ВІДГУК

офіційного опонента доктора технічних наук, професора,
завідувача кафедри кібербезпеки та програмного забезпечення,
Центральноукраїнського національного технічного університету,
Смірнова Олексія Анатолійовича
на дисертаційну роботу Дженюк Наталії Володимирівни
"Моделі синтезу систем безпеки соціокіберфізичних систем",
поданої на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека та захист інформації

1. Актуальність теми дисертації

У сучасному цифровому середовищі соціокіберфізичні системи набувають все більшого значення, поєднуючи в собі фізичні пристрої, кібернетичні компоненти та соціальні взаємодії. Їх використання охоплює безпілотні літальні апарати, інтелектуальні мережі, системи моніторингу та критичну інфраструктуру. Проте стрімкий розвиток таких систем супроводжується появою складних загроз, які поєднують технічні атаки, методи соціальної інженерії та інформаційно-психологічні впливи.

Існуючі підходи до захисту не охоплюють комплексної природи соціокіберфізичних систем, що потребує створення адаптивних, багатоконтурних моделей безпеки. Зростання кількості атак через вразливі канали зв'язку, недостатній захист інформаційних потоків та відсутність координації між рівнями безпеки вимагають системного вирішення.

Дисертаційна робота Дженюк Н.В. "Моделі синтезу систем безпеки соціокіберфізичних систем" присвячена підвищенню рівня захищеності інформаційних ресурсів соціокіберфізичних систем шляхом розробки та впровадження моделей та методів захищеності інформації таких систем на основі побудови багатоконтурної системи захисту інформації. Актуальність роботи

зумовлена необхідністю забезпечення стійкості систем до гібридних атак та швидкої адаптації до змінних умов середовища загроз.

Тема роботи пов'язана з виконанням науково-дослідних робіт на кафедрі 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.).

2. Наукова новизна одержаних результатів.

В дисертаційній роботі *вперше* розроблено математичну модель функціонування системи безпеки соціокіберфізичних систем, яка враховує гібридний і синергетичний характер сучасних атак, а також взаємозв'язок між структурою системи та стратегією поведінки зовнішнього середовища. *Вперше* розроблено модель інформаційної взаємодії у соціокіберфізичних системах, яка поєднує соціальні, кібернетичні та фізичні компоненти, враховує поведінку користувачів та потоки даних. *Запропоновано* метод проєктування безперервного функціонування системи безпеки соціокіберфізичних систем, який базується на формалізованому описі ризиків, виявленні аномалій та автоматизованому реагуванні. *Удосконалено* класифікатор загроз безпеки інформаційних ресурсів соціокіберфізичних систем на основі комплексного підходу, що враховує мережеві вразливості, соціальну інженерію, типологію атак, рівень критичності активів та фінансові можливості порушника. *Набула подальшого розвитку* концепція багатоконтурної системи безпеки соціокіберфізичних систем, у якій враховано розподіленість компонентів, різну форму власності елементів,

багаторівневу структуру ризиків і взаємодію між платформами (соціальні мережі, кіберпростір, кіберфізичні пристрої).

3. Практичне значення отриманих результатів полягає у можливості ефективного проєктування систем безпеки соціокіберфізичних систем, які здатні протистояти сучасним гібридним загрозам. Запропонована модель функціонування дозволяє підвищити стійкість соціокіберфізичних систем шляхом оптимізації співвідношення між захисними та функціональними компонентами, що дозволяє більш ніж у 1,5 рази збільшити ресурс, необхідний для їх руйнування. Запропонована модель інформаційної взаємодії демонструє, що асинхронна взаємодія агентів з упередженням забезпечує швидше (на 15–20%) формування кластерів інформаційного впливу, ніж синхронна. Дослідження також показали, що за високих значень волатильності агентів (μ=0.9) процес збіжності інформаційного впливу відбувається значно швидше.

Запропонований метод проєктування безперервного функціонування системи безпеки дає змогу виявляти загрози в реальному часі. Найвищу точність (до 99%) демонструють методи контролю промислових систем, а методи розпізнавання голосових маніпуляцій і шифрувальників показали точність 97–98%. Водночас аналіз мережевих загроз, таких як фішинг, DNS-атаки та перехоплення трафіку, забезпечує точність на рівні 90–93%, що підтверджує потребу в подальшому вдосконаленні методів аналізу мережевого середовища.

Удосконалений класифікатор загроз дозволяє оперативно проводити онлайн-оцінку загроз, враховуючи соціальні, кібернетичні та фізичні чинники. Це забезпечує можливість своєчасного виявлення критичних вузлів інфраструктури та формування інтегральної оцінки рівня захищеності системи в умовах динамічного середовища. Застосування класифікатора до систем з використанням безпілотних літальних апаратів дозволяє ефективно виявляти загрози, що надходять через канали управління, та запобігати витоку, підміні або втраті критичних даних.

Теоретичні та практичні результати роботи впроваджено в освітній процес Національного технічного університета "Харківський політехнічний інститут" 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 модулі анти-фрод підсистеми захисту Інтернет-банкінгу "ELPay" товариства з обмеженою відповідальністю "Сайфер ІТ" та у діяльності товариства з обмеженою відповідальністю "Мікрокрипт Текнолоджіс" по підвищенню стійкості до гібридних загроз, оптимізації витрат на інформаційну безпеку та підвищенню загального рівня готовності до інцидентів у цифровому середовищі в режимі реального часу.

Мова та стиль викладення дисертації дозволяє зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація відповідає вимогам, які висуваються до її оформлення, відповідно до "Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)", що затверджений постановою Кабінету Міністрів України від 12.01.2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426), й "Вимог до оформлення дисертації", затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. У цілому зміст дисертації викладено послідовно та логічно.

4. Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у роботі.

Положення та висновки, наведені в дисертаційній роботі Дженюк Наталії Володимирівни, в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні математичного апарату ймовірнісного аналізу для оцінки ймовірності руйнування робочих і захисних елементів системи під дією зовнішнього середовища, методів оптимізації для визначення

найкращого співвідношення робочих і захисних елементів у соціокіберфізичних систем для збільшення стійкості до атак, аналізу ризиків та управління загрозами для оцінки вразливостей безпровідного зв'язку та розробки моделей безпеки соціокіберфізичних систем, агентного моделювання для представлення взаємодії агентів та їх поведінки в соціокіберфізичних системах, методів кореляційного аналізу для встановлення взаємозв'язків між параметрами системи та їх впливом на безпеку.

У дослідженні застосовано математичний апарат і засоби сучасного комп'ютерного моделювання. Отримані результати було верифіковано за допомогою практичних експериментів, що підтверджує достовірність сформульованих у дисертаційній роботі наукових положень, висновків та рекомендацій.

5. Повнота оприлюднення результатів дисертаційної роботи

Результати досліджень опубліковані у 17 наукових роботах, 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.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426).

6. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота Дженюк Наталії Володимирівни складається з анотації двома мовами, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи викладено на 192 сторінках, серед них: 36 рисунків по тексту, 2 рисунки на 2 окремих сторінках, 11 таблиць по тексту, 6 додатків.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-технічні 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 досліджено існуючі загрози та вразливості соціокіберфізичних систем, зокрема в точках перетину фізичних, соціальних і кіберкомпонентів. Розглянуто проблеми захисту безпровідних каналів зв'язку, вплив соціальної інженерії та криптографічні обмеження. Запропоновано підхід до комплексного аналізу стану безпеки соціокіберфізичних систем як основи для подальшого моделювання.

Розділ другий присвячено класифікації загроз, які поєднують мережеві, соціальні та кіберфізичні атаки. Досліджено сучасні підходи до оцінювання рівня безпеки та обґрунтовано доцільність використання багатоконтурної архітектури. Визначено критерії вибору ефективних моделей безпеки з урахуванням ризиків, динаміки середовища та типів загроз.

У третьому розділі дисертації створено математичні моделі функціонування системи безпеки соціокіберфізичних систем з урахуванням зовнішніх завад і загроз. Представлено метод проєктування безперервної роботи захисної системи з інтеграцією моніторингу, виявлення аномалій та соціальних

факторів. Розроблено узагальнене математичне представлення багаторівневої структури безпеки.

Четвертий розділ містить перевірку достовірності розроблених моделей на основі симуляцій і порівняльного аналізу сценаріїв атак. Досліджено вплив атакуючих елементів на робочі й захисні компоненти системи та обчислено ефективність запропонованих стратегій. Проведено оцінку рівня захищеності соціокіберфізичних систем за допомогою інтегрального показника безпеки.

Висновки до розділів та за результатами роботи сформульовані чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел із 154 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

Загальні висновки дисертаційної роботи узгоджуються з метою і завданнями дослідження. Отримані результати характеризуються науковою новизною та практичною цінністю, обґрунтовані теоретично та підтверджені експериментальними дослідженнями.

В цілому, дисертація Дженюк Н.В. є завершеним і повним дослідженням, яке містить теоретичні розробки та відповідні їм експериментальні перевірки.

7. Зауваження по дисертаційній роботі

1. З дисертаційної роботи (п. 1.2.3, стор. 31) не зрозуміло, яким чином якість обслуговування в системі безпілотних літальних апаратів підвищується за рахунок розгортання декількох безпілотних літальних апаратів і яка енергоємність при цьому потрібна.

2. В другому розділі дисертаційної роботи наведені ключові етапи атак на канали передавання інформації в соціокіберфізичних системах (рис. 2.2), але при цьому не наведено, яким чином методи соціальної інженерії впливають на сучасні змішані або цільові атаки.

3. В дисертаційній роботі (стор. 51, формула 2.2) наведений математичний апарат побудови багатоконтурної системи захисту інформації в соціокіберфізичних системах, але не зрозуміло яким чином в наведеному математичному апараті враховуються синергія та гібридність сучасних загроз.

4. В третьому розділі дисертаційної роботи (п. 3.1) наведено розробку моделі функціонування системи безпеки мережі соціокіберфізичних систем в умовах завад, але при цьому не зрозуміло, яким чином безпілотні літальні апарати розглядаються як соціокіберфізична система, а також не зрозуміло чому вибрані саме такі вхідні дані (стор. 91), які забезпечують формування моделі руйнування робочих елементів системи при мінімальному витрачанні свого ресурсу.

5. В дисертаційній роботі (стор. 97) наведено аналіз процесів впливу у соціокіберфізичних системах, але з формули 3.18 не зрозуміло яким чином враховується соціальна складова соціокіберфізичних систем і яким чином визначені вагові коефіцієнти основних показників якості обслуговування.

6. В дисертаційній роботі (стор. 118) наведено математичний апарат оптимізації системи за допомогою мінімаксного рівняння, але не зрозуміло яким чином це впливає на загальній рівень захищеності елементів інфраструктури соціокіберфізичних систем.

Слід зазначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

8. Загальний висновок на дисертаційну роботу.

Дисертаційна робота Дженюк Наталії Володимирівни "Моделі синтезу систем безпеки соціокіберфізичних систем" за своїм змістом відповідає спеціальності 125 – Кібербезпека та захист інформації. Дисертація є завершеною кваліфікаційною науковою працею, має теоретичну та практичну цінність, в якій викладено авторський підхід до розробки нових та удосконалення існуючих моделей та методів захищеності інформації соціокіберфізичних систем. Він дозволяє створювати багатоконтурні системи захисту інформації, які враховують

комплексний характер сучасних загроз у соціально-керованих кіберфізичних середовищах.

Дисертаційна робота Дженюк Наталії Володимирівни відповідає вимогам 6, 7, 8, 9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії" від 12.01.2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426) та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40.

Використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувачки в науку.

Дисертаційна робота Дженюк Наталії Володимирівни є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, що дозволяють підвищити рівень захищеності інформаційних ресурсів соціокіберфізичних систем, а здобувачка Дженюк Наталія Володимирівна заслуговує присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
" 28 " липня 2025 року