РЕЦЕНЗІЯ

офіційного рецензента, доктора технічних наук, професора кафедри інформаційних та комп'ютерних систем Національного університету «Чернігівська політехніка» Зайцева Сергія Васильовича на дисертаційну роботу Бурмаки Івана Анатолійовича на тему «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain», представлену на здобуття ступеня доктора філософіїв галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації.

Останніми роками кількість кібератак на інформаційну інфраструктуру підприємств значно зросла. Ці атаки стали не лише більш частими, але й складнішими, що робить їх одним із інструментів у веденні гібридної війни. Вразливість малих та середніх підприємств до кібератак зумовлена недостатньою захищеністю їхніх мереж, через обмеженість фінансових ресурсів, що не дозволяє інвестувати в дорогі комерційні системи виявлення та попередження вторгнень. Окрім того, постійно з'являються нові варіанти кібератак, розроблених для обходу актуальних систем захисту, що підкреслює необхідність розробки надійних механізмів захисту інформацінйої інфраструктури для збереження безперервності бізнес-процесів і захисту конфіденційності інформації.

У цьому контексті технологія блокчейн представляє значний інтерес як засіб для створення розподілених систем виявлення та аналізу аномальних подій. Використання блокчейну дозволяє забезпечити надійність і цілісність збереження та передачі даних, а також створити систему, яка може оперативно реагувати на нові загрози. Це особливо важливо для малих та середніх підприємств, оскільки така система буде менш затратною в обслуговуванні та не вимагатиме кваліфікованих кадрів для її налаштування. Таким чином, розробка та впровадження інформаційних технологій на основі блокчейн для захисту комп'ютерних мереж є актуальним і перспективним напрямком досліджень.

Зв'язок роботи з науковими програмами, планами, темами.

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).

Наукова новизна та практичне значення дослідження

Наукова новизна результатів дисертаційного дослідження полягає в 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;
- 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.

Основні результати дослідження полягають у розробці методів, моделей та алгоритмів захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain.

Практичним результатом дисертації є нова інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж на основі blockchain, що може бути використана як розробниками систем захисту

комп'ютерних мереж, так і мережевими адміністраторами та ІБ спеціалістами малих та середніх підприємств. Також розроблено програмний модуль blockchain підсистеми, що слугує основою для побудови децентралізованої розподіленої системи виявлення вторгнень, а також програмний модуль мультикласифікатора, які є частиною інформаційної технології виявлення та аналізу аномальних подій.

Ступінь обґрунтованості наукових положень, висновків, сформульованих у дисертації

Всі положення дисертації, що захищається, обґрунтовані, що підтверджується експериментами. Обчислювальні досліди можуть бути відтворені, що забезпечує достовірність отриманих результатів. Наукові результати дисертації були апробовані, доповідались на міжнародних науково-практичних конференціях та підтверджуються довідками про впровадження. Це загалом підтверджує достатній рівень практичної значимості та обґрунтованості дослідження.

Поставлене наукове завдання в дисертаційній роботі виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Повнота викладення основних результатів дисертації в опублікованих працях

Наукові результати дисертації висвітлені у 10 наукових публікаціях здобувача, серед яких: 1 стаття у науковому виданні, включеному на дату опублікування до переліку наукових фахових видань України; 3 статті у періодичних наукових виданнях, проіндексованих у базі даних Scopus, з яких 2 статті у виданнях, віднесених до третього квартилю (Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports.

Також результати дисертації були апробовані на 4 наукових фахових конференціях.

У наведених публікаціях достатньо повно представлено результати дисертаційної роботи. Порушення академічної доброчесності в них не виявлено. Особистий внесок здобувача у публікаціях, зазначений у дисертації, свідчить про його авторство у відповідних наукових досягненнях.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Бурмаки І.А. повністю відповідає Стандарту вищої освіти зі спеціальності 122 Комп'ютерні науки та напрямкам досліджень відповідно до освітньої програми «Комп'ютерні науки».

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям «Комп'ютерні науки».

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Бурмаки Івана Анатолійовича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Виявлений відсоток співпадінь пояснюється наведенням у дисертації фрагментів з опублікованих статтей автора (на які вказане посилання) та використанням загальноприйнятої наукової термінології. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Текст дисертації викладений логічно та послідовно, його оформлення відповідає чинним вимогам. Автор дотримується наукового стилю та використовує загальноприйняту термінологію.

Зміст дисертації

Дисертаційна робота складається з вступу, 4 розділів висновків, переліку умовних скорочень, переліку посилань зі 129 джерел та 3 додатків. Загальний обсяг дисертації 231 сторінка.

У вступі дисертації обґрунтовано актуальність досліджуваної теми, сформульовано мету, завдання та методологію дослідження, а також розкрито його зв'язок із науковими програмами кафедри, а також наведено наукову новизну та практичне значення отриманих результатів.

У першому розділі проведено аналіз основних загроз інформаційній безпеці комп'ютерних мереж та факторів, що впливають на їх захищеність. Встановлено, що мережі малих та середніх підприємств особливо вразливі до атак і потребують засобів захисту, здатних швидко виявляти нові, раніше невідомі атаки та ефективно їх блокувати. Крім того, проведено огляд основних методів і засобів захисту комп'ютерних мереж, включаючи як комерційні рішення, так і рішення з відкритим вихідним кодом.

У другому розділі представлено модель розподіленої інформаційної системи для виявлення та аналізу аномальних подій на основі технології blockchain. Описано обґрунтування необхідності використання цієї технології для створення розподіленої системи виявлення вторгнень, для захисту комп'ютерних мереж малих та середніх підприємств. Також визначено основні методи класифікації аномальних подій, які можуть бути інтегровані як окремі модулі в систему виявлення вторгнень, утворюючи комплексний класифікатор

для підвищення точності виявлення аномалій. Запропоновано метод вибору протоколу консенсусу для компонента blockchain у розподіленій системі виявлення вторгнень та адаптовано протокол консенсусу PoS для використання в цих системах.

У третьому розділі подано загальну функціональну модель розподіленої системи захисту комп'ютерних мереж, що базується на технології blockchain. Визначено основні вхідні та вихідні параметри, обмеження і ресурси на трьох рівнях деталізації. Архітектура системи представлена за допомогою UML діаграм, що відображають її структуру.

У четвертому розділі розроблено імітаційну модель розподіленої системи захисту комп'ютерних мереж, призначену для тестування компонентів системи в різних умовах і оцінки її продуктивності. Експерименти проведені як у віртуальному середовищі, так і на фізичному обладнанні, з отриманням аналогічних результатів.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Недоліки та зауваження до дисертаціної роботи.

1. В роботі не зазначено які алгоритми генерації криптографічних ключів використовуються при побудові блокчейн компонента.
2. Ефективність роботи розподіленої системи захисту комп'ютерних мереж малих та середніх підприємств оцінюється тільки за часом реагування на невідомі загрози. Бажано було б також врахувати точність виявлення аномалій.
3. В запропонованому методі вибору протоколу консенсусу недостатньо чітко сформовані критерії які визначають особливості мереж малих та середніх підприємств.
4. В роботі наявна невелика кількість орфографічних та стилістичних помилок.

Усі наведені зауваження не зменшують цінність результатів роботи. Одежані в роботі результати є новими, відповідають поставленим цілям і задачамта мають теоретичне і практичне значення.

Висновок про дисертаційну роботу

Дисертаційна робота здобувача ступеня доктора філософії 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 повністю завершеним науковим дослідженням, що виконане на високому професійному рівні.

Диссертаційна робота повністю відповідає вимогам«Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої

ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (в редакції постанови Кабінету Міністрів України від 19 травня 2023 р. № 502).

Вважаю, що Бурмака Іван Анатолійович заслуговує присудження наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки»

Офіційний рецензент:

доктор технічних наук,
професор, професор кафедри
інформаційних та комп'ютерних систем
Національного університету
«Чернігівська політехніка» Сергій ЗАЙЦЕВ

М.П. «06» 08 2024 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний університет «Чернігівська політехніка»

Підпис С.О. Зайцева
засвідчую
ВІДДІЛ КАДРІВ
Нач. відділу кадрів
«06» 08 2024 р.