Голові разової спеціалізованої
вченої ради PhD 11813
Хмельницького національного університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО

ВІДГУК

офіційного опонента на дисертаційну роботу
Олександра Олександровича Бохонька
на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії», представлену на здобуття наукового ступеня доктора філософії в галузі знань Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації. Соціальна інженерія (СІ) залишається однією з найкритичніших загроз для розподілених комп'ютерних систем (РКС), що працюють на великій кількості гетерогенних вузлів. Зростання числа віддалених користувачів, сервісів, каналів взаємодії та гібридних хмар ускладнює поведінку РКС і збільшує простір її станів. На цьому тлі атаки СІ, поєднуючи психологічні, поведінкові й технічні впливи, підривають стабільність функціонування системи. Наявні підходи здебільшого зводяться до локальних детекторів окремих сценаріїв і моніторингу активності. Хоча вони підвищують точність на окремих каналах, загалом захист лишається фрагментованим: немає узгодженої координації, дані подаються по-різному, а масштабування вузлів і сервісів веде до різкого зростання витрат і слабкої керованості реакції на атаки. Для корпоративних РКС проблема особливо гостра: один успішний прорив у слабкому сегменті може спричинити каскадні наслідки, компрометацію даних і збої сервісів. Це вимагає переходу від «надбудов» до синтезу РКС як багаторівневих багатоагентних архітектур, де стійкість до СІ закладається вже на етапі проєктування.

Додатково ускладнює задачу масштабованість наступне: зі зростанням числа вузлів, каналів і шаблонів атак експоненційно збільшується простір

станів і дій, що обмежує аналітичні підходи та пряме застосування навчання з підкріпленням без засобів зниження розмірності. Тому потрібні механізми, які зберігають якість захисту при масштабуванні без вибухового зростання обчислювальної складності. Попри значний обсяг досліджень, нинішні результати не дають комплексного рішення, яке одночасно забезпечує визначені критерії стійкості, високу достовірність виявлення, адаптивність, масштабованість, живучість і ефективне колективне прийняття рішень.

Тому на даний момент часу існує суперечність між потребою в синтезі комп'ютерних системи, стійких до атак соціальної інженерії, з одного боку, і недосконалістю методів та засобів забезпечення стійкості РКС в умовах атак соціальної інженерії, з іншого боку. Відтак, підвищення стійкості розподілених комп'ютерних систем до атак соціальної інженерії є актуальною науково-прикладною задачею, одним із шляхів розв'язання якої є розроблення методів і засобів синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету. Її зміст відповідає тематиці науково-дослідних робіт за держбюджетною темою Хмельницького національного університету «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980).

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Наукова новизна результатів дисертаційного дослідження полягає в наступному:

вперше розроблено:

1) метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії, який на відміну від відомих підходів поєднує принципи динамічної декомпозиції, багатоагентної взаємодії та адаптивного перерозподілу ресурсів з урахуванням поведінкових характеристик користувачів і загроз, що дає змогу забезпечити керовану масштабованість розподіленої системи без зниження рівня захищеності, підвищити її живучість

за умов зростання кількості вузлів розподіленої КС та інтенсивності атак соціальної інженерії;

2) метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, який на відміну від відомих методів ґрунтується на багатовимірній системі формалізованих критеріїв адаптивності, масштабованості, живучості та достовірності виявлення, що дозволило отримати єдину універсальну метрику оцінювання стійкості РКС до атак соціальної інженерії;

набула подальшого розвитку:

3) архітектуру стійкої до атак соціальної інженерії розподіленої комп'ютерної системи, яка на відміну від відомих базується на ієрархічній багатоагентній основі з застосуванням підкріплювальним навчанням, ентропійно-орієнтованими функціями винагороди, апріорними знаннями у вигляді графа знань та модально-специфічними сервісними агентами, що дає змогу адаптивно зменшувати невизначеність у процесі виявлення атак, скорочувати кількість діалогових кроків і підвищувати точність виявлення та класифікації атак соціальної інженерії;

удосконалено:

4) метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання, який на відміну від відомих підходів ґрунтується на формуванні спеціалізованої множини унікальних мовних ідентифікаторів, їх попередній лінгвістичній нормалізації, експертному маркуванні та застосуванні методу k-найближчих сусідів із подальшим адаптивним налаштуванням гіперпараметрів і порогових значень довіри, що дає змогу підвищити точність та стійкість виявлення атак соціальної інженерії, зменшити кількість хибних спрацьовувань, забезпечити раннє реагування та інтеграцію результатів у контури захисту розподіленої комп'ютерної системи.

Наукові положення, висновки і рекомендації дисертаційної роботи Бохонька О. О. достатньо обґрунтовані коректним використанням математичного апарату, підкріплені успішною реалізацією, ефективним практичним впровадженням результатів дисертаційних досліджень, яке продемонструвало збігання теоретичних досліджень з реальними результатами. При розв'язанні поставленої науково-прикладної задачі використовувались

аналіз та синтез, методи аналізу та моделювання процесів, теоретико-множинні підходи, апарат модельно-орієнтованих підходів, принципи загальної теорії систем та системного аналізу, принципи побудови баз знань та формування логічного висновку, методи емпіричного дослідження, основні положення абстрактної алгебри, теорії розподілених систем, теорії елементів штучного інтелекту, теорія популяційних моделей та апарат середнього поля.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою і базується на детальному аналізі джерел за даною проблемою, чіткій постановці задач дослідження, використанні сучасних методів дослідження, правильним застосуванням математичного апарату при теоретичному розгляді наукових положень дисертаційної роботи, а також проявляється у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів, які були використані під час виконання роботи.

Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі, логічно випливають із результатів, отриманих за допомогою чітких викладок. Тому можна стверджувати, що висновки та практичні рішення, отримані у роботі, коректні та достатньо обґрунтовані.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності. За своїм змістом дисертаційна робота здобувача Бохнька О. О. повністю відповідає Стандарту вищої освіти зі спеціальності 123 – Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти та освітньо-науковій програмі Хмельницького національного університету «Комп'ютерна інженерія» за спеціальністю 123 Комп'ютерна інженерія. Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерної інженерії.

Розглянувши результати перевірки дисертаційної роботи, можна зробити висновок, що дисертаційна робота Бохонька Олександра Олександровича є

результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідне джерело.

Практичне значення одержаних результатів. Практична цінність результатів дослідження полягає у доведенні теоретичних положень до етапу програмно-апаратної реалізації та їх успішному впровадженні у діяльність профільних підприємств.

За результатами виконаних досліджень здобувачем реалізовано розподілену комп'ютерну систему, стійку до атак соціальної інженерії. Практична цінність роботи полягає у можливості використання отриманих результатів для розроблення корпоративних політик безпеки, побудови симуляційних тренажерів для дослідження взаємодії користувачів із атаками соціальної інженерії, створення інтелектуальних агентів для кіберзахисту та оптимізації архітектур розподілених систем з урахуванням ризиків. Запропоновані методи можуть застосовуватися у банківській, телекомунікаційній, енергетичній та державній сферах, де критично важливо забезпечити стійкість систем до складних поведінкових загроз.

Результати дисертаційної роботи впроваджено у: ПП «АВІВІ»; ТОВ «ДЖІ ЕМ ХОСТ»; у навчальному процесі Хмельницького національного університету.

Мова та стиль викладення результатів. Дисертаційна робота написана українською мовою. Дисертаційна робота написана логічно, доступно, на високому технічному рівні з використанням сучасної термінології. Матеріали дисертаційної роботи викладено послідовно, доступно для розуміння і сприйняття. Стиль мовлення задовольняє вимоги до текстів науково-технічного змісту. Текст дисертаційної роботи в достатній мірі проілюстрований таблицями та рисунками. Здобувач використовує загальноприйняту термінологію. Дисертаційна робота має логічну структуру.

Дисертація складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел із 190 найменувань на 23 сторінках та 4 додатків на 42 сторінках. Загальний обсяг

дисертаційної роботи становить 241 сторінка друкованого тексту, з них 157 сторінок основного тексту. Дисертаційна робота містить 7 рисунків та 16 таблиць.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи. Основні результати дисертаційної роботи опубліковані у 9 наукових працях, серед яких 5 статей у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б; 4 публікації, які засвідчують апробацію матеріалів дисертаційної роботи (статті в матеріалах конференцій, що індексуються в наукометричній базі Scopus).

Також результати дисертаційної роботи були апробовані на 4 міжнародних науково-технічних та науково-практичних конференціях та семінарах, а саме: 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2023), 2024 IEEE 14th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024), The 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2024), The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2025).

Сумарно опубліковані праці віддзеркалюють повноту викладу результатів дисертаційної роботи. Науковий рівень публікацій – високий. У всіх публікаціях здобувачем дотримано принципів академічної доброчесності.

Таким чином, наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи:

1. У першому розділі дисертаційної роботи в пункті 1.2 було б доцільно надати додатковим каналом та джерелом здійснення атак соціальної інженерії на розподілені комп'ютерні системи так звані зловмисні агенти на основі штучного інтелекту, що продукують атаки із застосуванням технології соціальної інженерії.

2. Пункт 2.1 другого розділу дисертаційної роботи має ознаку незавершеності. Було б доцільно вказати необхідність та повноту запропонованої моделі.

3. У другому розділі дисертаційної роботи в пункті 2.2, який присвячено опису архітектури стійкої до атак соціальної інженерії розподіленої комп'ютерної системи, робиться припущення розділення атак соціальної інженерії на групи (класи), що не перетинаються, однак на практиці частина операцій (атрибутів) кількох груп можуть бути спільними, що може ускладнити віднесення певного зловмисного функціоналу до певного класу.

4. У другому розділі в пункції 2.2.3 при описі розміру винагороди сервісних агентів та агентів прийняття рішення фігурує незрозуміле поняття «епізод» в реченні «…інформаційний приріст між епізодами…».

5. Схема архітектури РКС, стійкої до атак соціальної інженерії, на основі ієрархічної багатоагентної системи, яка подана рисунком 2.1 (стор. 58), містить слово «ВИХІД», що, очевидно, є некоректним перекладом слова «РЕЗУЛЬТАТ» з англомовної версії даного рисунку.

6. У другому розділі у викладці основ методу виявлення кібератак соціальної інженерії в розподілених КС на основі унікального лінгвістичного ідентифікатора формулювання не вказано конкретні значення гіперпараметрів при застосуванні методу k-найближчих сусідів.

7. Дисертаційна робота має певну кількості граматичних, орфографічних, синтаксичних та стилістичних помилок.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

Висновок про дисертаційну роботу. Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Бохонька Олександра Олександровича на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі інформаційних технологій. Дисертаційна робота за актуальністю,

практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 6 – 9 «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 від 12 січня 2022 р. № 44 (із змінами).

Здобувач Бохонько Олександр Олександрович заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент:
професорка кафедри
кібербезпеки та інтелектуальних
інформаційних технологій
факультету радіоелектроніки,
комп'ютерних систем та інфокомунікацій
Національного аерокосмічного університету
«Харківський авіаційний інститут»,
доктор технічних наук, професор Ольга МОРОЗОВА

Підпис д.т.н., професора Морозової Ольги Ігорівни засвідчую

Учений секретар
Національного аерокосмічного університету
«Харківський авіаційний інститут» Тетяна БОНДАРЄВА

М.П. «09» березня 2026 року