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

ВІДГУК
офіційного опонента на дисертацію 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

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується широким упровадженням розподілених комп'ютерних систем (РКС), які функціонують на значній кількості гетерогенних вузлів, інтегрують локальні та хмарні ресурси, підтримують мультимодальні канали взаємодії та забезпечують доступ великої кількості віддалених користувачів. Ускладнення архітектурної організації таких систем, зростання кількості сервісів і динамічність топології призводять до різкого збільшення розмірності простору станів РКС, що істотно ускладнює забезпечення їхньої інформаційної безпеки.

За цих умов соціальна інженерія залишається одним із найбільш небезпечних класів загроз, оскільки поєднує технічні механізми впливу з експлуатацією когнітивних і поведінкових вразливостей користувачів. На відміну від традиційних атак, спрямованих на програмно-апаратні компоненти, атаки соціальної інженерії реалізуються через людину як елемент системи, що суттєво ускладнює їх формалізацію, моделювання та прогнозування. Наслідком успішної реалізації таких атак є порушення конфіденційності, цілісності та доступності інформаційних ресурсів, а також дестабілізація функціонування РКС у цілому.

Аналіз існуючих підходів до протидії атакам соціальної інженерії свідчить, що більшість рішень орієнтовані на локальне виявлення окремих сценаріїв (фішинг, spear-phishing, pretexting тощо) та реалізуються у вигляді ізольованих детекторів або підсистем моніторингу. Хоча такі засоби забезпечують підвищення точності виявлення в межах окремих каналів взаємодії, вони не формують цілісної архітектури захисту. Фрагментованість даних, відсутність узгоджених механізмів координації між компонентами та зростання

обчислювальних витрат у процесі масштабування знижують загальну стійкість РКС. У корпоративних середовищах із сотнями та тисячами вузлів навіть високоточні локальні механізми детекції не гарантують системної безпеки, оскільки компрометація одного елемента може спричинити каскадне поширення інциденту.

Отже, виникає потреба переходу від точкових засобів виявлення до концепції синтезу розподілених комп'ютерних систем як багаторівневих багатоагентних архітектур, у яких механізми стійкості до атак соціальної інженерії інтегруються на етапі проєктування. Такий підхід передбачає формування узгоджених критеріїв стійкості, забезпечення адаптивності до змін загрозового ландшафту, підтримку масштабованості, живучості та колективного прийняття рішень в умовах невизначеності.

Незважаючи на значну кількість наукових досліджень у сфері синтезу РКС та методів протидії соціальній інженерії, на сьогодні відсутні комплексні рішення, які б одночасно забезпечували формалізовані критерії стійкості, гарантовану достовірність виявлення атак, узгоджену міжвузлову координацію, адаптивність до нових сценаріїв впливу та прийнятну обчислювальну складність. Наявні результати здебільшого розглядають окремі аспекти проблеми без інтеграції їх у єдину методологію синтезу систем.

Таким чином, актуальність теми дисертаційного дослідження зумовлена наявністю суперечності між об'єктивною потребою у створенні розподілених комп'ютерних систем, стійких до атак соціальної інженерії в умовах масштабованих гібридних середовищ, та недостатнім рівнем розвитку теоретичних і прикладних методів забезпечення такої стійкості. Розроблення методів і засобів синтезу РКС із вбудованими механізмами протидії соціальній інженерії є науково обґрунтованою та практично значущою задачею, розв'язання якої сприятиме підвищенню рівня інформаційної безпеки сучасних розподілених інфраструктур.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукова новизна дисертаційного дослідження полягає в отриманні таких наукових 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 актуальних загроз. Це дає змогу забезпечити

керовану масштабованість розподіленої системи без зниження рівня її захищеності, підвищити живучість в умовах зростання кількості вузлів розподіленої комп'ютерної системи та інтенсивності атак соціальної інженерії.

2. *Вперше розроблено метод комплексного оцінювання стійкості РКС до атак соціальної інженерії,* який, на відміну від існуючих методів, ґрунтується на багатовимірній системі формалізованих критеріїв адаптивності, масштабованості, живучості та достовірності виявлення. Це дозволило сформувати єдину універсальну метрику кількісного оцінювання стійкості розподілених комп'ютерних систем до атак соціальної інженерії.

3. *Набула подальшого розвитку архітектура розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії,* яка, на відміну від відомих рішень, базується на ієрархічній багатоагентній моделі із застосуванням підкріплювального навчання, ентропійно-орієнтованих функцій винагороди, апріорних знань у вигляді графа знань та модально-специфічних сервісних агентів. Запропонований підхід забезпечує адаптивне зменшення невизначеності в процесі виявлення атак, скорочення кількості діалогових кроків, а також підвищення точності 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, передбачає формування спеціалізованої множини унікальних мовних ідентифікаторів, їх попередню лінгвістичну нормалізацію, експертне маркування та застосування методу *k*-найближчих сусідів із подальшим адаптивним налаштуванням гіперпараметрів і порогових значень довіри. Це забезпечує підвищення точності та стійкості виявлення атак соціальної інженерії, зменшення кількості хибних спрацьовувань, реалізацію механізмів раннього реагування та інтеграцію результатів у контури захисту розподіленої комп'ютерної системи.

Наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі Бохонька Олександра Олександровича, характеризуються належним рівнем теоретичного обґрунтування та внутрішньою логічною узгодженістю. Їх достовірність забезпечується коректною постановкою наукової проблеми, системним аналізом вихідних передумов і використанням адекватного математичного апарату для формалізації досліджуваних процесів і явищ. Застосовані методи математичного моделювання, аналітичні викладки та отримані теоретичні результати є методологічно вивіреними й відповідають сучасному рівню розвитку відповідної галузі знань.

Обґрунтованість отриманих результатів підтверджується також експериментальною частиною дослідження. Проведені експерименти виконані за чітко визначеною методикою, з використанням релевантних вхідних даних та адекватних критеріїв оцінювання. Порівняння теоретично прогнозованих показників із результатами практичної реалізації засвідчило їх узгодженість, що свідчить про коректність побудованих моделей і достовірність сформульованих наукових положень.

Логічна послідовність викладення матеріалу, аргументованість висновків та їх безпосередній зв’язок із результатами дослідження дають підстави стверджувати, що сформульовані у дисертації наукові положення, практичні рекомендації та рішення є обґрунтованими, методично вивіреними та придатними до подальшого використання в науковій і прикладній діяльності.

Здобувач продемонстрував належний рівень володіння методологією наукових досліджень, уміння формулювати та розв’язувати складні науково-прикладні завдання, здійснювати критичний аналіз отриманих результатів і узагальнювати їх у вигляді завершених теоретичних та практичних положень. Поставлена в дисертаційній роботі мета досягнута повною мірою, а визначені завдання — розв’язані у відповідності до заявленої логіки дослідження.

Практичне значення одержаних результатів полягає у доведенні теоретичних положень до рівня конкретних технічних і організаційних рішень, їх апробації та впровадженні у виробничу діяльність підприємства. Реалізація результатів дослідження підтверджує їх прикладну цінність, економічну доцільність та можливість використання для підвищення ефективності функціонування відповідних систем.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

Зміст дисертаційної роботи Бохонька О.О. повністю відповідає вимогам Стандарту вищої освіти за спеціальністю 123 «Комп’ютерна інженерія» для третього (освітньо-наукового) рівня вищої освіти, а також освітньо-науковій програмі ХНУ «Комп’ютерна інженерія» за спеціальністю 123 «Комп’ютерна інженерія». Тематика дослідження узгоджується з об’єктом вивчення та професійної діяльності, як «комп’ютерні системи,…, комп'ютерні мережі, методи та способи подання, отримання, зберігання, передавання, опрацювання та захисту в них інформації,…, архітектура та організація їх функціонування; інформаційні процеси, технології, методи, способи, інструментальні засоби та системи для дослідження, проєктування, налагодження, виробництва й

експлуатації комп’ютерів та комп’ютерних систем і мереж, …, забезпечення якості, надійності та безпеки комп’ютерних систем».

У дисертації розглянуто комплекс взаємопов’язаних теоретичних і прикладних питань, що стосуються синтезу розподілених комп’ютерних систем, стійких до атак соціальної інженерії. Структура роботи є логічною та цілісною: постановка проблеми, аналіз сучасного стану досліджень, розроблення моделей і методів, експериментальна перевірка та узагальнення результатів послідовно відображають хід наукового пошуку. Отримані результати взаємопов’язані, узгоджені між собою та спрямовані на досягнення поставленої мети, що свідчить про завершеність дослідження.

Дисертація має чітко виражений авторський характер. Розроблені моделі, методи, архітектурні рішення та програмна реалізація є результатом самостійної наукової діяльності здобувача. Сукупність отриманих теоретичних і практичних результатів свідчить про наявність особистого внеску автора у розвиток наукового напряму комп’ютерної інженерії, зокрема у сфері підвищення стійкості розподілених систем до сучасних кіберзагроз.

За результатами аналізу звіту подібності, отриманого в процесі перевірки дисертації на текстові збіги, встановлено, що дисертація є результатом самостійних досліджень і не містить ознак фальсифікації, фабрикації, компіляції чи плагіату. Використані ідеї, наукові положення, результати та текстові фрагменти інших авторів належним чином оформлені з посиланнями на відповідні джерела, що відповідає вимогам академічної доброчесності.

Таким чином, зміст дисертації відповідає чинним нормативним вимогам до робіт третього (освітньо-наукового) рівня вищої освіти, дослідження є завершеним, самостійним і виконаним із дотриманням принципів академічної доброчесності.

Мова та стиль викладення результатів

Дисертація виконана державною мовою з дотриманням норм сучасної української науково-технічної мови. Виклад матеріалу характеризується послідовністю, логічною структурованістю та змістовною завершеністю окремих структурних елементів дослідження. Текст дисертації відповідає усталеним вимогам до наукових праць у галузі кібербезпеки та захисту інформації, зокрема щодо чіткості формулювань, аргументованості положень і коректності використання спеціальної термінології.

Стиль викладення є науковим, об’єктивним та аналітичним. Автор коректно застосовує загальноприйнятий категоріально-понятійний апарат, що забезпечує однозначність трактування ключових понять, зокрема у сфері атак

соціальної інженерії, розподілених комп’ютерних систем та багатоагентних архітектур. Формулювання визначень, наукових положень і висновків є виваженими та методологічно обґрунтованими, без надмірної описовості чи декларативності.

Матеріал дисертації структуровано відповідно до класичної логіки наукового дослідження: від постановки проблеми й аналізу сучасного стану питання до розроблення моделей, методів, архітектурних рішень та їх експериментальної перевірки. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 194 сторінки, що є достатнім для повного розкриття теми дослідження.

Ілюстративний матеріал (таблиці, рисунки, структурні та функціональні схеми) органічно інтегрований у текст і сприяє кращому сприйняттю результатів дослідження. Подані графічні матеріали є інформативними, логічно пов’язаними з текстом та відображають ключові етапи моделювання, синтезу й оцінювання стійкості розподілених комп’ютерних систем до атак соціальної інженерії.

У вступі дисертаційного дослідження здобувачем здійснено всебічне обґрунтування актуальності теми в контексті сучасного розвитку комп’ютерної інженерії та потреб інформаційної безпеки в умовах зростання загроз соціальної інженерії. Висвітлено об’єктивні передумови та ключові фактори, які зумовили вибір теми, аргументовано її значущість як у теоретичному, так і в прикладному вимірах. Встановлено місце і роль проведеного дослідження у системі наукових програм та державних і відомчих планів, а також у межах тематики науково-дослідних робіт, що узгоджується з концептуальною та методологічною основою розвитку РКС, стійких до атак соціальної інженерії.

Чітко сформульовано стратегічну мету дослідження та деталізовано комплекс наукових завдань, вирішення яких є необхідним для досягнення цієї мети. Окреслено об’єкт та предмет дослідження, що визначають зміст і спрямованість наукового пошуку. Надано розгорнуту характеристику методології дослідження, включаючи моделювання, методи синтезу та оцінювання стійкості РКС, обґрунтовано доцільність їх застосування та взаємодоповнюваність у процесі отримання достовірних наукових результатів, що забезпечують підвищення надійності та ефективності захисту розподілених комп’ютерних систем від атак соціальної інженерії.

У першому розділі дисертаційної роботи здійснено комплексний аналіз сутності атак соціальної інженерії та механізмів їх реалізації у розподілених комп’ютерних системах. Розкрито особливості впливу людського фактора на

функціонування РКС, визначено основні канали взаємодії, що можуть використовуватися зловмисниками для реалізації атак соціальної інженерії. Проведено систематизований огляд та порівняльний аналіз сучасних підходів до побудови розподілених комп'ютерних систем, стійких до атак СІ, із визначенням їх переваг, обмежень та невирішених проблем. За результатами аналітичного дослідження сформульовано висновки до розділу та обґрунтовано постановку наукової задачі.

Другий розділ присвячено розробленню теоретичних положень, моделей і методів синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії. Запропоновано концептуальну модель стійкої РКС та відповідну архітектуру, побудовану на основі ієрархічної багатоагентної системи, що забезпечує розподіленість функцій моніторингу та реагування. Розроблено формалізовані моделі типових атак соціальної інженерії, які враховують лінгвістичні та поведінкові ознаки. На цій основі запропоновано метод виявлення атак СІ, що базується на використанні унікального лінгвістичного ідентифікатора формулювання та забезпечує підвищення точності ідентифікації потенційно небезпечних інформаційних впливів.

У третьому розділі обґрунтовано підходи до синтезу масштабованої архітектури РКС, стійкої до атак соціальної інженерії. Сформовано метод забезпечення масштабованості на основі популяційної мультиагентної системи, що дозволяє адаптувати структуру та функціональні можливості системи до змін навантаження і характеру загроз. Крім того, запропоновано метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, який інтегрує показники виявлення, реагування та відновлення і забезпечує кількісне визначення рівня захищеності системи.

Четвертий розділ присвячено практичній реалізації запропонованих теоретичних положень. Здійснено розроблення програмного забезпечення та впровадження архітектури розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії. Проведено експериментальні дослідження ефективності синтезу РКС із використанням запропонованих моделей і методів, що підтвердили адекватність теоретичних положень та їх практичну придатність. За результатами апробації сформульовано узагальнені висновки щодо досягнутого рівня стійкості та ефективності функціонування системи.

У загальних висновках дисертації систематизовано отримані наукові та практичні результати, відображено ступінь досягнення поставленої мети та вирішення сформульованих завдань. Основні наукові положення, висновки та рекомендації є логічно обґрунтованими, взаємопов'язаними та безпосередньо

випливають із результатів теоретичних і експериментальних досліджень, наведених у розділах роботи.

Оформлення дисертації відповідає вимогам чинних нормативних документів, зокрема наказу Міністерства освіти і науки України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації». Структура, нумерація, посилання на джерела, оформлення таблиць і рисунків виконані належним чином.

Загалом мова та стиль викладення результатів відповідають вимогам до дисертацій на здобуття наукового ступеня, забезпечують наукову коректність, чіткість і повноту представлення отриманих результатів.

Оприлюднення результатів дисертаційної роботи

Основні наукові результати дисертаційної роботи повною мірою відображені у 9 наукових публікаціях здобувача, що відповідає встановленим вимогам щодо апробації та оприлюднення результатів досліджень. Зокрема, 5 статей опубліковано у фахових наукових виданнях України, які на момент опублікування входили до переліку наукових фахових видань України категорії «Б». У зазначених публікаціях висвітлено ключові теоретичні положення, результати моделювання, розроблені методи синтезу розподілених комп’ютерних систем та підходи до забезпечення їх стійкості до атак соціальної інженерії.

Ще 4 публікації підготовлено за матеріалами міжнародних наукових конференцій, що індексуються в наукометричній базі Scopus, що свідчить про належний рівень наукової новизни та міжнародне визнання отриманих результатів. У цих працях представлено результати експериментальних досліджень, апробацію розроблених моделей і методів, а також порівняльний аналіз їх ефективності.

Результати дисертаційного дослідження апробовано на 4 міжнародних науково-технічних і науково-практичних конференціях та семінарах, зокрема на IEEE 13th International Conference on Dependable Systems, Services and Technologies, IEEE 14th International Conference on Dependable Systems, Services and Technologies, The 5th International Workshop on Intelligent Information Technologies & Systems of Information Security та The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security. Участь у зазначених наукових заходах забезпечила фахове обговорення отриманих результатів, їх критичний аналіз та підтвердження наукової значущості у міжнародному професійному середовищі.

Загальна сукупність опублікованих праць відображає повноту викладу основних положень, висновків і рекомендацій дисертаційної роботи, підтверджує логічну завершеність дослідження та достатній рівень його апробації. Тематика публікацій безпосередньо відповідає змісту дисертації, а їх науковий рівень свідчить про належну теоретичну підготовку здобувача та практичну цінність отриманих результатів.

У підготовлених публікаціях дотримано принципів академічної доброчесності, коректного цитування та належного посилання на використані джерела. Таким чином, наукові результати, викладені в дисертаційній роботі, повністю та системно оприлюднені у фахових і міжнародних виданнях, що відповідає чинним вимогам до дисертаційних досліджень.

Недоліки та зауваження до дисертаційної роботи

Незважаючи на загалом позитивну оцінку дисертаційної роботи та її вагомі наукові й практичні результати, доцільно відзначити окремі зауваження та дискусійні положення, що мають рекомендаційний характер.

1. У підрозділі 1.3 першого розділу наведено ґрунтовний аналіз відомих методів створення розподілених комп’ютерних систем, стійких до атак соціальної інженерії. Водночас для підвищення аналітичної чіткості доцільним було б подання узагальнювальної порівняльної таблиці, у якій було б систематизовано основні переваги та недоліки розглянутих підходів з огляду на розв’язувану в роботі наукову задачу.

2. У першому розділі здійснено детальний огляд методів побудови стійких РКС, проте аналіз існуючих програмно-апаратних засобів реалізації таких систем подано недостатньо повно. Розширення цього аспекту дозволило б посилити практичну орієнтацію дослідження.

3. У роботі обмежено висвітлено питання використання технологій штучного інтелекту для здійснення атак соціальної інженерії. З огляду на сучасні тенденції розвитку генеративних моделей та автоматизованих інструментів впливу на користувачів, розширення цього аспекту сприяло б поглибленню аналітичної частини дослідження.

4. У підрозділі 2.1 при формалізації математичної моделі РКС визначено множину станів агентів і множину дій, проте їх конкретизація (опис можливих станів і типових дій агентів) подана недостатньо деталізовано, що ускладнює відтворюваність моделі іншими дослідниками.

5. В електронній версії рукопису зафіксовано технічну помилку, пов’язану з повторюваністю тексту пунктів 2.2.2–2.2.5 другого розділу.

6. У підрозділі 2.3 детально змодельовано три типи атак соціальної інженерії (вішинг, фішинг, клонування профілю), тоді як у роботі загалом ідентифіковано 16 видів атак. Більш повне формалізоване представлення поведінкових характеристик ширшого спектра атак посилило б універсальність запропонованого підходу.

7. У пункті 2.4 другого розділу для експериментальної перевірки методу виявлення атак соціальної інженерії із застосуванням телефонного зв'язку використано датасет CallHome (проєкт TalkBank). Водночас у тексті недостатньо деталізовано процедуру адаптації набору даних до задачі дослідження, зокрема не наведено обсяг вибірки, критерії відбору, лінгвістичні характеристики та особливості попередньої обробки даних.

8. У пункті 4.2 четвертого розділу наведено опис програмної реалізації комп'ютерної системи, стійкої до атак соціальної інженерії, проте відсутнє графічне подання архітектури програмного забезпечення, що могло б покращити наочність представлення структури та взаємодії компонентів системи.

9. У тексті дисертації наявні поодинокі граматичні, орфографічні, синтаксичні та стилістичні недоліки.

Зазначені зауваження мають рекомендаційний характер, стосуються переважно аспектів структурування матеріалу, деталізації окремих положень і редакційного опрацювання тексту. Вони не впливають на наукову новизну, обґрунтованість і достовірність отриманих результатів та не зменшують їх теоретичного і практичного значення.

Загалом дисертація є завершеним науковим дослідженням, у якому розв'язано актуальну науково-прикладну задачу у сфері кібербезпеки, пов'язану з підвищенням стійкості розподілених комп'ютерних систем до атак соціальної інженерії. Отримані результати характеризуються науковою новизною, методичною обґрунтованістю та практичною цінністю, а їх апробація та впровадження підтверджують досягнення поставленої мети дослідження.

Висновок про дисертаційну роботу

Вважаю, що дисертація здобувача наукового ступеня доктора філософії Бохонька Олександра Олександровича на тему «Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії» є завершеним самостійним науковим дослідженням, виконаним на високому теоретичному та методичному рівнях. У роботі отримано сукупність нових науково обґрунтованих теоретичних і практичних результатів, що забезпечують

розв'язання актуального наукового завдання у сфері комп'ютерної інженерії, пов'язаного з підвищенням стійкості розподілених комп'ютерних систем до атак соціальної інженерії.

Наукові положення, висновки та рекомендації є обґрунтованими, достовірними й підтвердженими результатами теоретичних і експериментальних досліджень. Дисертаційне дослідження не містить ознак порушення принципів академічної доброчесності. Отримані результати характеризуються науковою новизною, практичною значущістю та можуть бути використані у процесах проєктування і впровадження захищених розподілених комп'ютерних систем.

За актуальністю, рівнем наукової новизни, теоретичною та практичною цінністю дисертація повністю відповідає вимогам пунктів 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 Кабінет Міністрів України від 12 січня 2022 р. № 44 (із змінами).

Таким чином, здобувач Бохонько Олександр Олександрович заслуговує на присудження ступеня доктора філософії в галузі знань 12 – Інформаційні технології за спеціальністю 123 – Комп'ютерна інженерія.

Офіційний опонент:
професор кафедри управління інформаційною безпекою
навчально-наукового інституту цивільного захисту
Львівського державного університету
безпеки життєдіяльності
доктор технічних наук, професор Ростислав ТКАЧУК

Підпис д.т.н. Ростислава Ткачука
Засвідчую проректор університету з
навчальної роботи
доцент Олександр Придатко