ВИСНОВОК
Національного університету «Чернігівська політехніка»
про наукову новизну, теоретичне та практичне значення результатів дисертації
Бурмаки Івана Анатолійовича на тему: «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain» поданої на здобуття ступеня доктора філософії
з галузі знань 12 – Інформаційні технології
за спеціальністю 122- Комп'ютерні науки

1. Актуальність теми дослідження та її зв'язок з науково-дослідними роботами

Активний розвиток інформаційних технологій та цифровізація усіх галузей приводять також і до зростання кількості кібератак. Сучасні кібератаки при цьому є добре спланованими та адаптованими для обходу систем захисту. При цьому, найбільш вразливими до кіберзагроз є невеликі комп'ютерні мережі малих та середніх підприємств оскільки, такі мережі, з одного боку, представляють інтерес для зловмисників, а з іншого боку, рівень їх захищеності значно нижчий аніж у великих корпоративних мереж. Враховуючи сучасні реалії ведення гібридної війни, коли загрози можуть бути спрямовані на всі сфери життєдіяльності людини, завдання захисту інформаційної інфраструктури стає ще більш важливим. При цьому, важливо, щоб захищеними залишались мережі всіх рівнів незалежно від розмірів та об'ємів трафіку. Отже, розробка інформаційної технології виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain є актуальною задачею.

Технології колаборативного виявлення вторгнень розглянуті у працях науковців Carol J. Fung, Olga Baysal, Trinh Anh Tuan, Vinod Yegneswaran, Paul Barford, Wenjuan Li, Weizhi Meng, Yu Wang, Lam For Kwok, Zhichun Li. Над вдосконаленням механізмів виявлення вторгнень шляхом інтеграції blockchain технології працювали Nicholas Kolokotronis, Sotirios Brotsis, Georgios Germanos, Costas Vassilakis, Stavros Shiaeles, Abubakar, Aliyu Ahmed, Jinshuo Liu, Ezekia Gilliard, Gupta, Rajeev Kumar, Vedant Chawla, Rajesh Kumar Pateriya, Piyush Kumar Shukla, Saoucene Mahfoudh, Syed Bilal Hussain Shah, Kably, Salaheddine, Tajeddine Benbarrad, Nabih Alaoui, Mounir Arioua.

Виклики воєнного часу, стрімкий розвиток інноваційних технологій, а також потреба розробки систем захисту комп'ютерних мереж малих та середніх підприємств доводять актуальність дисертаційної роботи, визначають її мету, завдання, об'єкт, предмет, логіку проведення досліджень, наукову новизну та практичну значущість.

Представлена дисертаційна робота запланована та виконана в рамках міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)» та відповідно до плану науково – дослідної роботи Національного університету «Чернігівська політехніка» «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931).

2. Мета і задачі дослідження

Метою дисертаційного дослідження є підвищення ефективності захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain технології.

Для досягнення мети дослідження в дисертації сформульовані та вирішені наступні завдання:

- виконати аналіз основних загроз інформаційній безпеці комп'ютерних мереж, а також методів та засобів забезпечення їх захисту;

- розробити модель розподіленої інформаційної системи виявлення та аналізу аномальних подій в комп'ютерних мережах малих та середніх підприємств на основі blockchain технології;
- запропонувати метод вибору протоколу консенсусу для розробленої моделі інформаційної системи;
- виконати адаптацію та підвищити ефективність роботи протоколу консенсусу PoS в розподілених системах виявлення вторгнень;
- виконати аналіз можливих методів класифікації аномальних подій та атак в комп'ютерних мережах малих та середніх підприємств і запропонувати комплексний класифікатор для захисту таких мереж;
- розробити функціональну модель та архітектуру розподіленої системи захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain технології;
- виконати UML проектування компонентів розподіленої системи захисту комп'ютерних мереж на основі blockchain технології;
- виконати тестування запропонованих моделей та методів системи захисту комп'ютерних мереж малих та середніх підприємств.

3. Наукові положення, розроблені особисто здобувачем, та їх новизна.

Дисертаційна робота виконана здобувачем особисто, містить наукові положення і результати, які характеризуються як науково значущі з урахуванням потреб теорії та практики за спеціальністю 122–Комп'ютерні науки.

Основні результати дослідження, які становлять його наукову новизну, полягають у наступному:

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;
- 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.

Основні результати дисертаційної роботи, що характеризують новизну дослідження, полягають у наступному:

1) Результати аналізу основних загроз інформаційній безпеці комп'ютерних мереж малих та середніх підприємств дозволили визначити існуючі методи та засоби їх захисту з врахуванням особливостей функціонування та експлуатації мереж такого класу, що дає можливість створювати нові та покращувати існуючі методи захисту.
2) Розроблено модель розподіленої інформаційної системи виявлення та аналізу аномальних подій на основі блокчейн технології, яка є основою для побудови різноманітних розподілених систем захисту комп'ютерних мереж малих та середніх підприємств.
3) Запропоновано метод вибору протоколу консенсусу дозволив обрати для розподіленої інформаційної системи виявлення та аналізу аномальних подій протокол, який базується на методі PoS і дозволяє знизити навантаження на обчислювальне обладнання в процесі роботи системи, а також зменшити споживання електроенергії.
4) Адаптовано для використання в розподілених системах виявлення вторгнень протокол консенсусу PoS, який забезпечує надійну та стабільну роботу blockchain компонента та витрачає менше обчислювальних ресурсів аніж базовий варіант протоколу на 80%.
5) Сформовано перелік основних класифікаторів, які можуть бути об'єднані в комплексний класифікатор для підвищення точності виявлення невідомих аномальних подій розподіленою системою виявлення вторгнень.
6) Розроблена функціональна модель та архітектура розподіленої системи захисту комп'ютерних мереж на основі blockchain, яка забезпечує високий ступінь децентралізації та можливість масштабування в умовах обмежених обчислювальних ресурсів.
7) Побудовані UML діаграми основних компонентів розподіленої системи захисту комп'ютерних мереж на основі blockchain, що деталізують зв'язки між компонентами системи, будову самих компонентів та варіанти їх розгортання в комп'ютерних мережах малих та середніх підприємств.
8) Створена кросплатформена реалізація компонентів інформаційної технології виявлення та аналізу аномальних подій в мережах малих та середніх підприємств на основі blockchain технології для тестування запропонованих моделей та методів.

4. Обґрунтованість та достовірність наукових положень, висновків рекомендацій

Зміст дисертаційної роботи побудовано на відповідному первинному матеріалі, аналіз та узагальнення якого дозволили сформулювати основні наукові положення, висновки та рекомендації.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується глибоким аналізом наукових досягнень українських та зарубіжних науковців у відповідній сфері, нормативно-правових актів, аналітичних матеріалів міжнародних організацій, інформаційних ресурсів мережі Internet, що дозволило компетентно виконати завдання, поставлені у дослідженні.

Основні положення, висновки та практичні рекомендації базуються на матеріалах власних досліджень автора, логічно випливають із матеріалів дисертації та є науково обґрунтованими і чітко сформульованими.

Для досягнення поставлених в дисертаційному дослідженні завдань було використано як загально наукові, так і спеціальні методи, а саме: імітаційне моделювання, UML проектування компонентів blockchain технології, методи математичного моделювання для визначення оптимальних параметрів blockchain 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.

5. Теоретичне та практичне значення результатів дисертаційного дослідження.

Науково-практичні розробки та рекомендації автора було впроваджено у практичну діяльність:

- у навчальному процесі Національного університету «Чернігівська політехніка» при проведенні лекцій та лабораторних робіт з дисципліни «Системи захисту обчислювальних мереж» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії (довідка про впровадження №203/08-1128/ВС від 14.05.2024);
- в Чернігівському обласному філармонійному центрі фестивалів та концертних програм при виявленні аномальних подій зовнішнього та внутрішнього походження в комп'ютерній мережі підприємства з метою визначення основних векторів атак на мережу та подальшої розробки заходів з укріплення захисту мережевої інфраструктури Чернігівського обласного філармонійного центру (довідка про впровадження №131/01-08 від 7.05.2024);
- в ТОВ "ІНФОРМАЦІЙНІ СИСТЕМИ ЗАХИСТУ" при визначенні основних векторів атак на інформаційну інфраструктуру підприємства та розробці комплексу заходів для підвищення рівня захищеності мережевої інфраструктури (акт про впровадження №54 від 13.05.2024).

6. Апробація результатів дослідження.

Основні положення, результати та висновки дисертації доповідались на 8 наукових конференціях зокрема: II Міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO 17(м. Славутич, 2017), XIV Міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем МОДС»(Чернігів 2019), I Міжнародній науково-практичній конференції Безпека ресурсів інформаційних систем (Чернігів 2020), XV Міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем МОДС»(Чернігів 2020), V Міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO 20(м. Славутич, 2020), Другій міжнародній конференції «Digital Transformation, Cyber Security and Resilience» (DIGILIENCE 2020), XVI Міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем МОДС»(Чернігів 2020), VI Міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO 21(м. Славутич, 2021)

7. Повнота викладення основних наукових результатів дисертації в публікаціях таособистий внесок у них автора.

Аналіз кількості наукових публікацій, повноти опублікування результатів дисертації та особистого внеску здобувача до всіх наукових публікацій, опублікованих самостійно й у співавторстві та зараховані за темою дисертації, засвідчив, що результати дослідження, викладені у дисертаційній роботі, отримані автором самостійно та повною мірою відображені в публікаціях, доповідалися та обговорювалися на науково-практичних конференціях.

Основні результати дисертаційного дослідження опубліковано здобувачем самостійно та в співавторстві в 10 наукових працях загальним обсягом 14,09 друк. Арк, з

яких автору належить 2,82 друк.арк. Серед них 4 статті у наукових фахових виданнях України, обсягом 2,89 друк. арк., 3 з них включені до міжнародної наукометричної бази Scopus та опубліковані в закордонних виданнях, обсягом 0,81 друк. арк., розділ у колективній монографії обсягом 0,87 друк. арк., одна стаття у науковому періодичному виданні іншої країни обсягом 0,4 друк. арк.; 4 праці апробаційного характеру обсягом 0,77 друк.арк. Результати роботи доповідалися на 8 міжнародних наукових конференціях.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:
Статті у наукових фахових виданнях та виданнях, внесених до наукометричних баз:

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. https://doi.org/10.1007/978-3-030-58124-4_23 (SCOPUS) (0,7 ум. друк. арк.) (Особистий внесок здобувача: модифікація алгоритму Proof of Stake для використання в системі виявлення вторгнень). (0,2 ум. друк. арк.)

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. https://doi.org/10.1007/978-3-030-89902-8_24 (SCOPUS) (0,85 ум. друк. арк.) (Особистий внесок здобувача: розробка архітектури розподыленої системи виявлення вторгнень на основі блокчейн). (0,36 ум. друк. арк.)

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. https://doi.org/10.1007/978-3-030-25741-5_14 (SCOPUS) (0,52 ум. друк. арк.) (Особистий внесок здобувача: розробка алгоритму виявлення аномальної поведінки комп'ютерної системи за допомогою штучної імуної системи). (0,25 ум. друк. арк.).

4. Burmaka, I. A., Lytvynov, V. V., Skiter, I. S., & Lytvyn, S. V., "Evaluating a blockchain-based network performance for the intrusion detection system" *Математические машины и системы,* vol. 1, pp. 99-109, 2020. DOI: 10.34121/1028-9763-2020-1-99-109 (0,85 ум. друк. арк.) (Особистий внесок здобувача: Створення моделі розподіленої системи виявлення вторгнень на основі блокчейн). (0,35 ум. друк. арк.).

Розділ у колективній монографії:

5. 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. (10 ум. друк. арк.) (Особистий внесок здобувача розділ про побудову тренувального центра з кібербезпеки(. (0,87 ум. друк. арк.)

Статті опубліковані у періодичних виданнях інших країн:

6. 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 https://doi.org/10.11610/isij.4722 (0,4 ум. друк. арк.) (Особистий внесок здобувача: проектування атакуючої підсистеми). (0,1 ум. друк. арк.).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

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 (0,3 ум. друк. арк.).

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 (0,12 ум. друк. арк.).

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 (0,2 ум. друк. арк.).

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 (0,15 ум. друк. арк.) (Особистий внесок здобувача метод оптимізації використання обчислювальних ресурсів) (0,07 ум. друк. арк.).

8. Загальний висновок.

Дисертаційна робота Бурмаки Івана Анатолійовича на тему «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain» є оригінальним, самостійним, завершеним науковим дослідженням, що стосується актуальної проблематики і містить оригінальніпідходи до розв'язання теоретичних та практичних завдань щодо виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain.

Основні положення, висновки та рекомендації дисертації містять елементи наукової новизни, є повністю обґрунтовані та аргументовані і отримали необхідну апробацію на науково-практичних конференціях. У публікаціях здобувача знайшли відображення всі положення дисертаційного дослідження. Зміст дисертації відповідає визначеній меті, поставлені здобувачем наукові завдання вирішені повною мірою, мету дослідження досягнуто. Роботу виконано державною мовою.

За актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Бурмаки Івана Анатолійовича відповідає спеціальності 122-Комп'ютерні науки та вимогам «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових

установах)», затвердженого Постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (в редакції постанови Кабінету Міністрів України від 19 травня 2023 р. № 502), наукові публікації здобувача відповідають пункту 8 постанови Кабінету Міністрів України від 12 січня 2022 року № 44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Дисертація Бурмаки Івана Анатолійовича на тему «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain» може бути рекомендована до захисту у спеціалізовану вчену раду

Головуючий *Підпис* Казимир В.В.

Дата

20.05.2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ
Національний університет «Чернігівська політехніка»
ВІДДІЛ КАДРІВ

Підпис В. В. Казимира
засвідчую
Головний спеціаліст
відділу кадрів Т.М. Бурмака
«07» 05 2024 р.