РЕЦЕНЗІЯ

Кандидата технічних наук, старшого викладача кафедри захисту інформації

Партики Андрія Ігоровича

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 можна обґрунтувати зокрема у контексті глобального зростання цифровізації та залежності від комплексних інформаційних систем у різних секторах. Сучасний світ стикається з постійним зростанням кількості і складності кібератак, що вимагає розробки нових, більш досконалих методів для їх виявлення та протидії. Такі методи мають здатність не лише реагувати на поточні кіберзагрози, але й прогнозувати майбутні виклики, що дозволяє підготуватися та мінімізувати потенційний збиток.

Зокрема, розробка спеціалізованих моделей дослідження кіберзлочинів є ключовою для адекватного реагування на швидко мінливий ландшафт кібербезпеки. Ці моделі мають забезпечити не тільки виявлення та аналіз відомих загроз, але й мають включати алгоритми для виявлення нових патернів поведінки, що можуть вказувати на небезпеку. З цією метою, математичні та статистичні методи, разом із алгоритмами машинного навчання, можуть сприяти розвитку більш гнучких та ефективних систем.

Іншим важливим аспектом є впровадження цих моделей у реальні умови, що вимагає їх тестування та оптимізацію у різних середовищах. Для підтвердження достовірності та ефективності запропонованих методів необхідно використовувати обширні датасети, що відображають реальні умови

використання, та проводити ретельну верифікацію результатів. Такий підхід дозволяє не тільки вдосконалити існуючі методи, але й адаптувати їх до постійно змінюваних умов, що є критично важливим для забезпечення високого рівня кібербезпеки.

Дана дисертаційна робота зосереджена на актуальних проблемах та викликах кібербезпеки та присвячена вирішенню актуального науково-практичного завдання з підвищення ефективності виявлення кіберзлочинів в інфраструктурі інформаційних систем за рахунок використання моделей штучного інтелекту, не зменшуючи при цьому ефективність виявлення точно позитивних кібератак на різних рівнях інфраструктури інформаційної системи

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

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 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 даних.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна ґрунтується на професійному підході до формулювання дослідницьких завдань, коректному використанні аналітичного

та числового апарату досліджень методів та логічно правильному обґрунтуванні прийнятих припущень при виборі математичних моделей.

Результати досліджень представлені у вигляді таблиць, графіків і рисунків. Прийняті в дисертації рішення мають наукову новизну та вирішують поставлені завдання досліджень, у ході розв'язання яких здійснено програмну реалізацію системи дослідження кіберзлочинів.

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

Наукові результати, що включають моделі ізоляційного лісу та GPT, можуть слугувати основою для розробки прогностичних інструментів, які допомагають організаціям прогнозувати потенційні кіберзагрози та планувати відповідні стратегії зміцнення інформаційної безпеки. Також, використання моделей ізоляційного лісу та GPT може значно підвищити ефективність систем безпеки в енергетиці, телекомунікаціях та інших галузях, що відповідають за критичну інфраструктуру, та тим самим зміцнити національну безпеку. Крім того, результати дослідження можуть бути інтегровані в існуючі системи штучного інтелекту, щоб автоматизувати процес виявлення та реагування на інциденти безпеки, зменшуючи таким чином час до реагування та покращуючи загальну ефективність системи безпеки.

Також їх можна впровадити у навчальний процес у курсі "Технології Розслідування інцидентів Інформаційної Безпеки " для студентів спеціальності 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів полягає у тому, що:

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 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;

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.

Результати дисертаційної роботи використано і впроваджено у з метою покращення процесів виявлення інцидентів інформаційної безпеки компанією ТОВ “Бінарікс Україна”, 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.

Зауваження по дисертації.

1. У третьому розділі автор не описує як запропонована модель системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем інтегрується з існуючими інструментами моніторингу безпеки. Для забезпечення безперервної роботи інформаційних систем важливо, щоб модель безпеки могла легко взаємодіяти з уже наявними інструментами та системами повідомлень про події інформаційної безпеки. Наявність відповідного опису пришвидшило б інтеграцію та впровадження моделі в існуючі операційні центри безпеки.

2. Розділ 3.5 не містить достатнього обґрунтування вибору мови програмування для реалізації системи дослідження кіберзлочинів. Вибір мови програмування може впливанути на продуктивність, масштабованість та підтримку системи. Автор зазначає переваги Python, проте відсутня оцінка ризиків використання даної мови програмування. Зокрема, обмеження багатопоточності та можливі затримки через автоматичне управління пам'яттю можуть негативно впливати на роботу системи. Необхідно включити аналіз цих аспектів для повного обґрунтування для Python.

3. У четвертому розділі автором не зазначено як модель системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем опрацьовує хибно-позитивні події під час . Хибно-позитивні події можуть негативно впливати на ресурси компанії та на обробку подій інформаційної

безпеки операційних центрів безпеки. Високий рівень хибно-позитивних подій знижує ефективність моделі, тому варто було б дослідити відсоток хибно-позитивних подій який генерується моделлю більш детально.

4. При викладені змісту дисертації дисертант допускає окремі неточності термінологічного і стилістичного плану, у тексті є помилки.

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

Висновок

Дисертаційна робота Сусукайла Віталія Андрійовича на тему «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» є завершеним та цілісним науковим дослідженням, що містить достатню наукову новизну та практичну цінність отриманих результатів. Дисертаційна робота заслуговує позитивної оцінки, відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», постанові Кабінету Міністрів України №44 від 12.01.2022 р. «Порядок присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». а її автор, Сусукайло Віталій Андрійович заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека»

Офіційний рецензент
Кандидат технічних наук,
старший викладач кафедри захисту інформації
Національного університету
“Львівська політехніка” Андрій ПАРТИКА

Підпис к.т.н, ст.викладача Партики А.І. засвідчую
Вчений секретар Роман БРИЛИНСЬКИЙ
Національного університету
“Львівська політехніка”
к.т.н., доцент