ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії»

(назва роботи)

здобувача наукового ступеня доктора філософії

Бохонька Олександра Олександровича

(прізвище, ім'я, по батькові)

з галузі знань 12 – Інформаційні технології

(шифр, назва галузі знань)

за спеціальністю 123 – Комп'ютерна інженерія.

(шифр, назва спеціальності)

Публічна презентація проведена на кафедрі комп'ютерної інженерії та інформаційних систем

(назва)

«20» січня 2026 року, протокол № 15.

1. Актуальність теми дослідження

Соціальна інженерія (СІ) залишається одним із найнебезпечніших класів загроз для сучасних розподілених комп'ютерних систем (РКС), у яких події обробляються, ресурси надаються, а захист реалізується на великій кількості гетерогенних вузлів [1]. Збільшення кількості віддалених користувачів, сервісів, мультимодальних каналів взаємодії (електронна пошта, веб, голосові дзвінки, месенджери, соціальні мережі), а також поява гібридних хмарних середовищ призводить до різкого зростання розмірності простору станів РКС та складності їхньої поведінки. На цьому фоні атаки соціальної інженерії використовують психологічні вразливості користувачів, керують ланцюжками дій у часі та поєднують технічні й поведінкові вектори впливу, що перешкоджає стабільному функціонуванню РКС [2].

Існуючі рішення здебільшого зосереджуються на розробленні окремих детекторів конкретних сценаріїв атак (вішинг, фішинг, клонування профілю, шахрайські URL-адреси тощо) та локальних засобів моніторингу користувацької активності. Такі засоби підвищують точність виявлення на окремих каналах, однак залишаються «надбудовами» над уже побудованими системами і не змінюють сам спосіб формування РКС. У результаті захист має фрагментований характер: різні компоненти працюють із різними представленнями даних, відсутній цілісний механізм координації детекторів, а масштабування кількості вузлів і сервісів призводить до вибухового зростання обчислювальних витрат та неможливості забезпечити узгоджену реакцію на атаки.

Особливої гостроти проблема набуває для корпоративних РКС, де одночасно діють сотні й тисячі вузлів, об'єднаних складною топологією, з різними класами користувачів, сервісів і каналів обміну даними. У таких умовах навіть високоточні локальні детектори не гарантують стійкості системи в цілому: атака, що пройшла через один слабкий сегмент, здатна ініціювати каскадні ефекти, компрометацію конфіденційних даних і критичні порушення сервісів. Це зумовлює потребу переходу від локального

проєктування окремих засобів виявлення до синтезу самих РКС як багаторівневих, багатоагентних архітектур, у яких властивість стійкості до атак соціальної інженерії закладається вже на етапі проєктування.

Додатковим викликом є питання масштабованості, оскільки кількість вузлів у сучасних РКС постійно зростає і при цьому зростають кількість каналів взаємодії та шаблонів атак. Це призводить до експоненційного збільшення простору станів і дій, що робить неможливими як точні аналітичні розв'язки, так і пряме застосування методів навчання з підкріпленням без спеціальних засобів зниження розмірності. Тому від захисних механізмів вимагається не просто висока точність, а здатність зберігати якість роботи за зростання масштабів РКС без вибухового зростання обчислювальної складності.

Незважаючи на велику кількість проведених наукових досліджень в сфері синтезу РКС, стійких до атак соціальної інженерії, на сьогодні ці результати не забезпечують комплексних рішень щодо критеріїв стійкості, достовірносі виявлення атак, адаптивності, масштабованості, живучості та ефективності прийняття колективних рішень.

Таким чином, 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.

2. Зв'язок роботи з науковими програмами, планами, темами

Дослідження, результати яких викладено в дисертації, виконано під час виконання 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), у якій автор був виконавцем і виконував апробацію напрацьованих методів та засобів виявлення ЗПЗ та комп'ютерних атак в розподілених комп'ютерних системах.

3. Наукова новизна отриманих результатів.

У дисертації одержані такі нові наукові результати:

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.

4. Теоретичне та практичне значення результатів дисертації

На теоретичному рівні застосовуються методи ідеалізації (оперування ідеальними об'єктами, які, на відміну від реальних, характеризуються обмеженою кількістю властивостей), сходження від абстрактного до конкретного. Емпіричне дослідження в якості методів використовує емпіричний опис, реальний експеримент, складання графіків, таблиць тощо. В дисертації задача синтезу зводиться до розроблення моделей, методів та архітектури розподіленої комп'ютерної системи. Стійкої до атак соціальної інженерії», а задача аналізу – до підвищення стійкості до атак соціальної інженерії РКС.

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.

Практична цінність отриманих результатів полягає в реалізації усіх теоретичних положень, поданих в дисертаційному дослідженні, у прикладні рішення та можливості їх безпосереднього впровадження й використання на підприємствах.

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.

5. Використання результатів роботи

Результати дисертаційної роботи впроваджено у: ПП «АВІВІ» (акт впровадження від 08.1.2025 р.); ТОВ «ДЖІ ЕМ ХОСТ» (акт впровадження від 30.12.2025 р.); 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).

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі Бохонька О.О.

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету,
(*назва кафедри (відділу), назва установи)*
науковий керівник д.т.н., професор, професор кафедри комп'ютерної інженерії та інформаційних систем ХНУ Лисенко С.М., д.т.н., професор.
(*науковий ступінь, вчене звання, посада, прізвище, ініціали)*

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Бохонька Олександра Олександровича
(прізвище, ініціали здобувача)
є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковані 9 наукових праць. Основні результати дисертації викладені у: 5 статтях у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б, чотири з яких, згідно із п.8 Постанови Кабінету Міністрів України від 12 січня 2022 р. № 44 (із змінами), можуть бути зараховані як 0,5 одна публікація оскільки число співавторів у ній (разом із здобувачем) становить більше двох осіб, та 1.0 - решта чотири публікації; **отже, для захисту зараховано 4.5 наукових публікації з викладеними основними результатами досліджень**. Крім цього, результати дисертації викладені у 4 публікаціях, які засвідчують апробацію матеріалів дисертації (статті в матеріалах конференцій, що індексуються в наукометричній базі Scopus).

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Лисенко С., Атаманюк О., Бохонько О., Воробйов В. Дослідження методів виявлення кіберзагроз типу RANSOMWARE на основі застосування HONEYPOT. Вісник ХНУ. 2023. №1, (317). С. 300-309. https://doi.org/10.31891/2307-5732-2023-317-1-300-309

О. Бохоньком виконано аналіз методів та засобів виявлення кіберзагроз типу RANSOMWARE на основі застосування HONEYPOT, С. Лисенко виконував адміністрування та концептуалізацію дослідження, О. Атаманюк, В. Воробйов, сумісно з автором та під його керівництвом працювали над оглядом існуючих методів та рішень.

2. Лисенко С., Бохонько О. Методи виявлення кібератак соціальної інженерії. Вісник ХНУ. 2023. №327(5(2). С. 231-236. https://doi.org/10.31891/2307-5732-2023-327-5-231-236.

О. Бохоньком виконано аналіз методів виявлення атак соціальної інженерії, С. Лисенко виконував адміністрування та концептуалізацію дослідження.

3. Бохонько О., Лисенко С. Моделі атак соціальної інженерії. Measuring and computing devices in technological processes. 2025. № (1), С. 432–444. https://doi.org/10.31891/2219-9365-2025-81-55 .

О. Бохоньком розроблено моделі атак соціальної інженерії, С. Лисенко виконував адміністрування та концептуалізацію дослідження.

4. Бохонько О. Лисенко С. Метод синтезу розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії. Measuring and computing devices in technological processes, vol. 84(4), pp. 152–163. https://doi.org/10.31891/2219-9365-2025-84-16 .

О. Бохоньком розроблено метод синтезу розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, С. Лисенко виконував адміністрування та концептуалізацію дослідження.

5. Bokhonko O., Atamaniuk O. Method for synthesis of a scalable architecture of a distributed computer systems, resistant to social engineering attacks. Computer Systems and Information Technologies. 2025. Vol.4. pp. 60-76. https://doi.org/10.31891/csit-2025-4-7

О. Бохоньком розроблено метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії, О. Атаманюк сумісно з автором та під його керівництвом працювала над оглядом існуючих методів та рішень.

Праці, які засвідчують апробацію матеріалів дисертації:

6. Lysenko S., Bokhonko O., Savenko O., Vorobiov V., Gaj P., Wołoszyn J. Social Engineering Attacks Detection Approach. Proceedings of 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2023, Athens, Greece, October 13-15, 2023). Pp. 318-329.

О. Бохоньком розроблено метод виявлення атак соціальної інженерії, С. Лисенко виконував адміністрування та концептуалізацію дослідження.

7. Lysenko S., Bokhonko O., Vorobiyov V., Gaj P. A Method for identifying cyberattacks based on the use of social engineering over the phone. CEUR-WS. 2024. Vol. 3675. Pp. 318-329. URL: https://ceur-ws.org/Vol-3675/paper23.pdf .

О. Бохоньком розроблено метод виявлення атак соціальної інженерії через телефон, С. Лисенко виконував адміністрування та концептуалізацію дослідження.

8. Lysenko S., Bokhonko O., Savenko O., Gaj P., Social Engineering Attacks Models. Proceedings of 2024 IEEE 14th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024, Athens, Greece, October 11-13, 2024).

О. Бохоньком розроблено моделі атак соціальної інженерії, С. Лисенко виконував адміністрування та концептуалізацію дослідження

9. Bokhonko O., Atamaniuk O., Sochor T. Model of a distributed heterogeneous system resistant to leakage of confidential information CEUR-WS. 2025. Vol. 3963. Pp. 363-376. URL: https://ceur-ws.org/Vol-3963/paper29.pdf .

О. Бохоньком розроблено модель розподіленої системи, стійкої до витоку конфіденційної інформації, С. Лисенко виконував адміністрування та концептуалізацію дослідження

ВВАЖАТИ, що дисертаційна робота Бохонька Олександра Олександровича
(прізвище, ініціали здобувача)
«Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії»,
(назва)
яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам 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», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 123 – Комп'ютерна інженерія.
(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії»,
назва роботи
подану Бохоньком Олександром Олександровичем
прізвище, ім'я, по батькові
на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації:

доктор філософії, доцент
(науковий ступінь,
завідувач кафедри комп'ютерної інженерії
та інформаційних систем
вчене звання, посада)

Підпис дійсний підпис
Засвідчую
Начальник відділу кадрів
І.С.Мартинюк

Ольга ПАВЛОВА
Ім'я ПРІЗВИЩЕ