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 наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія

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

Актуальність дослідження виявлення атак соціальної інженерії в розподілених комп'ютерних системах зумовлена тим, що саме людський фактор дедалі частіше стає найменш захищеною ланкою у складних цифрових середовищах, де технічні засоби захисту вже досягли відносної зрілості. У розподілених комп'ютерних системах (РКС) взаємодія між великою кількістю користувачів, сервісів, вузлів і адміністративних доменів створює широкий "простір довіри", у якому зловмисник може маніпулювати не стільки вразливостями програмного коду, скільки поведінкою людей, регламентами та процесами доступу. Соціальна інженерія в такому середовищі перетворюється на інструмент, який обходить традиційні периметрові моделі безпеки: достатньо спровокувати неправильну дію оператора, розкрити облікові дані, підмінити контекст комунікації або змусити користувача легітимно виконати деструктивну операцію, і далі атака масштабується вже "зсередини" інфраструктури.

Особливість РКС полягає у високій динаміці та неоднорідності: компоненти можуть бути розміщені географічно, належати різним організаціям, мати різні політики доступу, оновлюватися з різною швидкістю, використовувати різні механізми аутентифікації та журналювання. У такому контексті соціальна інженерія набуває багатоканального характеру, коли вплив здійснюється через електронну пошту, месенджери, корпоративні портали, голосові дзвінки, підроблені сповіщення від систем моніторингу чи "адміністраторів", а інколи й через ланцюги постачання та партнерські взаємодії. Виявлення таких атак ускладнюється тим, що вони часто не містять явних технічних індикаторів компрометації на початкових етапах, а виглядають як нормальна робоча активність у розподіленому потоці подій.

Дослідження є актуальним тому, що профілактичні заходи на кшталт навчання персоналу, політик безпеки та регламентів доступу, хоча й необхідні, не гарантують прийнятного рівня захисту в умовах реальних операційних процесів і людської помилки. У РКС, де підрозділи працюють розподілено, а взаємодія часто відбувається асинхронно та через різні канали, контроль за дотриманням процедур стає складнішим, а ризик "переконливого" шахрайського втручання зростає. Відповідно, технічні методи виявлення соціальної інженерії повинні доповнювати організаційні засоби, надаючи можливість раннього попередження та локалізації інцидентів до того, як вони перейдуть у стадію масової компрометації або руйнівних змін у розподіленій інфраструктурі.

Попри значну кількість наукових робіт, присвячених синтезу РКС, стійких до атак соціальної інженерії, на сьогодні отримані результати все ще не формують цілісних комплексних рішень, здатних одночасно охопити критерії стійкості, достовірність виявлення атак, адаптивність, масштабованість, живучість і ефективність ухвалення колективних рішень.

Отже, нині спостерігається суперечність між нагальною потребою синтезу комп'ютерних систем, стійких до атак соціальної інженерії, та недостатньою ефективністю наявних методів і засобів забезпечення стійкості РКС в умовах таких атак. Тому підвищення стійкості розподілених комп'ютерних систем до атак соціальної інженерії є актуальною науково-прикладною задачею, одним із ключових шляхів розв'язання якої є розроблення методів і засобів синтезу РКС із вбудованою стійкістю до цих атак.

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 викладено в дисертаційній роботі, проведено 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), в якій автор дисертації був безпосереднім виконавцем.

2. Формулювання наукової задачі, мети й задач дослідження.

Здобувачем правильно визначено наукову задачу, об'єкт і предмет дослідження, відповідно до висунутої заздалегідь гіпотези дослідження. Так, об'єктом дослідження визначено процес синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем. Предметом дослідження є моделі, методи та засоби синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем.

Мету дисертаційної роботи 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 роботи досягнуто в результати розв'язання таких задач: 1) провести аналіз відомих методів і засобів забезпечення стійкості розподілених комп'ютерних систем до атак соціальної інженерії; 2) розробити 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; 3) розробити архітектуру стійкої до атак соціальної інженерії розподіленої комп'ютерної системи, яка базується на ієрархічній багатоагентній основі з застосуванням підкріплювальним навчанням, що дає змогу адаптивно зменшувати невизначеність у процесі виявлення атак та підвищувати точність виявлення та класифікації атак соціальної інженерії; 4) розробити 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; 5) розробити 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; 6) розробити 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; 7) розробити архітектуру програмної 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.

3. Наукова новизна одержаних автором результатів:

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 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;

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.

4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові положення, висновки й рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, успішною реалізацією розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, ефективним практичним впровадженням результатів дисертаційної роботи на підприємствах, що продемонструвало відповідність теоретичних досліджень із реальними результатами застосування.

5. Практичне значення одержаних результатів.

Практична значущість одержаних результатів полягає в тому, що всі теоретичні положення, викладені в дисертаційному дослідженні, доведені до рівня прикладних рішень і можуть бути безпосередньо впроваджені та використані на підприємствах.

У межах виконаних досліджень здобувачем розроблено й реалізовано розподілену комп'ютерну систему, стійку до атак соціальної інженерії. Отримані результати можуть бути застосовані для формування корпоративних політик безпеки, розроблення інтелектуальних агентів захисту та оптимізації архітектур розподілених систем із урахуванням відповідних ризиків.

Запропоновані методи доцільно використовувати в банківському секторі, телекомунікаціях, енергетиці та державних установах, де забезпечення стійкості інформаційних систем до складних поведінкових загроз є критично важливим.

Теоретичні та практичні результати дослідження впроваджені в: 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. Особистий внесок здобувача.

Розроблені здобувачем метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії; метод комплексного оцінювання стійкості РКС до атак соціальної інженерії; архітектуру стійкої до атак соціальної інженерії розподіленої комп'ютерної системи; метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання забезпечують розв'язання поставлених у дисертації задач. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. 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).

У роботах, опублікованих у співавторстві, здобувачеві належать основні ідеї, теоретична та практична розробка положень, а саме: аналіз методів та засобів виявлення атак соціальної інженерії, методи виявлення кібератак соціальної інженерії, дослідження методів виявлення кіберзагроз типу Ransomware на основі застосування Honeypot, моделі атак соціальної інженерії, метод синтезу розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, метод синтезу масштабованої архітектури розподілених комп'ютерних систем, стійкої до атак соціальної інженерії, метод виявлення атак соціальної інженерії, метод виявлення кібератак на основі використання соціальної інженерії під час телефонних розмов, модель розподіленої гетерогенної системи, стійкої до витоку конфіденційної інформації.

7. Апробація матеріалів дисертації.

Основні положення та наукові результати доповідалися та обговорювалися на 4 міжнародних науково-технічних та науково-практичних семінарах і конференціях: 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).

8. Структура та обсяг дисертації.

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. Дисертація 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».

9. Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації:

1) автором дисертації вперше розроблено метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, які детально описано у розділі 3, проте мені не вистачило його деталізованого схематичного представлення для більшого унаочнення;

2) у дисертаційній роботі автор використовує терміни «мультиагентна» і «багатоагентна», було б доречно використовувати один з них;

3) у розділі 4 у підпункті 4.2, присвяченому програмній реалізація КС, для роботи агентів зазначено використання бібліотек RLlib, spaCy, однак не наведено системи конкретних значень параметрів для вирішення поставленої задачі;

4) у методі виявлення кібератак соціальної інженерії в розподілених КС на основі унікального лінгвістичного ідентифікатора формулювання (пункт 2.4) розглядається телефонна атака соціальної інженерії. Однак не зовсім зрозуміло, чому саме ця атака є репрезентативною, оскільки, можливо, вона має типові сценарії для інших атак.

5) другий розділ містить технічну помилку повторного викладення тексту результатів дослідження пункту 2.2.

6) у дисертаційній роботі автор вперше розробив метод забезпечення масштабованості архітектури РКС та метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, а також удосконалив метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах, проте, на мою думку, не візуалізував їх взаємодію у складі цілісної технології в комплексі із розробленими засобами;

7) в роботі трапляються граматичні, орфографічні, синтаксичні та стилістичні помилки, трапляються неузгодженості відмінків слів.

Проте підкреслюю, що зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

10. Загальний висновок.

Дисертаційна робота Бохонька О.О. «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії» є завершеною науковою роботою, яка містить новий та актуальний науково-прикладний внесок. Усі результати, які виносяться на захист, є достовірними та отримані автором особисто.

Тому, з огляду на вище вказане, вважаю, що дисертаційна робота «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії», яка подана на здобуття наукового 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 Марія КАПУСТЯН

«Підпис Марії КАПУСТЯН засвідчую»:
Проректор з наукової роботи ХНУ Олег СИНЮК