Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002467

Особливі позначки: відкрита

Дата реєстрації: 10-07-2024

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ №66-ас/ВС від 23.09.2024 про видачу диплома Бурмаці І.А.

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бурмака Іван Анатолійович
2. Ivan Burmaka

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-7476-5757

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: 03-09-2024

Спеціальність за освітою: Інженерія програмного забезпечення

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): ДФ10/2024 (ID 6467)

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, 20.56.02, 20.56.03

Тема дисертації:

1. Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain.

2. Information technology for the detection and analysis of anomalous events for the protection of computer networks of small and medium-sized enterprises based on blockchain.

Реферат:

1. В роботі вирішено актуальне наукове завдання з розробки моделей та методів для інформаційної технології захисту комп'ютерних мереж, з врахуванням особливостей мереж малих та середніх підприємств, які базуються на методах зберігання та поширення інформації на основі blockchain технології. Крім того, важливим є завдання визначення архітектури інформаційної системи виявлення вторгнень для мереж малих та середніх підприємств, яка використовує blockchain компоненти. Об'єктом дослідження є інформаційні процеси в системах забезпечення захисту від кіберзагроз та аномального трафіку комп'ютерних мереж. Предметом дослідження було обрано методи, моделі та елементи інформаційної технології колаборативного захисту від кібератак та аномального трафіку для комп'ютерних мереж малих та середніх підприємств на основі blockchain технології. Метою дисертаційного дослідження є підвищення ефективності захисту

комп'ютерних мереж малих та середніх підприємств на основі блокчейн технології. Завдання дослідження полягає в побудові моделі розподіленої системи захисту комп'ютерних мереж на основі blockchain, спираючись на результати аналізу основних загроз для комп'ютерних мереж, зокрема, мереж малих та середніх підприємств. В основу методології дослідження покладено імітаційне моделювання, UML проектування компонентів блокчейн технології, методи математичного моделювання для визначення оптимальних параметрів блокчейн підсистеми. Методи експертних оцінок використовувались для коректного вибору типових атак та навантажень на атаковані системи при побудові імітаційних моделей. Методи об'єктно-орієнтованого аналізу та функціонального моделювання, зокрема, SADT проектування, використані при концептуалізації бізнес-процесів у нотації IDEF0, які були взяті за основу при проектуванні інформаційної технології виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain. Основні результати дослідження та наукова новизна роботи полягають у розробці методів моделей та алгоритмів захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain. На основі аналізу актуальних загроз для комп'ютерних мереж малих та середніх підприємств визначено найбільш ефективні методи та засоби захисту таких мереж із врахуванням особливостей їх функціонування та експлуатації. В роботі запропоновано перелік основних класифікаторів для інформаційної технології захисту комп'ютерних мереж, що можуть бути об'єднані в комплексний класифікатор для підвищення точності виявлення не відомих аномальних подій розподіленою системою виявлення вторгнень. Розроблений метод підвищення ефективності використання ресурсів blockchain підсистемою оцінює ймовірність успішного створення блоку та дозволяє знизити споживання ресурсів blockchain підсистемою. Вперше розроблена концептуальна модель розподіленої інформаційної системи виявлення та аналізу аномальних подій в комп'ютерних мережах малих та середніх підприємств, яка на відміну від існуючих містить blockchain компонент для виявлення, накопичення, збереження та спільного використання інформації про аномальні події та блок мультикласифікатора для визначення наявності загрози, що дозволяє підвищити швидкість реагування на невідомі атаки; Вперше запропоновано метод вибору протоколу консенсусу для розподіленої системи виявлення вторгнень на основі blockchain, який на відміну від існуючих враховує вимоги до обладнання, масштабування та керування учасниками систем виявлення вторгнень в комп'ютерні мережі, що забезпечує підтримку прийняття рішень при проектуванні систем захисту комп'ютерних мереж малих та середніх підприємств. Удосконалено метод консенсусу PoS blockchain технології, який на відміну від існуючих, використовує в якості значення ставки час роботи вузла в розподіленій системі і дозволяє використовувати blockchain для децентралізованого зберігання даних розподіленої системи виявлення вторгнень в комп'ютерні мережі малих та середніх підприємств. Набула подальшого розвитку функціональна модель розподіленої системи захисту комп'ютерних мереж на основі blockchain технології для виявлення, накопичення, збереження та спільного використання інформації про аномальні події, яка визначає основні вхідні, вихідні параметри, обмеження та ресурси з трьома рівнями деталізації та є основою для проектування систем захисту комп'ютерних мереж малих та середніх підприємств. Практичне значення отриманих результатів полягає в тому, що вони у своїй сукупності утворюють нову інформаційну технологію виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain. Запропонована інформаційна технологія може бути використана як розробниками систем захисту комп'ютерних мереж, так і мережевими адміністраторами та ІБ спеціалістами малих та середніх підприємств. Розроблені бізнес процеси та архітектура є основою для розробки більш потужних та функціональних розподілених систем виявлення вторгнень.

2. The thesis addresses the current scientific task of developing models and methods for information technology for protecting computer networks, taking into account the specifics of networks of small and medium-sized enterprises, which are based on methods of information storage and distribution using blockchain technology. Additionally, an important task is to determine the architecture of the intrusion detection information system for small and medium-sized enterprise networks that uses blockchain components. The object of the research is the information processes in cybersecurity systems and the analysis of anomalous traffic in computer networks. The

subject of the research was selected methods, models, and elements of collaborative information technology for protection against cyber-attacks and anomalous traffic for computer networks of small and medium-sized enterprises based on blockchain technology. The purpose of the research is to increase the efficiency of protecting computer networks of small and medium-sized enterprises based on blockchain technology. The research task is to build a model of a distributed computer network protection system based on blockchain, relying on the analysis results of the main threats to computer networks, especially networks of small and medium-sized enterprises. The research methodology is based on simulation modeling, UML design of blockchain technology components, mathematical modeling methods for determining optimal parameters of the blockchain subsystem. Expert assessment methods were used to select typical attacks and loads on attacked systems when building simulation models. Object-oriented analysis and functional modeling methods, including SADT design, were used in conceptualizing business processes in the IDEF0 notation, which served as the basis for designing information technology for detecting and analyzing anomalous events to protect computer networks of small and medium-sized enterprises based on blockchain. The main results of the research and the scientific novelty of the work lie in the development of methods, models, and algorithms for protecting computer networks of small and medium-sized enterprises based on blockchain. Based on the analysis of current threats to computer networks of small and medium-sized enterprises, the most effective methods and means of protecting such networks were determined, taking into account the specifics of their operation. The work proposes a list of main classifiers for information technology for protecting computer networks, which can be combined into a comprehensive classifier to improve the accuracy of detecting unknown anomalous events by the distributed intrusion detection system. The developed method for improving the efficiency of resource utilization by evaluating of the probability of successful block creation, and allows reducing the consumption of resources by the blockchain subsystem. For the first time, a conceptual model of a distributed information system for detecting and analyzing anomalous events in the computer networks of small and medium-sized enterprises has been developed. Unlike existing models, it includes a blockchain component for detecting, accumulating, storing, and sharing information about anomalous events, as well as a multi-classifier block for determining the presence of threats, which allows for increased response speed to unknown attacks. A method for selecting a consensus protocol for a distributed intrusion detection system based on blockchain has been proposed for the first time. Unlike existing methods, it takes into account the requirements for equipment, scalability, and management of participants in intrusion detection systems in computer networks, providing support for decision-making when designing protection systems for the computer networks of small and medium-sized enterprises. The functional model of a distributed computer network protection system based on blockchain technology has been further developed for detecting, accumulating, storing, and sharing information about anomalous events. This model defines the main input and output parameters, constraints, and resources with three levels of detail and serves as the foundation for designing protection systems for the computer networks of small and medium-sized enterprises. The practical significance of the obtained results is that they collectively form a new information technology for detecting and analyzing anomalous events to protect the computer networks of small and medium-sized enterprises based on blockchain. The proposed information technology can be used by developers of computer network protection systems, as well as network administrators and IT security specialists of small and medium-sized enterprises. The developed business processes and architecture serve as the basis for developing more powerful and functional distributed intrusion detection systems.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Не застосовується

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 1. Burmaka, I., Stoianov, N., Lytvynov, V., Dorosh, M., & Lytvyn, S., "Proof of stake for blockchain based distributed intrusion detecting system," Dorosh, M., & Lytvyn, S. (2020, August). Proof of Stake for Blockchain Based Distributed Intrusion Detecting System. In Mathematical Modeling and Simulation of Systems (MODS'2020): Selected Papers of 15th International Scientific-practical Conference, MOD, vol. 1265, p. 237, 2020.
- 2. Burmaka, I., Dorosh, M., Skiter, I., & Lytvyn, S, "Architecture of Distributed Blockchain Based Intrusion Detecting System for SOHO Networks," Mathematical Modeling and Simulation of Systems (MODS'2020): Selected Papers of 15th International Scientific-practical Conference, MODS, 2021 June 28–July 01, Chernihiv, Ukraine. Springer Nature, pp. 313-326, 2021.
- 3. Burmaka, I., Zlobin, S., Lytvyn, S., & Nekhai, V., "Detecting flood attacks and abnormal system usage with artificial immune system," Mathematical Modeling and Simulation of Systems: Selected Papers of 14th International Scientific-Practical Conference, MODS, 2019 June 24-26, Chernihiv, Ukraine, pp. 131-143, 2019.
- 4. Skiter, I., Burmaka, I., & Sigayov, A., "Design of Technical Methods for Analysing Network Security Based on Identification of Network Traffic Anomalies," Information & Security, vol. 47, no. 3, pp. 306-316, 2020
- 5. Burmaka, I. A., Lytvynov, V. V., Skiter, I. S., & Lytvyn, S. V., "Evaluating a blockchain-based network performance for the intrusion detection system" Математичні машини і системи, vol. 1, pp. 99-109, 2020.
- 6. V. Lytvynov, N. Stoianov, I. Stetsenko, I. Skiter, O. Trunova, A. Hrebennyk, V. Nekhai, I. Burmaka. Attacks defense of computer nets by tools using extended information about environment: monograph – Chernihiv: Chernihiv Politechnic National University, 2021. – 212 с.
- 7. I. Burmaka, «CONSENSUS ALGORITHM COMPARISON FOR BLOCKCHAIN BASED INTRUSION DETECTING SYSTEM». Безпека ресурсів інформаційних систем: збірник тез І Міжнародної науково-практичної конференції(м. Чернігів 16-17 квітня 2020р.). –Чернігів: НУЧП, 2020. –с.6-14
- 8. Бурмака І.А., «КЛАСИФІКАЦІЯ СИСТЕМ ВИЯВЛЕНЯ ВТОРГНЕНЬ В РОЗПОДІЛЕНІ ІНФОРМАЦІЙНІ СИСТЕМИ». Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 17): збірник матеріалів ІІ Міжнародної конференції (25–27 квітня 2017, м. Славутич). – Чернігів: ЧНТУ, 2017. – с. 59-63
- 9. Бурмака Іван Анатолійович, «Архітектура розподіленої системи виявлення вторгнень на основі blockchain технології». Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2020) в режимі онлайн: збірник матеріалів V Міжнародної конференції (27–29 квітня 2020, м. Славутич). – Чернігів : ЧНТУ, 2020. с.54-59
- 10. І. А. Бурмака, М. С. Дорош «Оптимізація використання обчислювальних ресурсів розподіленою системою виявлення вторгнень на основі blockchain». Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 21) : збірник матеріалів VI Міжнародної конференції (27–29 квітня 2021,м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2021. – с. 47-50

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:

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. Клименко Ірина Анатоліївна
2. Iryna A. Klymenko

Кваліфікація: д. т. н., доцент, 05.13.05

Ідентифікатор ORCID ID: 0000-0001-5345-8806

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: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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 Повітрофлотський, 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. Шелест Михайло Євгенович
2. Mykhailo Y. Shelest

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

Ідентифікатор ORCID ID: 0000-0001-7110-4876

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. 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:

VIII. Заключні відомості

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