision support for responding to existing and potential vulnerabilities in corporate computer networks. The research objective is to create methods for detecting and predicting threats to corporate computer networks, as well as to create an information technology model that takes into account the comprehensive use of the proposed methods and tools of expert systems to support decision-making. The first

chapter analyzes the main types of threats to information security for corporate computer networks, the ways they enter the corporate network and the mechanisms of their action. The threat model for the corporate computer network was defined and the threat detection process was simulated. A comparative analysis of approaches and existing threat detection systems for corporate networks is presented. The second chapter proposes a model of comprehensive information technology for threat detection using expert assessments for further prediction of the probability of implementation of certain vulnerability vectors and generation of recommendations for countering threats using Game Theory. Threat detection methods are also developed, the results of which are used to fill the expert system's knowledge base. Among the threat detection methods, a method for determining and classifying the Linux ELF file section for identifying malicious software is proposed and the relevance of threat detection for UNIX-like systems is substantiated. Compared with the existing researched method for identifying malicious software for UNIX-like systems, the proposed method showed a statistically significant improvement in accuracy and F1-measure. The application of NLP models to threat detection is investigated, as a result of which a method for identifying malicious Windows PE files using the word2vec model is proposed. To detect network anomalies, a method is proposed that is capable of detecting DDoS attacks taking into account the time context of series of observations of network parameters. As a threat prediction method, the use of Bayesian networks is proposed to form the probability of a threat based on network traffic analysis. The CVSS threat quantification system was also analyzed, which became the basis for building an information technology inference engine to support decision-making in protecting corporate computer networks. The third chapter presents a general functional model of an information system for detecting and predicting cyber threats for corporate computer networks, which defines the main input and output parameters, constraints, and execution mechanisms with three levels of detail. Modeling of the information system was carried out using UML diagrams, which allowed us to identify the main options for using information technology. The fourth chapter contains the developed modules of the information system for detecting and predicting threats to corporate computer networks. The results of experiments are presented, which confirm the effectiveness of the proposed methods and models. The main results of the research and the scientific novelty of the work consist in improving the methods and models of detecting and predicting threats to corporate computer networks using statistical models, machine learning methods, and expert systems. The main entities that collectively constitute a cyberthreat model and are analyzed in the process of its detection have been identified, which has allowed the formation of a set of methods for ensuring the protection of corporate computer networks. The presented methods increase the efficiency of the threat detection process by reducing the time for their identification and increasing accuracy. The work proposes a combination of expert system tools with the proposed methods of detecting and predicting threats, which, due to expert assessments and the driver of conclusions, provides a decision-making support process for responding to existing and predicted vulnerabilities.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Не застосовується

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 1. А.Г. Гребенник, О.В. Трунова, В.В. Казимир, М.В. Міщенко «Виявлення та прогнозування загроз для корпоративної комп'ютерної мережі.» Технічні науки та технології, 2020. - № 2 – с.175–184.
- 2. Mishchenko M.V., Dorosh M.S.. "Semantic analysis and classification of malware for UNIX-like operating systems with the use of machine learning methods". Applied Aspects of Information Technology. 2022; Vol. 5, No. 4: 371-386, DOI: https://doi.org/10.15276/aait.05.2022.25.
- 3. Mishchenko, M. V., Dorosh, M. S.. (2024). «An expert system of recommendations for combating cyber threats using CVSS metrics and game theory.» Вісник сучасних інформаційних технологій, 7(3), 284–295.

https://doi.org/10.15276/hait.07.2024.20
- 4. Міщенко, М. «Функціональна модель системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж з використанням експертних оцінок.» Технічні науки та технології – 2024. № 3 (37), - с. 143–152. https://doi.org/10.25140/2411-5363-2024-3(37)-143-152
- 5. Mishchenko, M., & Dorosh, M. (2024). Detection of Windows Portable Executable Malware using NLP Techniques and Proxy-server. International Journal of Computing, 23(4), 663-672. https://doi.org/10.47839/ijc.23.4.3765
- 6. Міщенко М.В., Гребенник А.Г., Трунова О.В.. "Прогнозування рівня загроз з використанням мереж Байєса" XV міжнародна науково-практична конференція математичне та імітаційне моделювання систем МОДС 2020. С. 120-123.
- 7. Міщенко М.В. «Створення сервісу для виявлення шкідливих elf файлів за допомогою машинного навчання з використанням хмарних технологій aws» Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених НОВІТНІ ТЕХНОЛОГІЇ У НАУКОВІЙ ДІЯЛЬНОСТІ І НАВЧАЛЬНОМУ ПРОЦЕСІ. – 2023 – с.107-108.
- 8. Міщенко М.В. «Створення експертної системи генерації рекомендацій з протидії кібератакам з використанням теорії ігор.» XIV Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених ЮНІСТЬ НАУКИ – 2024 – с. 1175-1176.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

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. Дорош Марія Сергіївна

2. Mariia S. Dorosh

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

Ідентифікатор ORCID ID: 0000-0001-6537-9857

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=56912183600; https://publons.com/researcher/3150165/mariia-dorosh/; https://www.researchgate.net/profile/Mariia_Dorosh2; https://scholar.google.com.ua/citations?hl=uk&user=saY6cfkAAAAJ; https://dblp.org/pid/256/0170.html

Повне найменування юридичної особи: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, 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. Стеценко Інна Вячеславівна
2. Inna V. Stetsenko

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

Ідентифікатор ORCID ID: 0000-0002-4601-0058

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Хлапонін Юрій Іванович
2. Yurii Khlaponin

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

Ідентифікатор ORCID ID: 0000-0002-9287-0817

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет будівництва і архітектури

Код за ЄДРПОУ: 02070909

Місцезнаходження: проспект Повітряних сил, буд. 31, Київ, 03037, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Зайцев Сергій Васильович
2. Serhii V. Zaitsev

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

Ідентифікатор ORCID ID: 0000-0001-6643-917X

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Акименко Андрій Миколайович
2. Andrii M. Akymenko

Кваліфікація: к. ф.-м. н., доц., 01.01.02

Ідентифікатор ORCID ID: 0000-0002-4594-6559

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Шелест Михайло Євгенович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Шелест Михайло Євгенович
Відповідальний за підготовку облікових документів	Лисенко Наталія Володимирівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна