РЕЦЕНЗІЯ

офіційного рецензента, доктора технічних наук, професора кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка» Шелеста Михайла Євгенійовича 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 філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації.

Сучасний світ стикається з постійним зростанням кількості та складності кібератак, що особливо відчувається на інформаційній інфраструктурі малих та середніх підприємств. Ці компанії часто не мають достатніх ресурсів для інвестування в дорогі комерційні системи захисту, що робить їх вразливими до кіберзагроз. До того ж, використання кібератак, як засобу ведення гібридної війни робить ситуацію ще складнішою, підкреслюючи важливість надійного захисту для збереження безперервності бізнес-процесів і захисту конфіденційної інформації.

Технологія блокчейн пропонує інноваційний підхід до вирішення цих проблем, даючи змогу створити розподілену систему виявлення та аналізу аномальних подій, яка може ефективно реагувати на нові загрози завдяки своїй здатності швидко виявляти та обробляти дані про аномалії. Це особливо актуально для малих та середніх підприємств, які потребують доступних і ефективних рішень для забезпечення безпеки своїх мереж. Розробка таких систем не лише підвищує захищеність, але й сприяє більш широкому використанню сучасних технологій у сфері кібербезпеки, що робить це дослідження актуальним в сучасних умовах.

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.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується глибоким аналізом наукових праць українських та зарубіжних науковців у відповідних сферах, нормативно-правових актів, аналітичних матеріалів міжнародних організацій, інформаційних ресурсів мережі Internet.

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 були представлені у 10 наукових публікаціях автора. З них: 1 стаття опублікована у науковому виданні, яке на момент публікації входило до переліку наукових фахових видань України; 3 статті вийшли у періодичних наукових журналах, що індексуються у базі даних Scopus, причому 2 з них опубліковані у журналах, які входять до третього квартилю (Q3) згідно з класифікацією SCImago Journal and Country Rank або Journal Citation Reports. Крім того, результати дослідження були представлені на 4 наукових фахових конференціях.

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 статей автора (на які вказане посилання) та використанням загальноприйнятої наукової термінології. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

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, розкрито 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».

Ідентичність анотації та основних положень дисертаційної роботи. Анотація в повному обсязі відображає основні положення дисертаційної роботи.

Недоліки та зауваження до дисертаційної роботи.

1. В роботі не вказано мінімальні системні вимоги до обладнання для розгортання розподіленої системи виявлення вторгнень на основі blockchain, тому не зовсім зрозуміло чи зможе задовольнити такі вимоги обладнання комп'ютерних мереж малих та середніх підприємств,
2. Бажано було б визначити етапи та ефективність проектів впровадження запропонованої системи захисту на малих та середніх підприємствах.
3. Недостатньо висвітлено питання можливостей масштабування розподіленої системи виявлення вторгнень на основі blockchain в залежності від кількості користувачів.
4. В роботі для оцінки ефективності запропонованої системи використовується тільки час реагування. Доцільним було б розширити кількість критеріїв і навести інтегральний показник.

Усі наведені зауваження не зменшують цінність результатів роботи. Отримані в роботі результати є новими, відповідають поставленим цілям і задачам та 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.

Дисертаційна 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 кібербезпеки та
математичного моделювання
Національного університету
«Чернігівська політехніка»

М. Шелест

«_12_» серпня 2024 року