Голові разової спеціалізованої вченої ради
Національного університету «Львівська політехніка»
д.т.н., професору Нємковій Олені Анатоліївні

ВІДГУК

офіційного опонента
доктора технічних наук, професора Смірнова Олексія Анатолійовича,
завідувача кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
на дисертаційну роботу

Сусукайла Віталія Андрійовича
«Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем»
подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертаційної роботи.

Фактори розвитку технологій та збільшення кількості кіберзагроз стимулює законодавство багатьох країн визначати вимоги до захисту інформації у критичній інфраструктурі. Відповідність вимогам законодавства стає критично важливою для організацій, оскільки невідповідність може призвести до значних штрафів та інших юридичних наслідків. Крім того, інциденти, пов'язані з витоком даних або іншими кіберзлочинами, можуть завдати значної шкоди репутації організації.

Постійне вдосконалення методів та способів проведення кібератак вимагає розробки складних та гнучких моделей систем дослідження, здатних оперативно реагувати на нові загрози. Традиційні методи захисту, такі як EDR системи, SIEM системи, системи запобігання вторгненням вже не є достатніми. Впровадження проактивних методів, таких як аналіз поведінки, машинне навчання та штучний інтелект, стає необхідним для виявлення та попередження загроз.

Сучасні інформаційні системи складаються з багатьох різнорідних компонентів, включаючи хмарні сервіси, мобільні додатки, інтернет речей та інші. Це створює потребу в розробці комплексних моделей, здатних адаптуватись до різних типів журналів подій, легко навчатись та виявляти аномалії безпеки у всіх цих компонентах, для своєчасного виявлення та реагування на події та інциденти інформаційної безпеки.

Тому, вирішення науково-практичного завдання з підвищення ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем завдяки використанню моделей штучного інтелекту є актуальним дослідженням та може бути використано державними та приватними організаціями.

2. Аналіз змісту дисертаційної роботи.

Дисертація Сусукайла Віталія Андрійовича є завершеним дослідженням, яке містить нові, науково обгрунтовані результати викладені на 196 сторінках у 4 розділах.

У **вступі** подані усі необхідні дані щодо актуальності поставленої в дисертації задачі, чітко подано мету та дані про наукову новизну і практичну цінність отриманих результатів.

У **першому розділі** "Аналіз стану проблеми розроблення комплексної системи дослідження кіберзагроз інфраструктури інформаційних систем" автор провів аналіз компонентів інфраструктури інформаційної системи та провів аналіз сучасних тенденцій та технологій. Зіставлено підходи побудови інформаційної системи у хмарних та локальних типах інфраструктури. Також, автор дослідив підхід DevSecOps та вплив алгоритмів ШІ на галузі використання інформаційних систем.

У **другому розділі** автор дослідив можливості традиційних систем забезпечення інформаційної безпеки та зіставив їх з моделями ШІ та їх впливом. Автор провів експериментальні дослідження для порівняння алгоритмів машинного навчання та визначив перевагу моделі ізоляційного лісу, над випадковим лісом та моделями глибокого навчання для дослідження журналів подій. Також у даному розділі автор провів експериментальне дослідження моделей GPT та порівняв моделі GPT-3.5 та GPT-4.0, та встановив, що GPT-4.0 загалом демонструє підвищену ефективність обробки та виявлення різних типів кібератак порівняно з GPT-3.5.

У **третьому розділі** автор представив модель системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем, що використовує методологію визначення аномалій шляхом навчання ізоляційного лісу нормальній поведінці інформаційної системи, що дало можливість адаптувати її під різні типи інформаційних систем. Запропонований підхід покращує класифікацію шкідливих запитів і зменшує кількість фальшивих спрацювань. Запропонована модель інтегрується з DevSecOps рішеннями для аналізу наявності вразливостей та за допомогою вагових коефіцієнтів забезпечує можливість дослідити вплив вразливості враховуючи атрибути досліджуваної системи.

У **четвертому розділі** дисертації автор провів наступні експерименти: атака сканування, ін'єкційні атаки, атаки Directory Traversal та атаки з порушенням логіки. Дані дослідження проводились для зіставлення традиційної SIEM системи з запропонованою системою. Автор визначив, що час виявлення відомих типів атак (Ін'єкції, сканування на вразливості, Directory Traversal) в порівнянні з традиційною SIEM зменшився до 31% і запропонована модель може виявляти невідомі атаки завдяки здатності моделі ізоляційного лісу розпізнавати аномалії. Зменшення часу виявлення не вплинуло на відсоток виявлених атак. Встановлено, що використання моделі GPT значно зменшує час дослідження кіберзлочинів. Час аналізу відомих атак зменшився до 60%, а для аномалій, що порушують логіку роботи інформаційної системи до 7 разів.

3. Наукова новизна одержаних результатів. Основні наукові положення, результати та висновки дисертації, отримані здобувачем самостійно, є новими, достатньо обґрунтованими і підтверджуються даними комп'ютерних експериментів та апробацією на всеукраїнських і міжнародних конференціях. Достовірність наукових положень, висновків і результатів забезпечена коректним та доцільним використанням математичного апарату, методології проектування інформаційних систем та успішною програмною реалізацією. У дисертаційній роботі отримані наступні результати, які мають наукову новизну:

1. Вдосконалено математичний апарат оцінки вразливостей інфраструктури інформаційних систем за рахунок додавання та обчислення атрибутів досліджуваної інформаційної системи, а також впровадження вагових коефіцієнтів. Це підвищило точність оцінки вразливостей, дозволяючи командам безпеки пріоритизувати виправлення вразливостей згідно з особливостями інформаційної системи.

2. Вперше розроблено метод збору журналів подій з приманок на основі технології Blockchain, що забезпечує децентралізацію даних за допомогою розподіленої бази даних. Розроблений метод дозволив зменшити ризики спотворення та втрати даних під час зберігання журналів подій.

3. Отримав подальший розвиток математичний апарат виявлення кібератак за рахунок впровадження моделей 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.

4. 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.

5. 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

4. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Наукове значення виконаного дослідження полягає у розробці ефективної системи для швидшого виявлення та аналізу кіберзлочинів, що може бути застосована у різних наукових галузях та навчальних курсах. У навчальних програмах ці результати можуть бути інтегровані у курси з інформаційної безпеки, аналізу даних, інтелектуальних систем, а також у спеціалізовані курси з виявлення та запобігання кіберзлочинам. Зокрема, результати даного дослідження Сусукайла Віталія Андрійовича впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни «Безпека програмного забезпечення» для студентів першого рівня вищої освіти напрямку підготовки 125 «Кібербезпека та захист інформації».

Результати даного дослідження можуть бути використані не лише в галузі інформаційної безпеки. Зокрема, для штучного інтелекту ці результати демонструють можливості застосування моделей машинного навчання для розпізнавання аномалій і поведінкових зразків, що можуть свідчити про кіберзлочини. У галузі машинного навчання дослідження показує ефективність використання моделей, таких як ізоляційний ліс і GPT, для складних завдань аналізу великих обсягів даних.

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна.

При вирішенні завдань, поставлених у дисертації, та створенні наукових положень, моделей та методологій здобувач проаналізував дані наукової літератури за тематикою дослідження.

Здобувачем були застосовані теорія машинного навчання та методи математичного і імітаційного моделювання для апробації запропонованих рішень. Теоретична база дослідження ґрунтується на фундаментальних принципах системного аналізу та інформаційних технологій. Вважаю, що створені наукові положення, методологія та методи є достатньо обґрунтованими, що підтверджується результатами моделювань, експериментальних досліджень та практичними результатами, які відображені у наведених результатах впровадження.

6. Практичне значення одержаних результатів полягає у тому, що:

- розроблена методологія дослідження кіберзлочинів, що побудована на основі моделей ізоляційного лісу та GPT забезпечила відповідність процесу моніторингу інформаційної безпеки у системі менеджменту інформаційної безпеки контролю 8.16 міжнародного стандарту ISO 27001:2022. Впровадження методології дослідження кіберзлочинів у систему менеджменту інформаційної безпеки дало можливість виявляти кіберзлочини на ранніх їх стадіях, мінімізуючи ресурси, необхідні для забезпечення відповідності контролям 5.25 та 5.26 міжнародного стандарту ISO 27001:2022.
- впровадження системи дослідження загроз інформаційної безпеки як одного із елементів моделі дослідження кіберзлочинів забезпечило виявлення відомих кіберзагроз, користуючись публічними ідентифікаторами компрометації інформаційних систем. Використання DevSecOps–підходу та сканування інформаційних систем на різних рівнях інфраструктури вразливостей дало можливість корелювати вплив вразливостей інформаційної системи на кіберзлочини. Цей підхід дозволяє ідентифікувати відомі кіберзагрози за допомогою загальнодоступних ідентифікаторів, оптимізує процес усунення вразливостей шляхом сканування інфраструктури інформаційних систем та надає комплексне уявлення про стан безпеки інформаційної системи.
- експериментально підтверджено, що модель GPT–4.0 не лише точно визначає тип кіберзлочину, але забезпечує загалом щонайменше до 5% швидше виявлення кібератак, ніж GPT–3.5, що може мати вирішальне значення в реальних сценаріях, де час відповіді потрібно мінімізувати.
- розроблена модель з використанням ізоляційного лісу дала можливість зменшити час виявлення кібератак у середньому до 31% в повірянні з класичною SIEM–системою та виявляти невідомі атаки, що зумовлено здатністю навчання моделі ізоляційний ліс відрізняти нормальну поведінку від аномальної та працювати з аномаліями різного типу.

- експериментально визначено, що модель на основі GPT обробляє дані швидше, ніж це можливо для людини, ідентифікуючи закономірності та взаємозв'язки, зменшуючи час дослідження кіберзлочинів у середньому до 60%, а для аномалій, що порушують логіку роботи додатку, до 7 разів.

7. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Сусукайла Віталія Андрійовича достатньо повно відображені у вісімнадцяти наукових публікаціях, а саме: у десяти статтях (із них дев'ять – у фахових наукових виданнях України та одній – у періодичному виданні закордоном) і восьми тезах виступів на науково-практичних заходах. Сім публікацій проіндексовано в наукометричній базі Scopus.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. З праць, опублікованих у співавторстві, у дисертації використано результати, які отримано здобувачем самостійно.

8. Оцінка структури дисертації, її мови та стилю викладення.

Дисертаційна робота має чітко визначену та логічно побудовану структуру, що відповідає вимогам МОН України. Усі розділи дисертації послідовно викладені, починаючи від вступу, який містить мету та завдання дослідження, і завершуючи висновками. Кожен розділ є самостійною частиною, але водночас послідовно описує проведене дослідження.

У роботі використовується сучасна професійна термінологія та викладення матеріалу здійснюється логічно, що робить текст зрозумілим для фахівців у відповідній галузі.

У дисертаційній роботі дотримані принципи академічної доброчесності. Використання ідей, результатів і текстів інших авторів супроводжується відповідними посиланнями на першоджерела, що свідчить про повагу до інтелектуальної власності та відповідальне ставлення до академічної етики.

9. Зауваження та дискусійні положення щодо змісту роботи.

Незважаючи на загальне позитивне враження від дисертаційної роботи, слід зазначити деякі зауваження та виділити окремі положення роботи, що викликають дискусії:

- у першому розділі автор представив детальне дослідження можливостей використання штучного інтелекту. Дане досліджує підкреслює позитивні аспекти використання штучного інтелекту. Проте, воно не приділяє достатньої уваги аналізу недоліків штучного інтелекту та потенційно негативного впливу, що може виникнути при його використанні.
- у розділі 2.2 описано використання наступних метрик: акуратність, влучність, відкликання, оцінка F1 та площа під кривою ROC (AUC-ROC) . Дані метрики детально описані, проте їх використання не достатньо обґрунтовано та не розглянуті інші можливі метрики для оцінки моделей штучного інтелекту, що могло б надати більш комплексний аналіз.
- у розділі 2.6 автор описав метод використання технології Blockchain для дослідження кіберзлочинів. Зокрема, цей метод передбачає збір журналів подій з приманок на основі технології Blockchain. Проте, автор не проаналізував обмеження масштабованості та обробки великих обсягів даних, які можуть виникнути при використанні даної технології в реальних умовах, що могло б ускладнити її застосування.

- у розділі 4.4. детально описано етапи експериментального проведення атак на досліджувану систему. Зокрема, автором описано проведення експерименту атаки сканування на досліджувану систему. Атака сканування може проводитись із використанням облікових даних користувачів інфраструктури для більш детального виявлення вразливостей. Проте автор не врахував даний тип сканування, що може обмежити повноту виявлених вразливостей. Хоча даний тип атаки не впливає на результати вказаного експерименту, проте враховуючи фактор наявності облікових даних автор може більш детально оцінити швидкодію виявлення та аналізу даного типу атаки.

Загальні висновки щодо дисертаційної роботи.

Аналіз дисертаційної роботи Сусукайла Віталія дозволяє дійти висновку, що дана робота є актуальним дослідженням, яке може вплинути на стан проблеми дослідження кіберзлочинів. Зміст роботи відзначається науковою цінністю, інноваційністю підходів та внеском у розвиток технологій дослідження кіберзлочинів.

Одержані наукові та практичні результати є вагомим внеском у розвиток теорії та практики управління інцидентами інформаційної безпеки та дослідження кіберзлочинів, що можуть використовуватись інфраструктурі інформаційних систем пришвидшуючи аналіз кіберзлочинів, не зменшуючи при цьому ефективність виявлення точно позитивних кібератак.

Взявши це до уваги, вважаю, що дисертація за своєю актуальністю, науковою новизною, практичним значенням отриманих результатів, обґрунтованістю основних положень та висновків повністю відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», вимогам освітньо-наукової програми, яку успішно завершив здобувач, вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (затвердженого Постановою Кабінету Міністрів України 12 січня 2022 р. № 44), а її автор Сусукайло Віталій Андрійович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент:

доктор технічних наук, професор,
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор,

Олексій СМІРНОВ

Підпис доктора технічних наук, професора, завідувача кафедрою кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету Смірнова Олексія Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету
Кандидат технічних наук, доцент

Андрій ТИХИЙ