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

РЕЦЕНЗІЯ
на дисертаційну роботу Бохонька Олександра Олександровича на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.

Розподілені комп'ютерні системи (РКС) стали основою сучасної цифрової економіки. Вони обробляють значні об'єми даних, підтримують та обслуговують критичну інфраструктуру, забезпечують роботу та взаємодію мільярдів пристроїв. Водночас, їх архітектура та принципи організації передбачають наявність множинних точок входу, зокрема і для атак. А компрометація навіть одного вузла чи користувача може призводити до каскадного поширення загроз.

Атаки соціальної інженерії в РКС залишаються одним із найрезультативніших векторів компрометації, експлуатуючи не вразливості коду чи апаратури, а людський фактор і організаційні прогалини. За даними провідних лабораторій з кібербезпеки, відсоток атак із використанням людського фактору становить від 55-75%, а атаки соціальної інженерії у цій частці становлять до 46%. Оцінки фінансових ризиків за даними CRC Group в середньому складають 130 тис. доларів на одну атаку соціальної інженерії. Це свідчить про недостатність наявних засобів та підходів протидії атакам соціальної інженерії.

Зростання складності й динамічності сучасних розподілених архітектур знижує ефективність класичних периметрових підходів і потребує нових принципів синтезу комп'ютерних систем. Важливим аспектом синтезу РКС є забезпечення їх стійкості. Соціальна інженерія часто є початковою стадією складніших кібератак, а наслідки в розподілених середовищах масштабуються швидше через автоматизацію та взаємозалежність компонентів. Тому стійкість має забезпечуватися не лише політиками й навчанням персоналу, а й

архітектурними механізмами контролю доступу, верифікації дій та управління довірою. Саме тому потрібні методи та засоби синтезу розподілених комп'ютерних систем, які інтегрують технічні й організаційні контрзаходи в єдину модель проєктування.

Наявні результати наукових досліджень у сфері синтезу РКС не формують цілісних комплексних рішень. Зокрема, залишаються недостатньо опрацьованими та узгодженими між собою критерії стійкості, достовірність виявлення атак, а також вимоги до адаптивності, масштабованості й живучості систем. Окремої уваги потребує підвищення ефективності механізмів прийняття колективних рішень в умовах динамічних загроз.

Таким чином, підвищення стійкості розподілених комп'ютерних систем до атак соціальної інженерії є актуальною науково-прикладною задачею, одним із напрямів розв'язання якої є розроблення методів і засобів синтезу РКС, здатних протидіяти атакам соціальної інженерії.

Зазначена науково-прикладна задача відповідає предметній області Стандарту вищої освіти України зі спеціальності 123 – Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти.

Дослідження, результати яких наведено в дисертації, проведені в рамках науково-дослідної тематики Хмельницького національного університету – держбюджетної науково-дослідної теми «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980), в якій автор дисертації був виконавцем.

Формулювання наукової задачі, мети й задач дослідження.

Здобувачем правильно визначено наукову задачу, об'єкт і предмет дослідження, відповідно до висунутої заздалегідь гіпотези дослідження. Так, науково-прикладною задачею визначено підвищення стійкості до атак соціальної інженерії розподілених комп'ютерних систем шляхом розроблення методів та засобів синтезу стійких до атак соціальної інженерії РКС, які комплексно забезпечують достовірність виявлення атак, адаптивність, масштабованості, живучість та ефективність прийняття колективних рішень вузлів РКС. Об'єктом дослідження визначено процес синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем. Предметом дослідження визначено моделі, методи та засоби синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем.

Мету дисертаційного дослідження визначено як підвищення стійкості до атак соціальної інженерії розподілених комп'ютерних систем шляхом розроблення методів та засобів синтезу стійких до атак соціальної інженерії РКС, які комплексно забезпечують достовірність виявлення атак, адаптивність,

масштабованості, живучість та ефективність прийняття колективних рішень вузлів РКС.

Поставлену мету досягнуто в результаті розв'язання таких задач:

- проведено аналіз відомих методів і засобів забезпечення стійкості розподілених комп'ютерних систем до атак соціальної інженерії;
- розроблено формальну модель розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, яка описує колективну поведінку агентів у динамічному середовищі шляхом узгодженого прийняття рішень, обміну інформацією та адаптивного керування ресурсами з метою максимізації глобальної функції корисності, що відображає стійкість системи до атак соціальної інженерії, забезпечення достовірного виявлення загроз, підтримання безперервності функціонування, збереження живучості за умов часткової компрометації вузлів і масштабування системи;
- розроблено архітектуру стійкої до атак соціальної інженерії розподіленої комп'ютерної системи, яка базується на ієрархічній багатоагентній основі з застосуванням підкріплювального навчання, що дає змогу адаптивно зменшувати невизначеність у процесі виявлення атак та підвищувати точність виявлення та класифікації атак соціальної інженерії;
- розроблено метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання, який ґрунтується на формуванні спеціалізованої множини унікальних мовних ідентифікаторів, застосуванні методу k-найближчих сусідів, що уможливлює раннє виявлення мовних та семантичних маніпуляцій у сценаріях атак на розподіленої комп'ютерної системи;
- розроблено метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії на основі популяційної моделі багатоагентної системи та середнього поля, що забезпечує формування оптимальної політики поведінки репрезентативного агента, інтеграцію архітектурних параметрів та гарантовану масштабованість системи при зростанні кількості вузлів і інтенсивності атак;
- розроблено метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, базований на багатовимірній системі критеріїв адаптивності, масштабованості, живучості та достовірності виявлення деструктивних впливів, із формуванням узагальненої метрики ефективності на основі нормованих вагових коефіцієнтів;
- розроблено архітектуру програмного забезпечення реалізації розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, яка включає агента прийняття рішень, сервісних агентів, компоненти моніторингу станів, менеджер взаємодії та модулі мовного/семантичного аналізу; провести

експериментальні дослідження її характеристик у сценаріях впливів атак соціальної інженерії та оцінити покращення показників стійкості системи.

Наукова новизна одержаних автором результатів полягає в наступному:

1) вперше розроблено 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) вперше розроблено 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;

3) набула подальшого розвитку архітектура 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;

4) удосконалено 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.

Короткий аналіз основного змісту дисертації.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку літератури та додатків. Загальний обсяг роботи становить 241 сторінка, з них 157 сторінок основного тексту.

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об'єкт дослідження, наведено наукову новизну, практичне значення одержаних результатів.

Перший розділ дисертації присвячений аналізу відомих методів і засобів забезпечення стійкості розподілених комп'ютерних систем до атак соціальної інженерії, уточнено поняття та вплив таких атак, визначено ключові канали РКС, що використовуються зловмисниками, виконано огляд і порівняння наявних підходів, сформульовано висновки та постановку задачі дослідження.

Другий розділ дисертації присвячено розробленню моделей і методів синтезу РКС, стійких до атак соціальної інженерії, запропоновано модель та архітектуру стійкої РКС на основі ієрархічної багатоагентної системи, визначено механізми винагороди та побудови знань для менеджера взаємодії, розроблено моделі атак, а також метод виявлення атак соціальної інженерії на основі унікального лінгвістичного ідентифікатора з використанням класифікації k-найближчих сусідів і проведено експериментальні дослідження.

Третій розділ дисертації присвячено синтезу масштабованої архітектури РКС, стійкої до атак соціальної інженерії, а саме розроблено метод забезпечення масштабованості на основі популяційної мультиагентної системи, виконано експериментальні перевірки, а також запропоновано метод комплексного оцінювання стійкості РКС до атак соціальної інженерії.

Четвертий розділ дисертації присвячено практичній реалізації розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії і сформульовано висновки щодо отриманих результатів.

У висновках дисертації подано отримані наукові та практичні результати дослідження. Основні висновки і рекомендації логічно витікають із результатів, які наведено у розділах роботи.

За своїм змістом дисертаційна робота Бохонька О.О. повністю відповідає Стандарту вищої освіти зі спеціальності 123 – Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти. Дисертаційна робота є завершеною науковою працею та свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерної інженерії.

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

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові висновки та рекомендації, наведені в дисертації, ґрунтуються на адекватному та цілеспрямованому використанні методів аналізу, аналізу та синтезу, методів аналізу та моделювання процесів, теоретико-множинних підходах, апарату модельно-орієнтованих підходів, принципів теорії систем та системного аналізу, принципів побудови баз знань та формування логічного висновку, методів емпіричного дослідження, основних положеннях абстрактної алгебри, теорії розподілених систем, теорії елементів штучного інтелекту, теорії популяційних моделей та апарату теорії середнього поля.

Успішна реалізація розподіленої системи, стійкої до атак соціальної інженерії, а також ефективне впровадження результатів дослідження в комерційну діяльність підприємств демонструє відповідність отриманих теоретичних результатів реальним результатам їхнього використання.

Практичне значення одержаних результатів.

Практична цінність отриманих результатів полягає у тому, що всі теоретичні положення, обґрунтовані в дисертаційному дослідженні, доведено до рівня прикладних рішень: розроблено моделі, методи та архітектурні підходи, які можуть бути безпосередньо інтегровані в інформаційну інфраструктуру організацій і використані під час побудови та модернізації систем кіберзахисту. Це забезпечує можливість практичного впровадження результатів на підприємствах різного профілю без необхідності суттєвого перегляду наявних технологічних процесів.

За підсумками виконаних досліджень здобувачем реалізовано прототип розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, що підтверджує працездатність запропонованих підходів і демонструє їх ефективність у реальних або наближених до реальних умовах експлуатації. Отримані результати можуть бути використані для формування та уточнення корпоративних політик інформаційної безпеки (зокрема щодо регламентів комунікації, верифікації запитів, управління інцидентами та навчання персоналу), а також для підвищення зрілості процесів кіберзахисту шляхом поєднання організаційних і технічних контрзаходів проти поведінкових загроз.

Запропоновані методи та реалізовані рішення можуть бути впроваджені в банківському секторі, телекомунікаціях, енергетиці, а також у державних структурах і критично важливих інформаційних системах, де особливо актуальним є забезпечення безперервності функціонування та стійкості до складних атак, що поєднують технічні й поведінкові (людиноорієнтовані) механізми впливу.

Теоретичні та практичні результати дослідження впроваджені в: ПП «АВІВІ»; ТОВ «ДЖІ ЕМ ХОСТ»; у навчальному процесі Хмельницького національного університету (акт впровадження від 30.09.2025 р.); при виконанні держбюджетної теми Хмельницького національного університету «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980).)

Особистий внесок здобувача полягає в аналізі відомих методів і засобів забезпечення стійкості розподілених комп'ютерних систем до атак соціальної інженерії; розробленні архітектури, стійкої до атак соціальної інженерії розподіленої комп'ютерної системи; розробленні методу виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання; розробленні методу забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії на основі популяційної моделі багатоагентної системи та середнього поля; розробленні методу комплексного оцінювання стійкості РКС до атак соціальної інженерії; розробленні архітектури програмної реалізації розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії. Усі наукові результати дисертаційного дослідження отримані автором особисто. У публікаціях, що опубліковані у співавторстві, здобувачеві належать основні ідеї, теоретична та практична розробка положень, відображених у науковій новизні отриманих результатів.

За результатами проведених досліджень основні наукові результати 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 дисертації (статті в матеріалах конференцій, що індексуються в наукометричній базі Scopus).

Апробація матеріалів дисертації.

Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету. Наукові результати доповідались та обговорювались на 4 міжнародних науково-технічних 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).

Недоліки та зауваження до дисертаційної роботи.

1. У другому розділі дисертації в пункті 2.1 детально подано модель розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, яка описує компоненти системи як частини багатоагентних систем. Однак опис досить узагальнений і не містять специфіки пов'язаної з засобами протидії атакам соціальної інженерії, що б додало цілісності моделі в розрізі вирішуваної дисертантом задачі.

2. Ефективність методу синтезу РКС у розділі 2.5 оцінено результатами моделювання, однак в роботі не оцінено достовірність, адекватність та точність запропонованих моделей.

3. При вирішенні задачі побудови розподілених комп'ютерних систем, стійких до атак соціальної інженерії у методах не враховано рівень підготовленості персоналу (користувачів), що, ймовірно, може впливати на кінцеву ефективність виявлення та протидії атакам соціальної інженерії.

4. Певні символи у роботі та формулах позначать кілька різних сутностей, зокрема, символ К у роботі зустрічається у багатьох формулах і позначає різне, наприклад, К - кількість груп атак соціальної інженерії (ст. 60), К - кількість сервісних агентів (ст.63), К - кількість відмінних типів вузлів (ст. 118) та ін. Це вносить певну невизначеність та ускладнює сприйняття матеріалу.

5. Другий розділ, а саме пункт 2.2 містить технічну помилку подання тексту, зокрема, повторення підпунктів 2.2.2 – 2.2.5.

6. У дисертації автор припустився деяких орфографічних та пунктуаційних помилок, зустрічаються неузгодженості відмінків слів, пропущені слова тощо.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий, рівень проведеного дослідження.

Загальний висновок.

Вважаю, що дисертаційна робота Бохонька Олександра Олександровича на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії» містить нові науково обґрунтовані теоретичні та експериментальні результати за спеціальністю 123 Комп'ютерна інженерія галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі Підвищення стійкості до атак соціальної інженерії розподілених комп'ютерних систем.

Дисертаційна робота «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає пп. 6, 7, 8, 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), а її автор, Бохонько Олександр Олександрович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
доцент кафедри комп'ютерної інженерії
та інформаційних систем
Хмельницького національного
університету, кандидат технічних
наук, доцент Дмитро МЕДЗАТИЙ

«Підпис Дмитра МЕДЗАТОГО засвідчую»:
Проректор з наукової роботи ХНУ Олег СИНЮК