РЕЦЕНЗІЯ

рецензента, кандидата технічних наук,
старшого наукового співробітника Ткачова Андрія Михайловича
на дисертаційну роботу **Дженюк Наталії Володимирівни**
“Моделі синтезу систем безпеки соціокіберфізичних систем”,
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека та захист інформації

Актуальність теми. У сучасному цифровому середовищі динамічний розвиток інформаційних технологій, глобалізація комунікаційних процесів, зростання обчислювальних потужностей та активне впровадження кіберфізичних і соціальних компонентів в єдині платформи призвели до формування нового класу об'єктів – соціокіберфізичних систем. Ці системи поєднують фізичні пристрої, програмні комплекси та соціальні взаємодії, утворюючи складне, адаптивне середовище, що функціонує на межі трьох вимірів: фізичного, інформаційного та соціального. Застосування соціокіберфізичних систем охоплює широке коло сфер – від оборонної галузі та розумних міст до охорони здоров`я, промисловості та безпілотних літальних апаратів, що підкреслює їх стратегічну важливість.

Разом із тим, поява таких систем супроводжується суттєвим ускладненням задач забезпечення їх безпеки. Інтеграція соціальних і технологічних факторів породжує нові типи гібридних загроз, у яких поєднуються класичні технічні атаки (наприклад, DDoS, проникнення через вразливості програмного забезпечення) з соціотехнологічними впливами (маніпуляції через соціальні мережі, фішинг, психологічний вплив тощо). Особливо вразливою складовою виявляються канали безпровідного зв`язку, що використовуються між компонентами соціокіберфізичних систем, зокрема безпілотні літальні апарати, які можуть бути об`єктами атак через перехоплення або підміну даних, втручання в сигнали навігації та командного управління.

Наявна наукова література і технічні підходи переважно орієнтовані на вирішення ізольованих аспектів безпеки (наприклад, криптографічний захист чи контроль доступу), але здебільшого ігнорують необхідність інтегральної системи, яка б об'єднувала технологічні, організаційні та соціальні механізми протидії. Крім того, стрімкий розвиток методів атак – зокрема із застосуванням машинного навчання, штучного інтелекту та потенційного впровадження квантових обчислень – знижує ефективність традиційних методів захисту, які не враховують високий рівень адаптивності та непередбачуваності загрозового середовища.

У такому контексті постає суперечність: з одного боку, існує гостра потреба в науково обґрунтованих, ефективних і практично реалізованих моделях захисту інформації в соціокіберфізичних системах, що враховують мультидисциплінарну природу цих систем; з іншого боку, наявні теоретичні підходи не забезпечують цілісного уявлення про моделі захищеності в умовах гібридних загроз. Саме тому розробка багатоконтурної системи безпеки, яка враховує впливи на фізичному, кібернетичному та соціальному рівнях, є вкрай актуальним завданням.

Таким чином, тема дисертаційної роботи Дженюк Наталії Володимирівни "Моделі синтезу систем безпеки соціокіберфізичних систем", є актуальною як з наукової, так і з прикладної точки зору, оскільки відповідає сучасним викликам в галузі кібербезпеки, орієнтована на розв'язання комплексної міждисциплінарної задачі та має високий потенціал для практичного впровадження в системах управління, моніторингу та захисту інформації в умовах розвитку соціокіберфізичних платформ.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи відповідає пріоритетним напрямам розвитку науки і техніки в Україні з розділу «Інформаційні та комунікаційні технології». Отримані результати дисертаційної роботи є частинами наукових досліджень кафедри кібербезпеки НТУ "Харківський політехнічний інститут" у межах ініціативної науково-дослідної роботи "Моделювання соціо-кіберфізичних систем" (ДР № 0123U101018, 2023) та науково-дослідних робіт НТУ "ХПІ":

"Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі" (ДР №0123U101020, 2023-2025рр.) та "Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кібер-просторі" (ДР№ 0123U101018, 2023-2025рр.).

Наукова новизна одержаних результатів. У дисертаційній роботі Дженюк Н.В. отримано такі науково обґрунтовані результати:

– запропоновано математичну модель функціонування системи безпеки соціокіберфізичних систем в умовах загроз з ознаками гібридності та синергізму, яка встановлює залежність між структурою соціокіберфізичної системи та стратегією поведінки зовнішнього середовища;

– розроблено математичну модель безпеки інформаційних взаємодій у соціокіберфізичних системах на основі комплексного аналізу поведінки користувачів та інформаційних потоків, в якому враховується взаємодія соціальних, кібернетичних та фізичних компонентів системи;

– розроблено метод проектування безперервного функціонування системи безпеки соціокіберфізичних систем, який забезпечує формалізований підхід до опису ризиків та загроз для інформаційних активів;

– удосконалено класифікатор загроз безпеці інформаційних ресурсів соціокіберфізичних систем на основі комплексного підходу, який поєднує аналіз мережевих вразливостей, соціальної інженерії та кіберфізичних атак;

– набула подальшого розвитку концепція багатоконтурної безпеки соціокіберфізичних систем, в якій враховуються загрози внутрішнього та зовнішнього контурів за кожною з платформ (соціальні мережі, кіберпростір, кіберфізичні системи) з урахуванням форми власності елементів і технологій соціокіберфізичних систем.

Вважаю, що робота дисертантки є внеском у розробку математичних моделей та методів захищеності інформації соціокіберфізичних систем.

Практична цінність одержаних результатів та рекомендації щодо їх подальшого використання. Одержані результати мають важливе значення для

подальшого розвитку теорії захисту інформації в соціокіберфізичних системах. Запропоновані математичні моделі формалізують взаємодію загроз, систем захисту та поведінкових характеристик користувачів у динамічному середовищі. Вперше реалізовано підхід до побудови багатоконтурної архітектури безпеки, що враховує як технічні, так і соціальні чинники. Розроблені методи дозволяють здійснювати адаптивне управління ресурсами безпеки на основі оцінки ризиків у реальному часі.

Практична реалізація модулів системи підтверджує їх ефективність у виявленні та нейтралізації складних гібридних атак. Результати можуть бути використані для підвищення рівня кіберзахисту в системах моніторингу, управління безпілотними літальними апаратами, інтелектуальних мережах та інших критичних інфраструктурах. Запропоновані рішення також придатні для впровадження у прикладне програмне забезпечення систем інформаційної безпеки. Таким чином, робота має як теоретичну новизну, так і високу прикладну цінність для галузі кібербезпеки.

Результати дослідження були впроваджені в навчальний процес НТУ "ХПІ" (м. Харків) при викладанні дисциплін "Безпека хмарних технологій", "Безпека серверних систем" та "Мережева та хмарна безпека" для вітчизняних студентів за спеціальністю 125 Кібербезпека та захист інформації, у діяльності товариства з обмеженою відповідальністю "Мікрокрипт Текнолоджіс" та у товаристві з обмеженою відповідальністю "Сайфер ІТ" для багаторівневого аналізу ризиків та балансування конфіденційності, цілісності та доступності інформації.

Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором. Основні положення та результати дисертаційного дослідження пройшли апробацію та були опубліковані у наукових журналах України, що входять до переліку фахових видань, а також у науково-технічних журналах, індексованих у міжнародних наукометричних базах, що відповідає встановленим вимогам для дисертаційних робіт на здобуття наукового ступеня доктора філософії.

За результатами дослідження дисертаційної роботи опубліковано 17 наукових праць, серед яких: 4 статті – у наукових фахових виданнях України категорії "Б", 3 статті – у наукових фахових виданнях, що входять до наукометричної бази Scopus, 8 публікацій у збірниках матеріалів та тез конференцій, з яких 2 включено до наукометричної бази Scopus, 1 патент України на корисну модель, 1 монографія (видання, що включено до наукометричної бази Scopus). Участь здобувачки у роботах, що опубліковані у співавторстві, зазначена у дисертаційній роботі. Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кібербезпеки.

Аналіз змісту дисертації. Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі. Дисертаційна робота Дженюк Наталії Володимирівни є завершеною науковою роботою, містить анотацію – українською та англійською мовами, вступ, чотири розділи, висновки, список використаних джерел і додатки.

Дисертація присвячена підвищенню рівня захищеності інформаційних ресурсів соціокіберфізичних систем шляхом розробки та впровадження моделей та методів захищеності інформації соціокіберфізичних систем на основі побудови багатоконтурної системи захисту інформації.

Об'єктом дослідження є процес забезпечення захисту інформації у соціокіберфізичних системах на основі моделі багатоконтурної системи захисту інформації.

У *першому розділі* дисертаційної роботи проведено комплексний аналіз сучасного стану захищеності соціокіберфізичних систем. Виокремлено основні загрози та вразливості, що виникають у результаті взаємодії фізичних, кібернетичних та соціальних компонентів, із особливою увагою до безпровідних каналів зв'язку. Розглянуто принципи побудови систем безпеки, проаналізовано існуючі моделі захисту та обґрунтовано підходи до підвищення ефективності

функціонування таких систем, що дозволило сформулювати наукову проблему дослідження.

У *другому розділі* здійснено удосконалення класифікатора загроз для соціокіберфізичних систем шляхом інтеграції мережевих, соціальних та кіберфізичних чинників. Проведено детальний аналіз відомих підходів до оцінювання безпеки з урахуванням багатоаспектності архітектури захисту. На основі проведеного аналізу обґрунтовано вибір найбільш доцільних підходів до побудови моделей багаторівневого захисту соціокіберфізичних систем.

У *третьому розділі* розроблено математичну модель функціонування системи безпеки соціокіберфізичних систем в умовах дестабілізуючих впливів. Побудовано модель організації захисту інформаційних взаємодій, яка враховує як технічні, так і соціальні аспекти, а також адаптивні стратегії реагування. Запропоновано метод проектування безперервного функціонування системи безпеки, що об'єднує оцінку ризиків, виявлення аномалій і координацію соціальних факторів.

Четвертий розділ присвячено верифікації запропонованих моделей за допомогою моделювання та порівняльного аналізу. Показано ефективність реалізації багатоконтурної системи захисту під впливом гібридних атак, з урахуванням різних стратегій атакуючих. Здійснено оцінку результатів функціонування системи в умовах загроз і підтверджено підвищення її стійкості, що свідчить про практичну доцільність застосування розроблених рішень.

Висновки, сформульовані у роботі, висвітлюють результати дослідження як вирішення висунутих в дисертації завдань. Висновки відповідають вимогам, які висуваються до результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії.

Список використаних джерел широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості джерел, пов'язаних з захистом інформації та інтелектуальними методами оцінки ефективності.

Додатки містять інформацію про практичне впровадження результатів дисертації, фрагменти кодів програм та список публікацій здобувачки.

Достовірність отриманих результатів та висновків.

Ґрунтовний аналіз дисертаційної роботи свідчить, що її наукові положення, висновки та рекомендації є достатньо обґрунтованими, повними та аргументованими. Авторка провела як теоретичні, так і емпіричні дослідження, використовуючи актуальні вітчизняні та міжнародні джерела. Достовірність висновків підтверджується застосуванням класичних і сучасних методів досліджень, логічним аналізом літератури, а також коректним формулюванням актуальних завдань.

Результати досліджень доповідалися на міжнародних науково-технічних конференціях і публікувалися у фахових виданнях. Узгодженість отриманих результатів, їх відповідність літературним даним і успішне впровадження підтверджують їх достовірність. У межах дисертаційного дослідження авторка повністю реалізувала поставлену мету і завдання, а логічні висновки до кожного пункту роботи дозволяють чітко зрозуміти основні етапи дослідження та практичну цінність отриманих результатів. Достовірність висновків підкріплюється комплексним підходом до вивчення визначеного об'єкта. Вищевикладене свідчить про обґрунтованість та достовірність наукових положень, висновків і рекомендацій, що викладено у дисертаційній роботі Дженюк Наталії Володимирівни.

Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях. Дисертація виконана з дотриманням вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи.

Основні ідеї авторки та результати дослідження викладено у семи статтях, а також дисертантка активно приймала участь в українських та закордонних конференціях, де була проведена апробація ідей, що викладено у дисертаційному дослідженні.

Недоліки та зауваження до дисертаційної роботи.

В процесі ознайомлення з роботою позитивне враження справило докладне обгрунтовування усіх висунутих у роботі положень, використання сучасних математичних методів.

Але при цьому виникли такі зауваження.

1. В дисертаційній роботі наведено методи захисту від атак на соціокіберфізичні системи (стор. 27, рис. 1.5), але не зрозуміло, які саме принципи управління безпекою в соціокіберфізичних системах вони забезпечують.

2. З рис. 1.8 дисертаційної роботи (стор. 30) не зрозуміло, які спеціальні механізми безпеки використовуються для забезпечення захисту від вразливостей у соціокіберфізичних системах.

3. В дисертаційній роботі (стор. 48) наведено, що найефективніший кіберзахист досягається через багаторівневий підхід, який поєднує базові заходи спеціальних механізмів безпеки, але не зрозуміло в чому полягає багаторівневість цього підходу.

4. На рис. 2.1 дисертаційної роботи наведена класифікація загроз на канали передавання інформації в соціокіберфізичних системах, але не зрозуміло, яким чином ці загрози розподіляються за основними складовими безпеки: кібербезпека, безпека інформації та інформаційна безпека.

5. В дисертаційній роботі формула 3.17 (стор. 96) визначає відносний виграш кількості захисних елементів від зовнішніх цільових атак, але не зрозуміло яким чином це забезпечує у 1,5 рази збільшення ресурсів, які здатні забезпечити превентивний захист від цільових атак.

6. На рис. 4.2 дисертаційної роботи (стор. 121) наведена залежність необхідного атакуючого ресурсу для знищення системи в цілому, але не зрозуміло, яким чином визначені ці показники та який результат вони забезпечують.

Проте наведені у результаті аналізу роботи зауваження не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також

наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як напрямки подальших досліджень.

Висновки. Дисертаційна робота Дженюк Наталії Володимирівни є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тема дослідження відповідає галузі знань 12 – "Інформаційні технології" та спеціальності 125 – "Кібербезпека та захист інформації".

За змістом, актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота "Моделі синтезу систем безпеки соціокіберфізичних систем" відповідає вимогам п.п. 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" від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426) та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а її авторка, Дженюк Наталія Володимирівна, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – "Кібербезпека та захист інформації".

Рецензент – доцент кафедри кібербезпеки
Національного технічного університету
"Харківський політехнічний інститут"
кандидат технічних наук,
старший науковий співробітник Андрій ТКАЧОВ

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"29" 07 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *