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

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора, Гнатюка Сергія Олександровича,
в.о. проректора з наукової роботи Національного авіаційного 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

Зі зростанням залежності від інформаційних технологій збільшується ризик кіберзлочинів, які становлять значну загрозу для безпеки інформаційних систем. Зокрема, однією з причин актуальності розроблення моделі системи дослідження кіберзлочинів є зростання кількості та складності кіберзлочинів на різних рівнях інфраструктури інформаційної системи. Крім того, інформаційні системи критичної інфраструктури, таких як енергетика, транспорт, фінансові установи, є особливо вразливими до кіберзагроз. Атаки на ці системи можуть мати катастрофічні наслідки для суспільства та національної безпеки.

Ще однією важливою причиною є законодавчі вимоги та стандарти. Багато країн впроваджують суворі регуляторні вимоги щодо захисту інформації та боротьби з кіберзлочинністю. Відповідність цим вимогам вимагає наявності

ефективних засобів для виявлення та розслідування кіберінцидентів. Крім того, кіберзлочини можуть призводити до значних фінансових втрат для організацій через прямі збитки, втрату даних, зниження довіри клієнтів та штрафні санкції.

В умовах сучасних загроз важливо мати можливість швидко виявляти, аналізувати та реагувати на кіберінциденти, щоб мінімізувати їхні наслідки та запобігти подальшим атакам. Розробка моделі системи дослідження кіберзлочинів дозволяє підвищити рівень захисту інформаційних систем, забезпечити ефективне виявлення та розслідування кіберінцидентів, а також сприяти зниженню ризиків та збитків від кіберзлочинності. Це є важливим кроком для забезпечення безпеки та стабільності сучасної цифрової інфраструктури.

Зазначене свідчить, що тема дисертаційного дослідження є актуальною та вирішує науково-практичне завдання з підвищення ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем завдяки використанню моделей штучного інтелекту, не зменшуючи при цьому ефективність виявлення точно позитивних кібератак на різних рівнях інформаційної системи. Що, зокрема, підтверджується зв'язком з науковими планами, темами та програмами. Так, дослідження виконувалось у відповідності до наукового напряму кафедри захисту інформації Національного університету «Львівська політехніка» - «Дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії», в межах кафедральної науково-дослідної роботи: «Розроблення та удосконалення методів і засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (шифр ЗІ-7) (№ д.р. 0119U101690) (2019-2022). Окремі частини роботи виконано в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ д.р. 0124U000407).

Аналіз змісту дисертаційної роботи. Структура дисертаційної роботи традиційна й включає вступ, чотири розділи, кожен з яких відрізняється певним науковим вкладом у вирішення науково-практичного завдання з підвищення ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем.

У вступі автор детально обґрунтовує важливість обраної теми, пояснюючи її актуальність у сучасному контексті. Далі визначаються основні цілі та завдання дослідження, які спрямовані на досягнення конкретних наукових результатів. Окремо підкреслюється наукова новизна роботи, що полягає у внесенні нових підходів у дослідженні кіберзлочинів. Також у вступі наведено інформацію про те, як результати дослідження були апробовані, що підтверджує їхню достовірність і значущість.

У **першому розділі** автором проаналізовано сучасні підходи до розслідування кіберзлочинів, вплив DevSecOps, та відповідальність за кіберзлочини згідно з Кримінальним кодексом України. Дослідження показало відсутність єдиної моделі системи дослідження кібербезпеки на різних рівнях інформаційних систем, що підкреслює необхідність розробки такої моделі. Використання рішень ШІ є актуальним, але потребує постійного вдосконалення. Підхід DevSecOps визначив важливість інтеграції сканерів вразливостей у процес розробки для своєчасного реагування та підвищення точності встановлення причин кіберзлочинів.

У другому розділі автор проаналізував можливості використання систем дослідження подій інформаційної безпеки, проаналізовано використання алгоритмів машинного навчання для дослідження аномалій у журналах подій та використання алгоритмів GPT для аналізу кібератак. Дослідження проведені в даному розділі визначають як моделі штучного інтелекту можуть бути використані для виявлення та аналізу кіберзлочинів.

У **третьому розділі** автор представляє методологію дослідження кіберзлочинів засновану на використанні системи дослідження загроз, підході DevSecOps, моделі ізоляційний ліс та моделі GPT. Запропонована автором модель системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем, що використовує методологію виявлення аномалій шляхом навчання моделі нормальній поведінці користувача. Також, дана система інтегрується з рішеннями виявлення вразливостей та пропонуються вагові коефіцієнти забезпечуючи їх точніший аналіз. Модель системи дослідження кіберзлочинів розроблена з урахуванням принципів “Безпека за замовчуванням” та “Безпека за дизайном”, що вказується застосуванням сховища ключів, використання алгоритму TLS 1.2 для

даних, що передаються та впровадженням функціоналу маскування даних для зібраної інформації з різних систем.

У **четвертому розділі** дисертації автором проведено порівняльний аналіз між запропонованою системою дослідження кіберзлочинів, яка використовує моделі ізоляційного лісу та GPT, і традиційними системами SIEM. Здатність системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем зменшує виявлення кібератак та дослідження кіберзлочинів, не зменшуючи відсоток виявлених атак. Результати дослідження також свідчать про те, що запропонована система сприяє покращенню контролів у сфері управління інформаційною безпекою та забезпеченню відповідності стандарту ISO 27001:2022.

У **висновках** дисертаційної роботи викладено основні результати дослідження і рекомендації, які випливають з проведених досліджень.

2. Наукова новизна одержаних результатів

Найсуттєвіші результати дослідження, що містять наукову новизну, полягають у тому, що:

- *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.

- *вперше розроблено* метод збору журналів подій з приманок на основі технології Blockchain, що забезпечує децентралізацію даних. Розроблений метод дозволив зменшити ризики спотворення та втрати даних під час зберігання журналів подій.

- *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 моделі GPT і цілісного фокусу безпеки DevSecOps, структура математичного апарату підвищила точність і швидкість виявлення кібератак.

- *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.
- *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

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

Наукові результати, отримані автором, мають потенціал для практичного застосування у кількох напрямках. Перш за все, їх можна використовувати для розробки новітніх систем моніторингу безпеки. Ці системи базуються на використанні моделей ізоляційного лісу та GPT, які пропонуються як ефективні рішення для виявлення вторгнень. Такі моделі здатні швидко та точно ідентифікувати аномалії та потенційні загрози в інформаційних системах.

Крім того, результати дослідження сприяють покращенню процесу управління інцидентами інформаційної безпеки. Використання запропонованих моделей дозволяє підвищити ефективність і швидкість реагування на інциденти, що є надзвичайно важливим як для державних, так і для приватних організацій. Це, в

свою чергу, підвищує загальний рівень безпеки та знижує ризики, пов'язані з інформаційними загрозами.

Отже, впровадження наукових результатів автора у практичну діяльність організацій сприятиме значному підвищенню рівня захищеності інформаційних систем і покращенню управління інформаційною безпекою.

Також, результати дисертаційної роботи можуть бути впроваджені у навчальний процес. Зокрема, результати даного дослідження Сусукайла Віталія Андрійовича вже впроваджені у навчальний процес кафедри захисту інформації Національного університету «Львівська політехніка» при вивченні дисципліни «Безпека програмного забезпечення» для студентів першого рівня вищої освіти напрямку підготовки 125 «Кібербезпека та захист інформації».

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

Результати, представлені в дисертації, ґрунтуються на ретельно продуманому підході до постановки завдань дослідження. Кожне завдання було чітко сформульовано, що забезпечило ясність і послідовність у проведенні дослідження. При виборі математичних моделей автор логічно та обґрунтовано підходив до прийняття припущень, що дозволило забезпечити точність і відповідність моделей реальним умовам.

Крім того, математичний апарат був використаний коректно, що гарантує адекватність та достовірність отриманих результатів, а також додатково підтверджується практичною реалізацією моделі системи дослідження кіберзлочинів. Ця модель була застосована для аналізу кібезлочинів на різних рівнях інфраструктури інформаційних систем, що дозволило на практиці перевірити її ефективність і точність. Практична реалізація демонструє, що запропоновані підходи і методи не тільки теоретично обґрунтовані, але й можуть бути успішно застосовані в реальних умовах для виявлення та аналізу кіберзлочинів.

5. 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.

6. Повнота оприлюднення результатів дисертаційної роботи

Основні результати дисертаційної роботи Сусукайла Віталія Андрійовича викладено у вісімнадцяти наукових публікаціях, а саме: у десяти статтях (із них

дев'ять – у фахових наукових виданнях України та одній – у періодичному виданні за кордоном) 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.

7. Оцінка структури дисертації, її мови та стилю викладення

За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Ознайомлення з текстом анотації дає змогу констатувати, що її зміст повною мірою відображає основні положення і висновки дисертації та не містить зайвої інформації.

8. Зауваження та дискусійні положення щодо змісту роботи

Загалом, позитивно оцінюючи дисертаційне дослідження, варто відзначити деякі аспекти, які потребують уточнень. Необхідно також звернути увагу на окремі положення роботи, які можуть бути предметом дискусії:

1. Дисертант декларує, що розроблена система дослідження кіберзлочинів ефективніша порівняно з традиційною SIEM системою. Було б добре порівняти такі системи (їх на сьогодні відомо досить багато і вони є різними) за певними критеріями і чітко вказати на переваги розробленого рішення.

2. Метою дисертаційної роботи є підвищення захищеності компонентів інформаційних систем від кібератак на різних рівнях її інфраструктури. Проте, з тексту дисертації (зокрема, із загальних висновків до роботи) не зрозуміло на скільки відсотків (чи у скільки разів) було підвищено рівень захищеності компонентів інформаційних систем від кібератак.

3. У вступі дисертації здобувач визначає методи дослідження, які були використані в процесі дослідження (оптимізаційні процедури, імітаційне та

аналітичне моделювання, методи математичної статистики, розробка на основі об'єктно-орієнтованого підходу, а також принципи теорії інформації та кодування), проте не вказує який метод для якого завдання було використано.

4. Методологію дослідження кіберзлочинів автор відображає і в наукових, і в практичних результатах. На мою думку, методологія – це науковий результат і здобувачу потрібно було цим обмежитись.

5. У підрозділі 2.2 представлені результати тестування алгоритмів штучного інтелекту для аналізу подій та інцидентів інформаційної безпеки. Автор пропонує використовувати журнали подій Nginx для цього аналізу. Проте вибір саме цього типу журналів подій не був достатньо обґрунтований. Було б корисно врахувати журнали подій інших сервісів, таких як Apache, IIS або різні системи управління базами даних (наприклад, MySQL, PostgreSQL), щоб забезпечити більш детальний і всебічний аналіз.

6. У підрозділі 3.1 автор детально розглянув вимоги міжнародних стандартів до системи дослідження кіберзлочинів. Основну увагу було приділено вимогам міжнародного стандарту ISO 27001, які узгоджуються з найкращими практиками та підходами до забезпечення інформаційної безпеки. Однак, доцільно було б більш детально дослідити вплив інших стандартів, таких як ISO 27002, NIST SP 800-53 або GDPR, а також врахувати міжнародні практики, такі як OWASP або CIS Controls, для надання більш всебічного огляду.

7. У підрозділі 4.1 автор зазначає про використання реверсивного проксі-сервера для тестового середовища. Проте не було надано обґрунтування щодо вибору саме реверсивного проксі-сервера, а також не розглянуто його переваги та недоліки. Було б корисно проаналізувати альтернативні рішення, такі як прямі проксі-сервери, балансувальники навантаження або застосування хмарних сервісів для цього завдання.

8. У дисертаційній роботі є певні неточності стилістичного характеру. Також у декількох літературних джерелах пропущені сторінки або посилання, присутні посилання на конкретні статті кодексу (замість посилання на сам документ) тощо.

Водночас, вказані зауваження мають дискусійний характер, не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової і практичної цінності.

Загальні висновки щодо дисертаційної роботи

Дисертаційна робота Сусукайла Віталя Андрійовича «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» є завершеною, самостійною працею та відповідає паспорту заявленої спеціальності і такою, що містить достатню наукову новизну та практичну цінність отриманих результатів, які дозволяють підвищити ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем завдяки використанню моделей штучного інтелекту, не зменшуючи при цьому ефективність виявлення точно позитивних кібератак на різних рівнях інфраструктури інформаційної системи.

Враховуючи актуальність, наукову новизну і практичне значення одержаних результатів, вважаю, що дисертаційна роботи «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» цілком відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №°44, а її автор Сусукайло Віталій Андрійович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент

в.о. проректора з наукової роботи
Національного авіаційного університету
доктор технічних наук, професор Сергій ГНАТЮК