ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
д.т.н., проф. _____ Іван ДЕМИДОВ
"30" квітня 2024р.

Висновок
про наукову новизну, теоретичне та практичне значення результатів дисертації «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» здобувача наукового ступеня доктора філософії за спеціальністю *125 Кібербезпека* (галузь знань *12 Інформаційні технології*) Сусукайла Віталія Андрійовича наукового семінару кафедри захисту інформації

1. Актуальність теми дисертації

Розроблення моделі системи дослідження кіберзлочинів в 2024 році є надзвичайно важливим, враховуючи ускладнення кіберзагроз у глобальному масштабі. В контексті стрімкого розвитку цифрових технологій, зокрема хмарних обчислень, і штучного інтелекту, зловмисники знаходять нові шляхи для здійснення своїх атак. Це вимагає від бізнесу і державних установ впровадження передових методів захисту інформаційних активів.

Одним із ключових аспектів актуальності цієї теми є забезпечення адаптивності та гнучкості моделей в розпізнаванні нових типів кібератак, які розвиваються та стають більш складними. Розроблені моделі повинні мати можливість аналізувати величезні обсяги даних у реальному часі, ідентифікувати потенційні загрози з мінімальним запізненням та допомогти SOC командам вчасно реагувати на них. Такий підхід дозволяє мінімізувати можливі збитки і захистити дані.

Також, розвиток та впровадження моделей системи дослідження кіберзлочинів сприяє культурі безпеки в організації, підвищуючи обізнаність та готовність співробітників реагувати на можливі інциденти. Це формує загальну стратегію кібербезпеки, яка є критично важливою для сучасних організацій, чиї операції все більше залежать від стабільності та безпечності їхніх інформаційних систем.

Таким чином, актуальність розробки моделі системи дослідження кіберзлочинів для складових інформаційних систем обумовлена не тільки необхідністю захисту від поточних і майбутніх загроз, але й вимогами сучасного регулятивного середовища, а також стратегічною потребою в цілісному підході до кібербезпеки на всіх рівнях системи управління інформаційною безпекою.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Тема дисертації відповідає науковому напрямку кафедри захисту інформації Національного університету "Львівська політехніка": дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії.

Удосконалення інформаційної безпеки держави, контррозвідувальних методів протидії та техніки.

Дисертаційні дослідження виконувалися в межах держбюджетної науково-дослідної роботи "Розроблення та удосконалення методів та засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах" (№ державної реєстрації 0119U101690; терміни виконання 2019-2022 рр.). 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» (№ держреєстрації 0124U000407).

3. Особистий внесок здобувача в отриманні наукових результатів

Дисертація є самостійною науковою працею, в якій автор особисто розробив і впровадив нові наукові ідеї та методи, спрямовані на покращення процесу виявлення та дослідження кіберзлочинів, використовуючи модель ізоляційного лісу, GPT та підхід DevSecOps. Це дозволило зменшити час виявлення та дослідження кіберзлочинів не знижуючи ефективність аналізу подій інформаційної безпеки. Ідеї, положення чи гіпотези інших авторів, які присутні в дисертації, мають відповідні посилання і використані лише для підкріплення ідей та результатів здобувача.

4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій базується на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання і практичною реалізацією системи дослідження кіберзлочинів, а також збіжністю з результатами експериментальної верифікації.

5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру

Наукова новизна основних результатів дисертації полягає в розробленні методології дослідження кіберзлочинів на основі алгоритмів штучного інтелекту, як елементу захисту інформаційних систем на різних рівнях інфраструктури.

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 моделі 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

6. Перелік наукових праць, які відображають основні результати дисертації

Основні результати дослідження викладено у вісімнадцяти наукових публікаціях, а саме: у десяти статтях (із них дев'ять – у наукових фахових виданнях України та одній – у періодичному виданні закордоном, з яких 3 індексуються у наукометричній базі даних Scopus) і восьми тезах виступів на науково-практичних заходах. Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. Основні положення та результати дисертації викладені в таких наукових працях здобувача:

Статті у наукових фахових виданнях України:

1. Опірський І.Р., Василишин С.І., Сусукайло В.А. Розслідування кіберзлочинів за допомогою приманок у хмарному середовищі. Безпека інформації, 27(1). – 2021. – С.13-20. *Особистий внесок здобувача: представлено порівняльну характеристику програмних приманок, проведено порівняння найпоширеніших систем дослідження кіберзлочинів у хмарах.*
2. В. Сусукайло С. Василишин, І. Опірський. Дослідження можливостей використання чатботів зі штучним інтелектом для дослідження журналів подій" // НАУ: "Захист інформації". – Том 24, №4 – Київ, 2022р. – С.177-183. *Особистий внесок здобувача: представлено порівняльну характеристику моделі GPT 3.5 та GPT 4.0;проведено експериментальне дослідження можливостей GTP моделей для аналізу експлуатації вразливості Log4j.*
3. Опірський І.Р., Василишин С.І., Сусукайло В.А. Аналіз загроз та безпеки технології NFC при передачі даних для автоматизованої реплікації профілю користувача // Вісник Східно-Українського національного університету імені Володимира Даля. Інформаційна безпека. – 2018. – №3/4 (31/32). С. 37-44. *Особистий внесок здобувача: проведено аналіз захищеності технології NFC.*
4. Опірський І.Р., Сусукайло В.А., Василишин С.І., Луковський Т.І. Розробка методу використання технології NFC для автоматизованої реплікації профілю користувача // Вісник Східно-Українського національного університету імені Володимира Даля. Інформаційна безпека. – 2018. – №3/4 (31/32). – С. 151–157. *Особистий внесок здобувача: проведено аналіз впливу реплікації профілю користувача на технологію NFC.*
5. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. A model of decoy system based on dynamic attributes for cybercrime investigation // Eastern-European Journal of Enterprise Technologies. 2023. Vol. 1 (9 (121)). P. 6-20. (Scopus, Q3) *Особистий внесок здобувача:*

представлено метод збору журналів подій з приманок на основі технології Blockchain, як доказів для дослідження кіберзлочинів.

6. Сусукайло В. Використання підходу DevSecOps для аналізу сучасних загроз інформаційної безпеки // Кібербезпека: освіта, наука, техніка. – 2021. – Вип. 2, вип. 14. – С. 26–35. *Особистий внесок здобувача: представлено аналіз впливу DevSecOps підходу на ризики пов'язані з розробкою програмного забезпечення на всіх етапах SDLC; визначено Визначено набір застосунків для оптимізації процесу безпечної розробки додатків.*
7. Kostiak M., Yevseiev S., Pohasii S., Zhuchenko O., Milov O., Lysechko V., Kovalenko O., Volkov A., Lezik A., Susukailo V. Development of crypto-code constructs based on LDPC codes // Східно-Європейський журнал передових технологій. – 2022. – № 2/9 (116). – P. 44–59 *Особистий внесок здобувача: проведено аналіз кібератак на мережевому рівні інфраструктури інформаційних систем.*
8. Сусукайло В. А., Опірський І. Р., Піскозуб А. З., Волошин Р. Я., Друзюк О. С. Аналіз атак, що використовуються кіберзлочинцями під час пандемії covid 19 // Захист інформації. – 2021. – Т. 22, № 4. – С. 220–226. *Особистий внесок здобувача: представлено вектори кібератак під час пандемії COVID-19; визначено заходи захисту для протидії кібератакам під час під час пандемії COVID-19.*
9. Опірський І. Р., Курій Є. О., Сусукайло В. А. Розробка методології оцінки відповідності стандарту ISO 27001 // Захист інформації. – 2023. – Т. 25, № 3. – С. 132–139. *Особистий внесок здобувача: представлено зміни в основній частині стандарту ISO 27001:2022, що мають вплив на систему управління інформаційною безпекою.*

Статті у наукових періодичних виданнях інших держав, що включені до міжнародної наукометричної бази даних (Scopus):

10. Susukailo V., Opirskyy I., Yaremko O. Methodology of ISMS Establishment Against Modern Cybersecurity Threats // Lecture Notes in Electrical Engineering. – 2022. – Vol. 831: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks. – p. 257–271. *Особистий внесок здобувача: представлено методологію побудови системи управління інформаційною безпекою.*

Наукові публікації у збірниках матеріалів та тез конференцій:

11. Susukailo V., Opirskyy I., Kret T. Advantages of Threat Hunting with Endpoint Detection and Response Solutions // Information Protection and Security of Information Systems: VII International Scientific and Technical Conference "Information Protection and Security of Information Systems". *– 2019. – Pp. 17-19.*). *Особистий внесок здобувача: представлено переваги використання технології EDR для процесу полювання на кіберзагрозу.*
12. Susukailo V. A., Opirskyy I. R. Researching the possibilities of the Azure Log Analytics system for the analysis of information security incidents in cloud solutions // Information security and information technologies: a collection of abstracts of reports of the IV All-Ukrainian scientific and practical conference of young scientists, students and cadets (Lviv, November 27, 2020). – 2020. – Pp. 57–59.) *Особистий внесок здобувача: проведено експериментальне дослідження можливостей Azure Log Analytics для аналізу подій інформаційної безпеки.*
13. Sviatoslav Vasylyshyn, Ivan Opirskyy, Vitalii Susukailo. Analysis of the use of software baits (honeypots) as a means of ensuring information security // International Workshop on Information Modeling. Zbarazh, Ukraine, 2020. Vol. 2, P. 242–245, 9321925. (Scopus, QX). *Особистий внесок здобувача: представлено реалізацію використання програмних приманок для дослідження подій інформаційної безпеки.*

14. Sviatoslav Vasylyshyn, Ivan Opirskyy, Vitalii Susukailo. Analysis of the attack vectors used by threat actors during pandemic // International Workshop on Information Modeling. Zbarazh, Ukraine, 2020. Vol. 2, P. 261–264, 9321897. (Scopus, QX). *Особистий внесок здобувача: представлено аналіз сучасних векторів атак зловмисників на інформаційні системи.*
15. Opirskyy I., Tyshyk I., Susukailo V. Evaluation of the possibility of Realizing the Crime of the Information System at Different Stages of TCP/IP // 2021 IEEE 4th International conference on advanced information and communication technologies: conference proceedings AICT- 2021 (Lviv, Ukraine, September 21-25, 2021). – 2021. – С. 261–265.). *Особистий внесок здобувача: представлено аналіз кібератак мережевого рівня . Вдосконалено математичний апарат оцінки ймовірності реалізації мережевих атак.*
16. Susukailo V., Vasylyshyn S., Opirskyy I., Buriachok V., Riabchun O. Cybercrimes investigation via honeypots in cloud environments // CEUR Workshop Proceedings. – 2021. – Vol. 2923: Proceedings of selected papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021 (online). – Pp. 91–96. *Особистий внесок здобувача: представлено аналіз впливу, поведінки та ефективність програмних приманок у хмарному середовищі.*
17. Опірський І.Р., Василишин С.І. Сусукайло В.А., Дослідження вразливості Zerologon // "Технічні засоби захисту інформації", семінар при науковій раді НАН України, Київ, Україна. 2021. Особистий внесок здобувача: *представлено аналіз експлуатації вразливості Zerologon.*
18. Susukailo V., Opirskyy I., Vasylyshyn S. Analysis of the possibility of using chatbots with Artificial Intelligence to detect information security incidents // Protection of information and security of information systems: materials of the IX International Scientific and Technical Conference (Lviv, 25–26 May 2023). – 2023. – С. 120–121*) Особистий внесок здобувача: проведено експериментальне дослідження можливостей GTP моделей для аналізу ін'єкційних атак.*

7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні результати дисертаційного дослідження апробовано на міжнародних наукових та науково-практичних конференціях, наукових школах та консорціумах, семінарах:

- VII Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем" (30-31 травня 2019 року, Львів 2019, Україна);
- VIII Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем" (10-11 листопада 2021 року, Львів 2021, Україна);
- The 15th IEEE International Conference on Computer Sciences and Information Technologies (23-26 вересня, 2020 року, Збараж, Україна);
- IV Всеукраїнська науково-практична конференція молодих учених, студентів і курсантів (26 листопада 2020 року, Львів 2020 р, Україна);
- IV Міжнародна конференція «Нові досягнення в галузі інформаційно-комунікаційних технологій» - AICT 2021 (21-25 вересня 2021 року, Львів 2021, Україна)
- Семінар із забезпечення кібербезпеки в інформаційно-телекомунікаційних системах, CPITS 2021- CPITS II 2021(28 січня 2021 року, Київ, Україна);
- Міжвідомчому міжрегіональному семінар Наукової Ради НАН України "Технічні засоби захисту інформації" (11 квітня 2021 року, Київ, Україна);
- Наукові семінари кафедри захисту інформації (2018-2024 рр.).

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

Наукові результати, отримані автором, можуть бути використані при розробці новітніх систем моніторингу безпеки, які використовують моделі ізоляційного лісу та GPT в якості рішень виявлення вторгнень та для покращення процесу управління інцидентами інформаційної безпеки в державних або приватних організаціях.

Також їх можна впровадити у навчальний процес у курсі "Технології розслідування інцидентів інформаційної безпеки" для студентів спеціальності 125 Кібербезпека та захист інформації.

9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані

Методологія та методи, представлені в науковій роботі, покращують можливості активного та пасивного захисту інформації в державних та приватних організаціях завдяки використанню моделей штучного інтелекту та підходу DevSecOps. Розроблена модель системи дослідження кіберзлочинів, яка інтегрує підхід DevSecOps, алгоритм Ізоляційного лісу та модель GPT для виявлення зловмисної діяльності, дає можливість підвищити захищеність інформаційних систем шляхом зменшення часу аналізу кіберзлочинів, без втрат ефективності, та забезпечити дослідження подій інформаційної безпеки враховуючи вразливості інформаційної системи на різних її рівнях

Результати дисертаційної роботи впроваджено у технологічні процеси підприємств ТОВ "Бінарікс Україна"(м. Львів), ТОВ "ТЕХМЕДЖИК" (м. Львів) та AG "Hiveon" (м. Київ).

10. Оцінка структури дисертації, її мови та стилю викладення

Дисертаційна робота викладена на 196 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 35 рисунків та 15 таблиць, списку використаних джерел з 101 найменування, а також 4 додатки. 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 ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

11. З врахуванням зазначеного, **на науковому семінарі кафедри захисту інформації ухвалили:**

11.1. Дисертація Сусукайла Віталія Андрійовича на тему "Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем" є завершеною науковою працею, у якій розв'язано конкретне наукове завдання – 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 інфраструктури інформаційної системи, що має важливе значення для галузі знань *12 Інформаційні технології.*

11.2. Основні наукові положення, методичні розробки, висновки та практичні рекомендації, викладені у дисертаційній роботі, логічні, послідовні, аргументовані, достовірні, достатньо обґрунтовані. Дисертація характеризується єдністю змісту.

11.3. У 18 наукових публікаціях відображені основні результати дисертації (з них 9 статей у наукових фахових виданнях України, 1 стаття у науковому виданні іншої держави, що входить до міжнародної наукометричної бази (Scopus), та 8 матеріалів конференцій).

11.4. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44, зі змінами).

11.5. Дисертація є результатом самостійних досліджень, не містить елементів фальсифікації, компіляції, плагіату та запозичень, що констатує відсутність порушення академічної доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

11.6. З урахуванням наукової зрілості та професійних якостей Сусукайла В.А. дисертаційна робота "Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем" рекомендується для подання до розгляду та захисту у разовій спеціалізованій вченій раді.

За затвердження висновку проголосували:

"за"	***55***	***(п'ятдесят п'ять)***
"проти"	***–***	***(немає)***
"утримались"	***–***	***(немає)***

Головуючий на засіданні фахового семінару, д.т.н., професор, завідувач кафедри захисту інформації — Іван ОПІРСЬКИЙ

Рецензенти:

к.т.н., доцент, доцент кафедри захисту інформації — Олег ГАРАСИМЧУК

к.т.н., старший викладач кафедри захисту інформації — Андрій ПАРТИКА

Відповідальний в ІКТА за атестацію PhD, д.т.н., професор, професор кафедри захисту інформації — Любомир ПАРХУЦЬ

"23" квітня 2024 р.