Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002612

Особливі позначки: відкрита

Дата реєстрації: 16-07-2024

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: №1791 СТ від 18 вересня 2024 р.

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бондаренко Кирило Олександрович
2. Kyrylo O. Bondarenko

Кваліфікація: 125

Ідентифікатор ORCID ID: 0000-0002-2168-155X

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: 02-09-2024

Спеціальність за освітою: менеджмент

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.050.148-6619

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, 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 "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, 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

Тема дисертації:

1. Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки

2. Mathematical models and computational methods for detecting anomalies in security systems

Реферат:

1. Бондаренко К.О. Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації, галузь знань 12 – Інформаційні технології, Національний технічний університет “Харківський Політехнічний Інститут”, Міністерства освіти і науки України, Харків, 2024. Дисертація присвячена вирішенню завдання забезпечення належного рівня безпеки захищаємих об’єктів шляхом розробки та впровадження математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки. Завдяки використанню розроблених моделей та методів інтелектуального аналізу даних та нейронних мереж для виявлення аномалій стає можливим виявляти та попереджувати невідомі системі безпеки атаки, що є необхідною умовою для підвищення рівня кібербезпеки

будь якої системи. Об’єкт дослідження – процеси виявлення аномалій в системах безпеки захисту інформації. Предмет дослідження – математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки на основі методів нейроних мереж та інтелектуального аналізу даних (дерев класифікації). Метою дисертаційної роботи є розробка математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки, які забезпечують підвищення рівня безпеки систем захисту інформації. Сама система повинна бути проста у використанні та налаштуванні, а також легко переноситися між різними програмними системами. У вступі обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв’язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача. Подано відомості про апробацію результатів роботи, особистий внесок здобувача та його публікації. У першому розділі виконано аналіз сучасного стану виявлення аномалій в системах безпеки, розглянуті мережеві аномалії, їх походження та таксономія. Виявлені джерела походження аномалій в системах безпеки. Наведено зіставлення аномалій з кібератаками, які здійснюються на комп'ютерні системи та мережі та представлено причинно-наслідковий зв’язок між атаками зловмисників, мережевими аномаліями та їх наслідками для безпеки мережі організації. Побудовано відображення впливу аномалій мережевих послуг на цілі безпеки та якості обслуговування. У другому розділі проаналізовано існуючі теоретичні моделі виявлення аномалій: операційна модель, модель середнього значення та середньоквадратичного відхилення, багатоваріаційна модель, модель марковського процесу, модель часових серій. Запропоновано алгоритм виявлення вторгнень. Проаналізовані атрибути заходів та методів виявлення аномалій, що дозволило визначити відповідні методи виявлення аномалії. Проведений аналіз метрик аномалій на основі мір близькості дозволив обґрунтувати вибір міри близькості Махалонобіса як основи метрики аномалій. У третьому розділі проаналізовані різні методи виявлення аномалій на основі машинного навчання. Сформульовані відповідності використовуваних методів машинного навчання штучних нейронних мереж та задач кібербезпеки. Розроблена математична модель виявлення аномалій та вторгнень на основі генетичних алгоритмів. У четвертому розділі запропоновано підхід, який послідовно класифікує відомий трафік атак на різні типи атак та паралельно відокремлює аномалії від звичайного трафіку. Продемонстровано застосування моделі виявлення зловживань щодо набору даних KDD CUP 99. Запропоновано використання генетичного алгоритму для вибору відповідних значень параметрів, оптимізації RF-класифікатора та підвищення точності класифікації нормального та аномального мережевого трафіку та її реалізація з використанням побудованої штучної нейронної мережі багаторівневого перцептрона та методів побудови дерев класифікації у пакеті Statistica. У висновках дисертаційної роботи викладено основні результати які випливають з проведених досліджень, представлено та охарактеризовано показники ефективності при використанні запропонованих рішень. За результатами дослідження отримано такі наукові результати: 1. Вперше обґрунтовано вибір метрики Махаланобіса як основи для визначення аномалій. 2. Удосконалено систему причинно-наслідкових зв’язків між атаками зловмисників, мережевими аномаліями та їх наслідками для безпеки мережі організації. 3. Удосконалено математичну модель виявлення аномалій та вторгнень на основі генетичних алгоритмів. 4. Удосконалено підхід, послідовної класифікації відомого трафіку атак на різні типи атак. Практичне значення результатів: розроблені моделі побудови випадкового лісу з використанням генетичних алгоритмів; методи нейрокомп’ютінгу дозволяють побудувати структурні схеми модулів виявлення аномалій в системах кібербезпеки; реалізовані структурні схеми модулів у програмному забезпеченні при моделюванні нейронної мережі.

2. Bondarenko K.O. Mathematical models and computational methods for detecting anomalies in security systems - Qualification scientific work on the rights of manuscript. Dissertation for the degree of Doctor of Philosophy in speciality 125 Cybersecurity and Information Protection, field of knowledge 12 - Information Technology, National Technical University "Kharkiv Polytechnic Institute", Ministry of Education and Science of Ukraine, Kharkiv, 2024. The dissertation is devoted to solving the problem of ensuring an adequate level of security of protected objects by developing and implementing mathematical models and computational methods for detecting anomalies in security systems. By using the developed models and methods of data mining and neural networks for anomaly

detection, it becomes possible to detect and prevent attacks unknown to the security system, which is a prerequisite for improving the cybersecurity of any system. The object of research is the processes of detecting anomalies in information security systems. The subject of the research is mathematical models and computational methods for detecting anomalies in security systems based on neural network and data mining (classification trees) methods. The purpose of the dissertation is to develop mathematical models and computational methods for detecting anomalies in security systems that ensure an increase in the level of security of information protection systems. The system itself should be easy to use and configure, as well as easily transferable between different software systems. The introduction substantiates the relevance of the topic of the dissertation research, formulates the purpose of the research and the scientific and applied tasks necessary to achieve it, shows the connection of the research with scientific programmes and topics, presents the scientific novelty of the results obtained, their practical value and the personal contribution of the applicant. Information on the testing of the results of the work, the personal contribution of the applicant and his publications is provided. The first chapter analyses the current state of anomaly detection in security systems, discusses network anomalies, their origin and taxonomy. The sources of anomalies in security systems are identified. A comparison of anomalies with cyber attacks on computer systems and networks is provided, and the cause-and-effect relationship between intruder attacks, network anomalies and their consequences for the security of an organisation's network is presented. A reflection of the impact of network service anomalies on security and quality of service goals is built. The second section analyses the existing theoretical models of anomaly detection: operational model, mean and standard deviation model, multivariate model, Markov process model, time series model. An intrusion detection algorithm is proposed. The attributes of measures and methods of anomaly detection are analysed, which allowed to determine the appropriate methods of anomaly detection. The analysis of anomaly metrics based on proximity measures allowed to justify the choice of the Mahalonobis proximity measure as the basis of anomaly metrics. Section 3 analyses various methods of anomaly detection based on machine learning. The correspondence between the used machine learning methods for artificial neural networks and cybersecurity tasks is formulated. A mathematical model of anomaly and intrusion detection based on genetic algorithms is developed. In the fourth section, an approach is proposed that consistently classifies known attack traffic into different types of attacks and simultaneously separates anomalies from normal traffic. The application of the abuse detection model to the KDD CUP 99 dataset is demonstrated. It is proposed to use a genetic algorithm to select appropriate parameter values, optimise the RF classifier and improve the accuracy of classification of normal and anomalous network traffic and its implementation using the built artificial neural network of a multi-level perceptron and methods of building classification trees in the Statistica package. The conclusions of the dissertation outline the main results arising from the research, present and characterise the performance indicators when using the proposed solutions. The following scientific results were obtained as a result of the study: 1. For the first time, the choice of the Mahalanobis metric as a basis for determining anomalies is substantiated. 2. The system of cause-and-effect relationships between intruder attacks, network anomalies and their consequences for the security of an organisation's network has been improved 3. The mathematical model for detecting anomalies and intrusions based on genetic algorithms has been improved 4. An improved approach to the sequential classification of known attack traffic into different types of attacks.

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:

- Євсеєв С. П., Хвостенко В. С., Бондаренко К. О. Розробка комплексного показника якості обслуговування на основі постквантових алгоритмів. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2021. Т. 3 (65). С. 82-88 (Б)
- Shmatko O., Herasymov S., Lysetskyi Y., Yevseiev S., Sievierinov O., Voitko T., Zakharzhevskyi A., Makogon H., Nesterov A., Bondarenko K. Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologie. 2023. Kharkiv. 6(9 (126). P. 39 – 49 (А)
- Havrylova A. A., Korol O. G., Voropay N. I., Sevriukova Y. O., Bondarenko K. O. Analysis of cryptographic authentication and manipulation detection methods for big data. Сучасний захист інформації. Київ: Державний університет інформаційно-комунікаційних технологій, 2024. 1(57). P. 97–102 (Б)
- Бондаренко К. О. Аналіз і вибір релевантної метрики виявлення мережних аномалій. Сучасний стан наукових досліджень та технологій в промисловості. Харків, 2023. 4(26). С. 145–157 (Б).
- Herasymov S., Soroka V., Yevseiev S., Milevskyi S., Bondarenko K. Development of a method for measuring small nonlinear distortions of periodic electrical signals. International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). Ankara: IEEE, 2022. P. 45 – 52 (Scopus, Туреччина)
- Yevseiev S., Milevskyi S., Bortnik L., Voropay A., Bondarenko K., Pohasii S. Socio-cyber-physical systems security concept. Proceedings of the IVth International congress on Human-computer interaction, optimization and robotic applications (HORA). Ankara: IEEE, 2022, Paper ID 393 (Scopus, Туреччина).
- Євсеєв С. П., Хвостенко В. С., Бондаренко К. О. Комплексний показник якості обслуговування клієнтів Ethernet-мереж на основі постквантових алгоритмів, IX Міжнародна науково-технічна конференція "Інформатика, управління та штучний інтелект – 2022". Харків-Краматорськ, 2022. С. 45
- Tomashevsky B., Zviertseva N., Bondarenko K. Cyber security technology assessment metrics, VIIIth International Scientific and Technical Conference "Information protection and information systems security". Lviv, 2021. P. 39-40

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

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: ДР № 0123U101018, ДР № 0123U101020, ДР № 0123U101018

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Євсеєв Сергій Петрович

2. Serhii P. Yevseiev

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0003-1647-6444

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, 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. Лаптєв Олександр Анатолійович
2. Oleksandr A. Laptiev

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-4194-402X

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університ імені Тараса Шевченка

Код за ЄДРПОУ: 02070994

Місцезнаходження: , Київ, 01601, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii A. Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кучук Георгій Анатолійович

2. Heorhii A. Kuchuk

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

Ідентифікатор ORCID ID: 0000-0002-2862-438X

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Копп Андрій Михайлович

2. Andrii M. Kopp

Кваліфікація: д.філософ, доц., 122

Ідентифікатор ORCID ID: 0000-0002-3189-5623

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Мілов Олександр Володимирович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Мілов Олександр Володимирович

Відповідальний за підготовку облікових документів Гаврилова Алла Андріївна

Реєстратор

УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна