РЕЦЕНЗІЯ

Кандидата технічних наук, доцента,
доцента кафедри захисту інформації
Гарасимчука Олега Ігоровича
Національного університету «Львівська політехніка»
на дисертацію
Сусукайла Віталія Андрійовича
«Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем»,
подану на здобуття наукового ступеня доктора філософії за спеціальністю
125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Актуальність розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем у 2024 році можна обґрунтувати рядом ключових чинників:

1. Технологічний прогрес сприяє еволюції кіберзагроз та збільшення площі атак. Сучасні кібератаки стають все більш складними та витонченими, а також можуть призвести до значних фінансових та репутаційних втрат для компаній. Розробка детальних та ефективних моделей дослідження допоможе виявляти та нейтралізувати ці загрози на ранніх стадіях.

2. Зростаюча увага держав до питань кібербезпеки призводить до суворішого регулювання у цій сфері. Організації потребують не тільки відповідати існуючим нормам, але й адаптуватись до постійно оновлюваних законодавчих вимог. Вдосконалені дослідницькі моделі допоможуть компаніям залишатися на крок попереду вимог та забезпечити їх дотримання.

3. Втрати від кібератак зростають, що вимагає більшого фокусу на превентивні заходи та відновлення після інцидентів. Витрати на кіберзахист виявляються значно меншими порівняно з потенційними збитками від

інцидентів, що змушує бізнеси інвестувати у розробку та впровадження передових технологій та методик.

4. Швидкий розвиток технологій, зокрема в областях штучного інтелекту та великих даних, відкриває нові можливості для кіберзлочинців і одночасно надає нові інструменти для кіберзахисту. Ефективне використання цих технологій в моделях дослідження може значно підсилити здатність до прогнозування, виявлення та реагування на кіберзагрози.

5. Міжнародний аспект: кіберзлочини не знають кордонів, і співпраця між країнами та міжнародними організаціями стає вирішальною для боротьби з глобальними кіберзагрозами. Розробка міжнародно прийнятих моделей дослідження кіберзлочинів може сприяти більш ефективному обміну інформацією та координації зусиль.

Ці аспекти підкреслюють критичну потребу в розробці і впровадженні моделей для дослідження кіберзлочинів, що є не тільки реакцією на існуючі загрози, але й проактивним кроком у забезпеченні довготривалої стійкості інформаційних систем.

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).

Наукова новизна основних результатів дисертації полягає у тому, що:

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. 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 даних.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.

Дисертація базується на глибокому аналізі потреб сучасної кібербезпеки та розробляє передові методи для ефективного дослідження та протидії кіберзагрозам. Наукові положення, представлені в дисертації, відзначаються високим ступенем обґрунтованості. Вони базуються на кваліфікованому підході до постановки завдань досліджень і логічно обґрунтованому використанні математичних моделей. Таке використання математичного апарату дозволяє не лише аналізувати існуючі загрози, але й адаптувати системи до майбутніх викликів у кібербезпеці.

Достовірність наукових результатів дисертації підтверджується за допомогою комп'ютерного моделювання. Результати використання моделей штучного інтелекту для аналізу кіберзлочинів дозволяють не тільки підтвердити теоретичні припущення, але й показати практичну застосовність розроблених методик. Крім того, реалізація цих підходів у практичних сценаріях забезпечує нові можливості для захисту інформаційних систем та стійкості до кіберзагроз.

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 .

Також їх можна впровадити у навчальний процес у курсі "Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки" для студентів спеціальності 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів полягає у можливості їх безпосереднього застосування для покращення процесу управління інцидентами інформаційної безпеки у державних та приватних системах менеджменту інформаційної безпеки.

1. 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.

2. 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.

3. 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.

4. Розроблена модель з використанням Ізоляційного Лісу дала можливість зменшити час виявлення кібератак в середньому до 31% в порівнянні 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.

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

Основні результати дисертаційної роботи використано і впроваджено з метою покращення процесів виявлення інцидентів інформаційної безпеки компанією ТОВ "Бінарікс Україна", для реагування на інциденти інформаційної безпеки, компанією AG "Hiveon" та як елемент забезпечення відповідності заходам захисту стандарту ISO/IEC 27001:2022 для компанії ТОВ "Техмеджик", що підтверджено актами впровадження.

Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дослідження викладено 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.

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.
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.
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.

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.
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)
6. Сусукайло В. Використання підходу DevSecOps для аналізу сучасних загроз інформаційної безпеки // Кібербезпека: освіта, наука, техніка. – 2021. – Вип. 2, вип. 14. – С. 26–35.
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
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.
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.

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.

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.*).
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.)
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).
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).
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. – C. 261–265.).
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.

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.
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)

Зауваження по дисертації.

1. Хоча результати комп'ютерного моделювання і експериментальна верифікація підтвердили ефективність розробленої моделі, дане наукове дослідження можна розширити збільшенням обсягу та різноманітності даних дослідження. Збільшення об'єму дата сетів може допомогти в підвищенні загальної надійності моделей та їх універсальності.

2. Розділ 3.1 описує відповідність системи стандарту ISO 27001:2022, проте для забезпечення більш детального дослідження вимог міжнародних практик управління інцидентами інформаційної безпеки варто проаналізувати вимоги SOC2 та CIS 20, які можуть визначити додаткові контролі безпеки не вказані у ISO 27001:2022.

3. У розділі 4, під час дослідження атак на інформаційну систему, автор не описує відмінність впливу внутрішніх та зовнішніх атак на дослідження кіберзлочинів розробленою системою. Важливість цієї відмінності полягає в різних методах та підходах, які застосовуються для виявлення, аналізу та запобігання цих типів атак. Аналіз внутрішніх атак на інформаційну систему може бути корисним при визначенні критичності кіберзлочину та його впливу на організацію.

4. У роботі зустрічаються описки, неточності формулювання, варто було притримуватись однакової термінології

Слід відзначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок

Не зважаючи на виявлені недоліки дисертаційна робота Сусукайла Віталія Андрійовича на тему «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» є завершеною науковою працею, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека " (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 125 "Кібербезпека" та чинним вимогам, які встановлені у "Порядку присудження ступеня доктора філософії", який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека".

Офіційний рецензент

Кандидат технічних наук, доцент,
Доцент кафедри захисту інформації
Національного університету
"Львівська політехніка" Олег ГАРАСИМЧУК

Підпис к.т.н, доцента Гарасимчука О.І. засвідчую
Вчений секретар
Національного університету
"Львівська політехніка" Роман БРИЛИНСЬКИЙ
к.т.н., доцент