ВІДГУК

офіційного опонента докторки технічних наук, професорки,
завідувачки кафедри інформаційних технологій,
Одеського національного університету імені І. І. Мечнікова,
Казакової Надії Феліксівни
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

Інтенсивний розвиток цифрових технологій та зростання взаємозалежності фізичних, кібернетичних і соціальних компонентів зумовили формування соціокіберфізичних систем як нового типу складних адаптивних структур. Такі системи широко застосовуються в управлінні безпілотними літальними апаратами, функціонуванні інтелектуальних сенсорних мереж, моніторингових платформах та елементах критичної інфраструктури. Водночас із їх розширенням загострюється проблема безпеки, оскільки сучасні загрози поєднують кібернетичні методи з соціально-психологічними впливами, спрямованими на маніпуляцію користувачами та втручання у фізичні процеси.

Традиційні підходи до захисту виявляються недостатньо ефективними, оскільки не враховують міждисциплінарну природу соціокіберфізичних систем та взаємодію різнотипних чинників у режимі реального часу. Зростає потреба в адаптивних системах захисту, що базуються на багатоконтурних архітектурах та здатні забезпечити стійкість навіть за умов порушень каналів зв’язку, фрагментації інформаційних потоків та слабкої взаємодії між підсистемами. Саме ці виклики стали підґрунтям для розробки нових моделей, які системно поєднують соціальні, кібернетичні й фізичні аспекти безпеки.

Дисертаційна робота Дженюк Н.В. “Моделі синтезу систем безпеки соціокіберфізичних систем” присвячена розробці математичних моделей та методів захищеності інформації соціокіберфізичних систем на основі побудови багатоконтурної системи захисту інформації, спрямованої на підвищення рівня захищеності інформаційних ресурсів. У зв’язку з необхідністю забезпечення стабільного функціонування складних інформаційних структур навіть за умов гібридних атак тема роботи є актуальною.

Дисертація органічно пов’язана з тематикою наукових досліджень, що виконуються на кафедрі кібербезпеки НТУ “Харківський політехнічний інститут”. Зокрема, робота проводилася в рамках ініціативної НДР “Моделювання соціокіберфізичних систем” (ДР № 0123U101018, 2023), а також у межах проєктів “Розробка симетричної криптосистеми на основі згорткової штучної нейронної мережі” (ДР № 0123U101020, 2023–2025) та “Розробка моделей соціокіберфізичних систем для підвищення ефективності захисту у кіберпросторі” (ДР № 0123U101018, 2023–2025). Результати дисертаційного дослідження стали невід’ємною частиною зазначених тем і демонструють комплексний підхід до забезпечення кібербезпеки в умовах зростаючої складності загроз.

2. Наукова новизна одержаних результатів.

У дисертаційній роботі *вперше* запропоновано математичну модель функціонування системи безпеки соціокіберфізичних систем з урахуванням гібридних та синергетичних загроз. Модель дозволяє вибирати оптимальні параметри конфігурації системи та сценарії реагування, які мінімізують ризик вторгнення й гарантують стабільність роботи навіть при складних загрозах. *Вперше* було сформовано модель інформаційної взаємодії в соціокіберфізичних системах, яка інтегрує соціальні, цифрові та фізичні складові, а також враховує особливості поведінки користувачів і передавання інформаційних потоків. *Розроблено* новий підхід до проєктування безперервної роботи системи безпеки

соціокіберфізичних систем, що ґрунтується на формалізованому представленні ризиків, механізмах виявлення аномальних дій та реалізації автоматизованих заходів реагування. *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). *Удосконалено* класифікатор загроз, що об'єднує характеристики кіберфізичних, соціоінженерних і мережевих атак із урахуванням їх критичності, цільової спрямованості, регуляторних вимог та ресурсних можливостей зловмисника. Це дозволяє комплексно оцінювати ризики й розробляти адаптивні стратегії захисту інформаційних ресурсів соціокіберфізичних систем. Проведено комплексну верифікацію моделей, зокрема на основі симуляційних експериментів, що охоплюють різні сценарії атак та параметри загроз.

3. Практичне значення отриманих результатів полягає у створенні ефективної моделі функціонування системи безпеки соціокіберфізичних систем, яка враховує взаємозв'язок структури системи із поведінкою зовнішнього середовища, що дозволяє встановити оптимальні параметри системи. Це дає змогу підвищити ресурс зовнішнього впливу, необхідного для руйнування системи, більш ніж у 1,5 рази.

Модель інформаційних взаємодій у соціокіберфізичних системах виявила, що асинхронна взаємодія прискорює утворення стійких інформаційних кластерів на 15–20% у порівнянні з синхронною. Найшвидша збіжність відбувається за волатильності агентів $\mu=0.9$, тоді як при $\mu=0.1$ процес уповільнюється.

Реалізований метод проектування безперервного функціонування системи безпеки дає змогу виявляти загрози в реальному часі та знижувати ризики. DDoS-атаки, SQL-ін'єкції, фішинг і ботнети виявляються за 1.2–1.4 сек., а аномалії у промислових системах – за 2.0–2.3 сек. Методи контролю промислових систем досягли точності 99%, а розпізнавання голосових маніпуляцій і шифрувальників

– 97–98%. Виявлення фішингу, DNS-атак та перехоплення трафіку забезпечує точність 90–93%, що вказує на необхідність подальшого вдосконалення.

Удосконалений класифікатор загроз забезпечує оперативну оцінку безпеки з урахуванням соціальних, кібернетичних та фізичних чинників. Це дозволяє визначати критичні вузли, формувати інтегральну оцінку захищеності системи та своєчасно виявляти загрози в середовищах із використанням безпілотних літальних апаратів.

Теоретичні та практичні результати роботи впроваджено у модулі анти-фрод підсистеми захисту Інтернет-банкінгу “ELPay” товариства з обмеженою відповідальністю “Сайфер ІТ”, у діяльності товариства з обмеженою відповідальністю “Мікрокрипт Текнолоджіс” по підвищенню загального рівня готовності до інцидентів у цифровому середовищі в режимі реального часу та в освітній процес кафедри кібербезпеки НТУ “Харківський політехнічний інститут” при викладанні дисциплін “Безпека хмарних технологій”, “Безпека серверних систем” та “Мережева та хмарна безпека”.

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 січня 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.

Наукові положення, висновки та рекомендації, викладені в дисертації Дженюк Наталії Володимирівни, мають належне теоретичне та технічне

обґрунтування. Достовірність отриманих результатів забезпечена використанням комплексу математичних методів, серед яких: ймовірнісний аналіз – для оцінювання ризику втрати функціональності робочих та захисних компонентів під впливом зовнішніх загроз; методи оптимізації – для визначення раціонального балансу між структурними елементами системи з метою підвищення її стійкості; аналіз ризиків та керування загрозами – для побудови моделей захисту безпровідних каналів у соціокіберфізичних системах; агентне моделювання – як засіб формалізації поведінки учасників соціальних процесів у системі; кореляційний аналіз – для виявлення взаємозв'язків між параметрами системи, що впливають на її безпеку.

У процесі дослідження застосовувалися сучасні математичні засоби моделювання та спеціалізовані комп'ютерні інструменти. Результати були перевірені шляхом імітаційного моделювання та верифіковані на основі практичних сценаріїв атак і захисту. Це підтверджує логічну узгодженість та обґрунтованість сформульованих наукових положень і рекомендацій, а також їх прикладну цінність для розробки комплексних систем кібербезпеки соціокіберфізичних систем.

5. Повнота оприлюднення результатів дисертаційної роботи

Результати досліджень опубліковані у 17 наукових роботах, серед яких: 3 статті – у наукових фахових виданнях, що входять до наукометричної бази Scopus, 4 статті – у наукових фахових виданнях України категорії "Б", 8 публікацій у збірниках матеріалів та тез конференцій, з яких 2 включено до наукометричної бази Scopus, 1 монографія (видання, що включено до наукометричної бази Scopus), 1 патент України на корисну модель. Роль здобувачки у колективних публікаціях чітко відображена в дисертаційній роботі.

Усі опубліковані матеріали повністю корелюють із змістом дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії,

затвердженого постановою КМУ від 12.01.2022 № 44 (зі змінами від 08 квітня 2025 року № 426).

Усі результати, які винесено авторкою на захист, отримані самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

6. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота Дженюк Наталії Володимирівни складається зі вступу, чотирох розділів, висновків, списку використаних джерел, 6 додатків.

У вступі дисертаційної роботи обґрунтовано актуальність теми, що пов’язана з необхідністю забезпечення безпеки соціокіберфізичних систем в умовах зростання гібридних загроз. Сформульовано мету дослідження та визначено наукові й прикладні завдання, які спрямовані на розробку комплексної системи захисту з урахуванням фізичних, кібернетичних і соціальних аспектів. Описано зв’язок дослідження з науковими програмами, висвітлено новизну та практичне значення результатів, а також подано інформацію про особистий внесок здобувачки, апробацію результатів і публікаційну активність.

Перший розділ присвячено аналізу поточного стану захищеності соціокіберфізичних систем. У ньому розглянуто основні загрози, що виникають через взаємодію різнорівневих компонентів – від бездротових каналів зв’язку до соціальних платформ. Детально проаналізовано типові вразливості, вплив соціальної інженерії та проблеми впровадження криптографічного захисту в умовах обмежених ресурсів.

У другому розділі досліджено складну природу атак, що спрямовані на інформаційні, фізичні та соціальні рівні соціокіберфізичних систем. Запропоновано класифікацію загроз, засновану на інтегрованому підході до аналізу уразливостей. Доведено, що багаторівнева архітектура безпеки підвищує стійкість систем до динамічних загроз.

У третьому розділі розроблено математичні моделі систем захисту, що поєднують методи оцінки ризиків, виявлення аномалій і реагування на інциденти. Запропоновано оптимізаційні рішення для управління безпекою в умовах змінного середовища загроз.

Четвертий розділ містить верифікацію моделей, моделювання сценаріїв атак і оцінку ефективності запропонованих стратегій. Підтверджено доцільність використання багатоконтурної системи захисту в умовах складних гібридних впливів.

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. В дисертаційній роботі (підрозділ 1.4) не зрозуміло, яким чином ресурси соціальних мереж та месенджерів впливають на рівень захищеності елементів інфраструктури соціокіберфізичних систем.

2. З табл. 2.1 дисертаційної роботи не зрозуміло, яким чином рівень вразливості та складність застосування механізмів кіберзахисту впливає на складність побудови адаптивних механізмів захисту.

3. З дисертаційної роботи (стор. 53, формула 2.7) не зрозуміло, яким чином вибрані вагові коефіцієнти можливостей реалізації загроз на основі методів соціальної інженерії.

4. На рис. 3.1 наведена структурна схема концепції багатоконтурної безпеки соціокіберфізичних систем (стор. 89), але не зрозуміло, з яких етапів вона складається.

5. В дисертаційній роботі формула 4.1 (стор. 117) забезпечує загальне рівняння витрат зовнішнього ресурсу, але не зрозуміло, яким чином ця формула забезпечує можливість отримання кількісних витрат по кожній платформі соціокіберфізичних систем.

6. В дисертаційній роботі у табл. 4.1 наведений необхідний атакуючий ресурс, але не зрозуміло, яким чином враховується в кількісних показниках комплексування цільових атак з методами соціальної інженерії.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

8. Загальний висновок на дисертаційну роботу.

На основі критичного вивчення дисертації та праць здобувачки, які опубліковані за темою дисертації, об’єктивно встановлено:

– 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 сформувати багатоконтурні системи інформаційного захисту із врахуванням складних природних сучасних загроз у соціально-керованих кіберфізичних середовищах.

– авторка дисертації роботи Дженюк Наталія Володимирівна заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент
Завідувачка кафедри інформаційних технологій,
Одеський національний університет імені І. І. Мечнікова,
докторка технічних наук, професорка Надія КАЗАКОВА

04.08.2025

Особистий підпис
КАЗАКОВОЇ Надії
ЗАСВ[illegible]
Ст. інспектор відділу к[illegible]
[illegible] Г.В. Любарська

ВІДДІЛ КАДРІВ