Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002935

Особливі позначки: відкрита

Дата реєстрації: 30-08-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сусукайло Віталій Андрійович
2. Vitalii Susukailo

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

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: 125 кібербезпека

Дата захисту: 13-08-2024

Спеціальність за освітою: кібербезпека

Місце роботи здобувача: 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:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ID 5913

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:

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

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:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.01

Тема дисертації:

1. Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем

2. Development of a cybercrime investigation system model for information system infrastructure components

Реферат:

1. У дисертаційній роботі вирішено важливу науково-практичну проблему з підвищення ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем внаслідок використання моделей штучного інтелекту, не зменшуючи при цьому ефективність виявлення точно позитивних кібератак на різних рівнях інфраструктури інформаційної системи. Вдосконалено математичний апарат оцінки вразливостей інфраструктури інформаційних систем завдяки додаванню та обчисленню атрибутів досліджуваної інформаційної системи, а також впровадженню вагових коефіцієнтів. Це підвищило точність оцінки вразливостей, дозволяючи командам безпеки пріоритезувати виправлення вразливостей згідно з особливостями інформаційної системи. Вперше розроблено метод збору журналів подій з приманок на основі технології Blockchain, що забезпечує децентралізацію даних. Розроблений метод дозволив зменшити ризики спотворення та втрати даних під час зберігання журналів подій. Отримав подальший розвиток математичний апарат виявлення кібератак завдяки впровадженню моделі ізоляційного лісу, GPT та

DevSecOps-підходу Завдяки інтеграції можливостей виявлення аномалій ізоляційного лісу, властивостей обробки передбачуваної моделей GPT і цілісного фокусу безпеки DevSecOps, структура математичного апарату підвищила точність і швидкість виявлення кібератак. Вперше розроблено модель комплексної системи дослідження кіберзлочинів, здатну виявляти та аналізувати кіберзлочини на різних рівнях інформаційної системи. Ця модель інтегрує моделі штучного інтелекту ізоляційний ліс, GPT та підхід DevSecOps, відрізняючись від традиційних систем дослідження подій інформаційної безпеки завдяки використанню комплексного підходу та інтеграції сучасних моделей та підходів інформаційної безпеки в єдину систему. Зокрема, використання ізоляційного лісу та GPT, а також систем аналізу вразливостей на різних рівнях розробки підвищує ефективність виявлення первинних причин кіберзлочинів та зменшує час реакції на атаки. Вперше розроблено методологію дослідження кіберзлочинів, що використовує моделі ізоляційного лісу, GPT та DevSecOps-підхід. Дана методологія, на відміну від існуючих, виявляє кібератаки на різні рівні інфраструктури інформаційної системи, включно з атаками сканування, ін'єкціями шкідливого коду, атаками типу Directory Traversal та виявленням аномалій з порушенням логіки додатків, які можуть залишатися непоміченими класичними SIEM системами за відсутності поведінкових сигнатур, гарантуючи високий рівень безпеки даних.

2. The dissertation solves an important scientific and practical problem of increasing the effectiveness of detecting cybercrimes in the infrastructure of information systems due to the use of artificial intelligence models, without reducing the effectiveness of detecting positive cyber attacks at various levels of the infrastructure of the information system. The mathematical apparatus for assessing the vulnerabilities of the infrastructure of information systems has been improved thanks to the addition and calculation of the attributes of the investigated information system, as well as the introduction of weighting factors. This has increased the accuracy of vulnerability assessment, allowing security teams to prioritize vulnerability remediation according to the specifics of the information system. For the first time, a method of collecting event logs from decoys based on Blockchain technology has been developed, which ensures data decentralization. The developed method made it possible to reduce the risks of distortion and loss of data during the storage of event logs. The mathematical apparatus for detecting cyber attacks has been further developed due to the implementation of the isolation forest model, GPT and the DevSecOps approach. By integrating the anomaly detection capabilities of the isolation forest, the processing properties of the predictive GPT models and the holistic security focus of DevSecOps, the structure of the mathematical apparatus has increased the accuracy and speed of cyber attack detection. For the first time, a model of a comprehensive cybercrime investigation system capable of detecting and analyzing cybercrimes at various levels of the information system has been developed. This model integrates artificial intelligence models isolation forest, GPT and the DevSecOps approach, differing from traditional information security incident investigation systems due to the use of an integrated approach and the integration of modern information security models and approaches into a single system. In particular, the use of isolation forest and GPT, as well as vulnerability analysis systems at different levels of development, increases the effectiveness of identifying the root causes of cybercrimes and reduces the response time to attacks. For the first time, a cybercrime research methodology using isolation forest models, GPT and the DevSecOps approach has been developed. This methodology, unlike the existing ones, detects cyber attacks on various levels of the information system infrastructure, including scanning attacks, malicious code injections, Directory Traversal attacks and detection of anomalies with violation of application logic, which may remain unnoticed by classic SIEM systems in the absence of behavioral signatures, guaranteeing a high level of data security.

Державний реєстраційний номер ДіР: 0119U101690 0124U000407

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:

- 1. Опірський І.Р., Василишин С.І., Сусукайло В.А. Аналіз загроз та безпеки технології NFC при передачі даних для автоматизованої реплікації профілю користувача // Вісник Східно-Українського національного університету імені Володимира Даля. Інформаційна безпека. – 2018. – №3/4 (31/32). – С. 37–44.
- 2. Опірський І.Р., Сусукайло В.А., Василишин С.І., Луковський Т.І. Розробка методу використання технології NFC для автоматизованої реплікації профілю користувача // Вісник Східно-Українського національного університету імені Володимира Даля. Інформаційна безпека. – 2018. – №3/4 (31/32). – С. 151–157.
- 3. Опірський І.Р., Василишин С.І., Сусукайло В.А. Розслідування кіберзлочинів за допомогою приманок у хмарному середовищі // Безпека інформації. –2021. – 27(1). – С.13–20.
- 4. Vasylyshyn S., Susukailo V., Opirskyy I., Kurii Y., Tyshyk I. A model of decoy system based on dynamic attributes for cybercrime investigation // Eastern-European Journal of Enterprise Technologies. – 2023.– 1 (9 (121)), pp. 6–20. (Scopus)
- 5. Сусукайло В. Використання підходу DevSecOps для аналізу сучасних загроз інформаційної безпеки // Кібербезпека: освіта, наука, техніка. – 2021. – Вип. 2, вип. 14. – С. 26–35.
- 6. Опірський І.Р., Сусукайло В.А., Василишин С.І. Дослідження можливостей використання чатботів зі штучним інтелектом для дослідження журналів подій // Захист інформації. – 2022. – Т. 24, № 4. – С. 177–183.
- 7. Kostiak M., Yevseiev S., Pohasii S., Zhuchenko O., Milov O., Lysechko V., Kovalenko O., Volkov A., Lezik A., Susukailo V. Development of crypto-code constructs based on LDPC codes // Східно-Європейський журнал передових технологій. – 2022. – № 2/9 (116). – P. 44-59.
- 8. Susukailo V., Opirskyy I., Yaremko O. Methodology of ISMS Establishment Against Modern Cybersecurity Threats // Lecture Notes in Electrical Engineering. – 2022. 7– Vol. 831: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks. – p. 257-271.
- 9. Сусукайло В.А., Опірський І.Р., Піскозуб А.З., Волошин Р.Я., Друзюк О.С. Аналіз атак, що використовуються кіберзлочинцями під час пандемії covid 19 // Захист інформації. – 2021. – Т. 22, № 4. – С. 220-226.
- 10. Опірський І.Р., Курій Є.О., Сусукайло В.А. Розробка методології оцінки відповідності стандарту ISO 27001 // Захист інформації. – 2023. – Т. 25, № 3. – С. 132-139.

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. Опірський Іван Романович

2. Ivan Opirskyy

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

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:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Гнатюк Сергій Олександрович
2. Serhii Hnatiuk

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Alexsey A. Smirnov

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

Ідентифікатор ORCID ID: Не застосовується

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. Партика Андрій Ігорович
2. Andriy I. Partyka

Кваліфікація: к. т. н., 05.27.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

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:

Власне Прізвище Ім'я По-батькові:

1. Гарасимчук Олег Ігорович
2. Oleh I. Harasymchuk

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

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:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Нємкова Олена Анатоліївна

Власне Прізвище Ім'я По-батькові головуючого на засіданні Нємкова Олена Анатоліївна

Відповідальний за підготовку облікових документів

Пархуць Любомир Теодорович

Реєстратор

УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна