Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002934

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. Банах Роман Ігорович

2. Roman Banakh

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:

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): ID 5974

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. Удосконалення технології виявлення вторгнень і систем приманок у мережах стандарту IEEE 802.11

2. Improvement of intrusion detection and honeypot technology in IEEE 802.11 networks

Реферат/анотація:

1. В роботі вирішено важливу науково-практичну задачу з покращення ефективності виявлення вторгнень і підвищення ефективності систем-приманок для бездротових комп'ютерних мереж стандарту IEEE 802.11. Вперше розроблено концептуальну модель системи захисту інформації із застосуванням систем виявлення вторгнень і систем-приманок для мереж IEEE 802.11 Wireless Honeypot as a Service використовуючи хмарні обчислення, яка на відміну від існуючих підходів до розгортання інфраструктури із системами приманками дає можливість покращити характеристики швидкості та гнучкості розгортання цілісної системи захисту інформації для бездротових мереж. Вперше розроблено методику відслідковування зловмисників за метаданими, зібраними з їх пристроїв, застосовуючи публічні бази даних геолокації Wi-Fi пристроїв. Розроблено алгоритм з покращеними характеристиками визначення геолокації конкретної точки доступу, який на відміну алгоритму запису інформації за допомогою часових рядів, дозволяє точніше визначити геолокацію Wi-Fi точок доступу, що дає можливість уникнути хибних відображень на карті, а відповідно ідентифікувати попередні місця перебування зловмисників із вищою точністю. Вперше розроблено

діагностичну модель системи-приманки для бездротових мереж стандарту IEEE 802.11, яка на відміну від підходів зі "сліпої конфігурації" чи клонування існуючої бездротової інфраструктури дозволяє оцінити рівень захищеності системи-приманки на відповідність до профілю зловмисника, що дає змогу згенерувати конфігурацію системи-приманки для зловмисника з потрібним рівнем підготовки у автоматичному режимі, і відповідно покращити пристосовуваність систем-приманок у бездротових мережах стандарту IEEE 802.11. Вперше розроблено метод виявлення вторгнень із застосуванням машинного навчання, а саме алгоритму K-найближчих сусідів, в якому на відміну від існуючих застосовано оригінальний метод агрегації даних про потужність сигналу, що дає можливість уникнути надлишкового навантаження на комп'ютерні мережі. Розроблений метод дає змогу ідентифікувати атаку «злий двійник» на ранніх стадіях атаки на точки доступу, як елемента мережевої інфраструктури WiFi.

2. The work solves an important scientific and practical problem of improving the efficiency of intrusion detection and increasing the efficiency of decoy systems for wireless computer networks of the IEEE 802.11 standard. For the first time, a conceptual model of an information protection system using intrusion detection systems and decoy systems for IEEE 802.11 Wireless Honeypot as a Service networks using cloud computing has been developed, which, in contrast to existing approaches to infrastructure deployment with decoy systems, makes it possible to improve the characteristics of the speed and flexibility of deploying a complete information protection systems for wireless networks. For the first time, a technique was developed for tracking attackers based on metadata collected from their devices, using public databases of geolocation of Wi-Fi devices. An algorithm with improved features for determining the geolocation of a specific access point has been developed, which, unlike the algorithm for recording information using time series, allows you to more accurately determine the geolocation of Wi-Fi access points, which makes it possible to avoid false reflections on the map, and, accordingly, to identify the previous locations of intruders with a higher accuracy For the first time, a diagnostic model of a decoy system for wireless networks of the IEEE 802.11 standard has been developed, which, in contrast to the approaches of "blind configuration" or cloning of the existing wireless infrastructure, allows to evaluate the level of security of the decoy system in accordance with the profile of the attacker, which makes it possible to generate the configuration of the decoy system for an attacker with the required level of training in automatic mode, and accordingly improve the adaptability of decoy systems in wireless networks of the IEEE 802.11 standard. For the first time, a method of detecting intrusions using machine learning was developed, namely the K-nearest neighbors algorithm, in which, unlike the existing ones, an original method of aggregating data on signal strength is used, which makes it possible to avoid excessive load on computer networks. The developed method makes it possible to identify an "evil double" attack in the early stages of an attack on access points as an element of the WiFi network infrastructure.

Державний реєстраційний номер ДіР: 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. Дудикевич В.Б. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку / Дудикевич В.Б., Микитин Г.В., Ребець А.І., Банах Р.І. // Сучасна спеціальна техніка. – 2014. № 4, С. 75-82.
- 2. Дудикевич В.Б. Інформаційна модель безпеки технологій зв'язку / Дудикевич В.Б., Хорошко В.О., Микитин Г.В., Банах Р.І., Ребець А.І. // Інформатика та математичні методи в моделюванні. – 2014. Том 4. – №2. – С. 137-148.
- 3. Банах Р.І. Створення концепції захищеної хмарної обчислювальної мережі з використанням систем приманок / Банах Р.І., Піскозуб А.З.,Стефінко Я.Я. // Вісник Національного університету "Львівська

політехніка": Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 74-78.

- 4. Стефінко Я.Я., Піскозуб А.З., Банах Р.І. Тестування на проникнення з Metasploit і shell скриптами. Вісник Національного університету "Львівська політехніка": Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 90-93.
- 5. Банах Р.І. Автоматизація розгортання Wi-Fi точки доступу, як зовнішнього елементу системи приманки. / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". – 2016. – № 852. С. 130-136.
- 6. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Р.І.Банах, А.З.Піскозуб // Щоквартальне наукове видання "Системи обробки інформації". Випуск 2 (148): Харківський національний університет Повітряних Сил імені Івана Кожедуба, – 2017. С. 77-83.
- 7. Банах Р.І. Оцінка надійності елементів системи-приманки у мережі стандарту IEEE 802.11, як розгалуженої системи зі складним підпорядкуванням / Банах Р.І., Піскозуб А.З. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". – 2017. – № 880. С. 94-98.
- 8. Р.І.Банах. Визначення параметрів ключа методу автентифікації WPA/WPA2 для системи-приманки мережі стандарту IEEE 802.11 / Р.І.Банах // Радіоелектроніка, інформатика, управління. – 2018. № 1. Запорізький Національний технічний університет. С. 110-118.
- 9. Attackers' Wi-Fi devices metadata interception for their location identification / Roman Banakh, Andrian Piskozub // Proceedings of the 2018 IEEE 4th 7 International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018, 2018, pp. 112-116.
- 10. Банах Р.І. Застосування хмарних обчислень для визначення рівня захищеності бездротових мереж стандарту IEEE 802.11. / Банах Р.І., Піскозуб А.З. // Сучасна спеціальна техніка. Науково-практичний журнал. – 2021. №4(67). С. 5-15.
- 11. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices / Banakh, R., Piskozub, A., Opirskyy, I. // Advances in Intelligent Systems and Computing, – 2019, 754, pp. 468-477.
- 12. Banakh, R., Piskozub, A., Opirskyy, I. Devising a method for detecting "Evil Twin" attacks on IEEE 802.11 networks (WI-FI) with KNN classification model. Eastern European Journal of Enterprise Technologies, 3 (9 (123)). – 2023, pp 20-32.

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. Піскозуб Андріан Збігнєвич

2. Andrian Piskozub

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:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Киричок Роман Васильович
2. Roman V. Kyrychok

Кваліфікація: д.філософ, 125

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Одарченко Роман Сергійович
2. Roman Odarchenko

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

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:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Мельник Віктор Анатолійович

2. Viktor Melnyk

Кваліфікація: д. т. н., професор, 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:

Власне Прізвище Ім'я По-батькові:

1. Коробейнікова Тетяна Іванівна

2. Tetyana I. Korobeynikova

Кваліфікація: к. т. н., доц., 05.13.06

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 Бешлей Микола Іванович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бешлей Микола Іванович

Відповідальний за підготовку облікових документів

Пархуць Любомир Теодорович

Реєстратор

УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Тетяна Анатоліївна