# РЕЦЕНЗІЯ

**рецензента, доктора філософії, доцента,**
**завідувача кафедри програмної інженерії та інтелектуальних**
**технологій управління Коппа 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

Детальний аналіз дисертаційної роботи Дженюк Н.В. на тему “Моделі синтезу систем безпеки соціокіберфізичних систем”, що представлена для захисту на здобуття наукового ступеня доктора філософії у Національному технічному університеті «Харківський політехнічний інститут», дає змогу зробити комплексний висновок щодо її актуальності, ступеня обґрунтованості наукових положень, висновків, рекомендацій, достовірності та значущості отриманих результатів, наукової новизни, теоретичної та практичної цінності, надати загальну оцінку дисертації.

## 1. Ступінь актуальності теми дисертаційної роботи

Стрімкий розвиток інформаційних технологій, зокрема інтеграція соціальних платформ, безпілотних літальних апаратів, сенсорних мереж та хмарних технологій, призвів до формування нового класу систем – соціокіберфізичних систем. Вони забезпечують критичні процеси в обороні, транспорті, телекомунікаціях та енергетиці. Проте зростання складності архітектури таких систем і збільшення обсягів оброблюваних даних створює нові вектори атак, зокрема гібридного типу, які поєднують технічні, соціальні та інформаційно-психологічні методи впливу. Актуальність теми дисертаційної роботи зумовлена саме потребою у комплексному, багаторівневому захисті таких складних структур.

Більшість існуючих підходів до захисту соціокіберфізичних систем орієнтовані на ізольовані аспекти – кіберкомпонент або фізичний рівень, тоді як

взаємодія між ними, а також з соціальними чинниками, залишається поза увагою. Це призводить до відсутності цілісної стратегії безпеки, яка б забезпечувала адаптивність, стійкість та безперервність функціонування системи навіть у складному загрозовому середовищі. Тема дослідження є надзвичайно актуальною у зв'язку з тим, що соціокіберфізичні системи активно використовуються в оборонно-промисловому комплексі, зокрема для управління безпілотними літальними апаратами, які можуть бути уразливими через відкриті канали зв'язку та обмеження обчислювальних ресурсів.

Для реалізації поставленої мети в дисертації застосовано широкий спектр методів: ймовірнісний аналіз, оптимізаційне моделювання, агентне моделювання, методи виявлення аномалій, а також адаптивні механізми управління ризиками. Особливу увагу приділено формуванню багатоконтурної системи захисту, яка враховує як технічні, так і соціальні аспекти загроз. Таким чином, дисертаційна робота Дженюк Наталії Володимирівни "Моделі синтезу систем безпеки соціокіберфізичних систем", спрямована на вирішення важливої науково-практичної проблеми захисту інформаційних ресурсів у новому класі складних інформаційних систем.

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

Дисертаційне дослідження здійснювалося в межах наукової спеціальності 125 – Кібербезпека та захист інформації та виконувалося на базі кафедри кібербезпеки НТУ "ХПІ".

Результати, отримані в процесі виконання роботи, інтегровані в наукові дослідження, що здійснюються на кафедрі кібербезпеки НТУ "Харківський політехнічний інститут". Зокрема, положення дисертації є складовими ініціативної НДР "Моделювання соціо-кіберфізичних систем" (ДР № 0123U101018, 2023). Крім того, дослідження пов'язані з виконанням проєктів "Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі" (ДР № 0123U101020, 2023–2025 рр.) та "Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки

та підвищення рівня її ефективності у кіберпросторі” (ДР № 0123U101018, 2023–2025 рр.).

**3. Наукова новизна одержаних результатів.**

Наукова новизна здобутих результатів полягає у теоретичному узагальненні та запропонуванні нового підходу до вирішення актуального наукового завдання – підвищенні рівня захищеності інформаційних ресурсів соціокіберфізичних систем в умовах дії складних і комбінованих загроз.

Основою дослідження є новітній підхід до побудови захисних механізмів, який поєднує фізичні, цифрові та соціальні складові в єдину багаторівневу систему. У межах дисертаційного дослідження отримані такі основні науково обґрунтовані результати:

1. Вперше розроблено математичну модель функціонування системи безпеки соціокіберфізичних систем, яка враховує специфіку загроз з ознаками гібридності та синергії. Модель встановлює зв’язок між архітектурою соціокіберфізичної системи та поведінковими характеристиками зовнішнього середовища, що реалізує змішані типи атак.

2. Розроблено математичну модель безпеки інформаційної взаємодії в соціокіберфізичних системах, засновану на інтеграції поведінкового аналізу користувачів і динаміки інформаційних потоків. За допомогою моделі можна локалізувати критичні вузли інфраструктури, які є найбільш уразливими до деструктивного впливу.

3. Розроблено метод проектування безперервного функціонування системи безпеки соціокіберфізичних систем, який дозволяє оптимізувати процес управління безпекою соціокіберфізичних систем на основі математично обґрунтованих критеріїв ефективності та комплексної інтеграції елементів методу, що забезпечує підвищення рівня стійкості системи захисту.

4. Удосконалено класифікатор загроз безпеці інформаційних ресурсів соціокіберфізичних систем, який базується на інтегральному аналізі мережевих вразливостей, методів соціальної інженерії та кіберфізичних впливів. Запропонована класифікація враховує критичність загроз, їх відповідність конкретним компонентам безпеки та послугам захисту.

5. Набула подальшого розвитку концепція багатоконтурного захисту соціокіберфізичних систем, що передбачає урахування загроз як із зовнішнього, так і з внутрішнього середовищ для кожної з платформ: соціальних, кібернетичних та кіберфізичних. Модель доповнено урахуванням форми власності компонентів системи та використовуваних технологій.

**4. Наукова та практична цінність одержаних результатів.**

Робота має логічно вибудувану структуру, в якій чітко простежується послідовність постановки дослідницьких завдань і шляхів їх реалізації. Результати дослідження підтверджені достатньо обґрунтованими доказами, а обрана математична база відповідає сучасним підходам у сфері кібербезпеки. Запропоновані підходи до оцінки рівня захищеності соціокіберфізичних систем порівнювались з відомими методами, продемонстрували аргументовану ефективність на тлі актуальних наукових джерел.

Усі сформульовані в дисертаційній роботі висновки й практичні рекомендації логічно узгоджені з метою дослідження та його актуальністю. Вони можуть бути використані для практичної реалізації в системах оцінювання кіберзахисту.

Отримані в дисертаційному дослідженні результати становлять вагомий внесок у розвиток теоретичних основ захисту інформації в контексті функціонування соціокіберфізичних систем. Запропоновані математичні моделі дозволяють формалізувати процеси взаємодії між загрозами, системами безпеки та поведінковими реакціями користувачів у змінному середовищі. Уперше запропоновано підхід до побудови багаторівневої архітектури захисту, яка комплексно враховує як технічні характеристики, так і соціальні аспекти потенційних впливів. Розроблені методики забезпечують можливість адаптивного управління засобами безпеки з урахуванням поточного рівня ризиків у режимі реального часу. Отримані результати можуть бути успішно застосовані для підвищення кіберстійкості систем спостереження, керування безпілотними платформами, інтелектуальних мереж і критичних інформаційних об’єктів. Розроблені рішення також мають потенціал інтеграції в практичне програмне забезпечення для забезпечення інформаційної безпеки. Таким чином,

дисертація поєднує в собі глибоку теоретичну складову та високу прикладну значущість у сфері кібербезпеки.

Результати дослідження були впроваджені у товаристві з обмеженою відповідальністю “Сайфер ІТ” для багаторівневого аналізу ризиків та балансування конфіденційності, цілісності та доступності інформації, у діяльності товариства з обмеженою відповідальністю “Мікрокрипт Технолоджіс” та 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.

**5. Повнота викладення наукових і прикладних результатів дисертації в опублікованих працях та академічна доброчесність.**

Результати дослідження представлено у 17 наукових публікаціях, 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.

Дисертація виконана з дотриманням вимог 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. Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кібербезпеки.

**6. Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі.**

Детальний аналіз дисертаційної роботи свідчить про те, що наукові положення, висновки та рекомендації, представлені в дослідженні, є достатньо обґрунтованими, повними та всебічно аргументованими. Для їх формулювання

та підтвердження авторка провела як теоретичні, так і емпіричні дослідження, включаючи експериментальні перевірки, використовуючи як вітчизняні, так і міжнародні спеціалізовані та актуальні джерела.

Достовірність отриманих результатів забезпечується застосуванням як класичних, так і сучасних методів дослідження, серед яких глибокий аналіз літературних джерел, чітка постановка актуальних завдань та їх коректне вирішення. Результати теоретичних і експериментальних досліджень були представлені на міжнародних науково-технічних конференціях та опубліковані у фахових наукових виданнях. Крім того, їх надійність підтверджується взаємоузгодженістю, відповідністю існуючим літературним даним і позитивними результатами практичного впровадження.

У ході дослідження авторка повністю реалізувала поставлену мету та завдання, визначені на початковому етапі роботи. До кожного розділу подано логічні висновки, що дозволяють чітко зрозуміти сутність дослідження та практичну значущість отриманих результатів. Достовірність висновків також підтверджується комплексним підходом до аналізу досліджуваного об’єкта.

Таким чином, наведені факти свідчать про належний рівень обґрунтованості та достовірності наукових положень, висновків і рекомендацій, викладених у дисертаційній роботі Дженюк Наталії Володимирівни.

**7. Оцінка змісту дисертації, її завершеності й оформлення.**

Побудова дисертації відповідає прийнятим для наукового дослідження нормам. Усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана грамотною науковою мовою та оформлена відповідно до існуючих нормативних документів.

Дисертаційна робота Дженюк Наталії Володимирівни має чітку структуру, що включає вступ, чотири розділи, висновки, список використаних джерел і додатки.

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

У *вступі* обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача.

У *першому розділі* дисертаційної роботи здійснено всебічний аналіз поточного стану захищеності соціокіберфізичних систем. Визначено ключові загрози та вразливі місця, що виникають унаслідок взаємодії фізичних, кібернетичних і соціальних елементів, з акцентом на ризики, пов'язані з бездротовими каналами зв'язку. Детально розглянуто принципи організації захисту, критично проаналізовано наявні моделі безпеки та визначено шляхи підвищення ефективності їх функціонування, що дозволило чітко сформулювати наукову проблему дослідження.

*Другий розділ* присвячено вдосконаленню класифікації загроз для соціокіберфізичних систем шляхом урахування сукупного впливу мережевих, соціальних та кіберфізичних складових. Проведено порівняльний аналіз сучасних підходів до оцінювання рівня безпеки в умовах складної, багатокомпонентної архітектури. На основі отриманих результатів здійснено обґрунтований вибір концепцій для побудови моделей багаторівневого захисту соціокіберфізичних систем.

У *третьому розділі* сформульовано математичну модель функціонування захисної системи соціокіберфізичних систем за умов дестабілізаційних чинників і впливів. Розроблено модель організації інформаційної безпеки, яка інтегрує технічні параметри, соціальні впливи та адаптивні механізми реагування. Запропоновано методологію забезпечення безперервності функціонування системи, що поєднує аналіз ризиків, виявлення аномальних подій і врахування соціально-контекстуальних факторів.

У *четвертому розділі* здійснено перевірку ефективності запропонованих моделей на основі математичного та імітаційного моделювання. Представлено результати аналізу роботи багатоконтурної архітектури захисту в умовах реалізації гібридних атак з різними сценаріями поведінки порушника. Проведено оцінювання ефективності системи в умовах ризику, що дозволило підтвердити

зростання її стійкості та практичну придатність запропонованих рішень для реального застосування.

*Висновки* підсумовують досягнення дослідження, підтверджуючи виконання поставлених завдань і відповідність вимогам для здобуття науковго ступеня.

Список літератури охоплює широкий спектр джерел, включаючи іноземні, а додатки містять інформацію про практичне впровадження результатів, розширений перелік завдань і публікації авторки.

**8. Зауваження до дисертаційної роботи**

1. З дисертаційної роботи (рис. 1.4) не зрозуміло в чому полягає комплексний підхід до безпеки і які рівні (платформи) соціокіберфізичних систем потрібно включити.

2. В дисертаційній роботі в табл. 1.4 (стор. 39) наведено моделі синтезу систем безпеки, але не зрозуміло яким чином вони забезпечують комплексний підхід до формування систем захисту соціокіберфізичних систем.

3. На стор. 53 дисертаційної роботи наведена загальна формула оцінки загроз внутрішнього контуру з урахуванням методів соціальної інженерії, але не зрозуміло, яким чином враховуються ознаки гібридності та синергізму загроз.

4. В дисертаційній роботі (стор. 92) наведено математичний апарат, який забезпечує визначення стратегії поведінки зовнішнього середовища із структурою системи безпеки, але не зрозуміло яким чином враховується багатоконтурність запропонованої системи безпеки соціокіберфізичних систем.

5. На рис. 4.1 дисертаційної роботи (стор. 119) наведено процес руйнування соціокіберфізичної системи під впливом руйнівних елементів, але не зрозуміло, що саме мається на увазі під робочими елементами і яким чином вони впливають на захищеність соціокіберфізичної системи.

Проте наведені у результаті аналізу роботи зауваження не носять принципового характеру та жодним чином не знижують позитивне враження від роботи та її наукову та практичну цінність.

**9. Відповідність дисертації встановленим вимогам і загальні 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", із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 426 від 08.04.2025, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, 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 – Завідувач кафедри програмної
інженерії та інтелектуальних технологій
управління
Національного технічного університету
«Харківський політехнічний інститут»,
доктор філософії, доцент Андрій КОПП

Підпис Андрій Копп
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"10" 02 2026 р.

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