Голові спеціалізованої вченої ради
Д 26.861.06 Державного
університету інформаційно-
комунікаційних технологій

вул. Солом'янська, 7, м. Київ

ВІДГУК
офіційного опонента

завідувачки кафедри інформаційних технологій Одеського національного університету ім. І. І. Мечнікова, д.т.н., професорки Казакової Надії Феліксовни на дисертаційну роботу Погасія Сергія Сергійовича на тему «Моделі і методи захисту інформації в кіберфізичних системах», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

1. Актуальність теми дисертації, зв'язок з науковими програмами, планами, темами.

Розвиток кібернетичних технологій, мобільних каналів, Інтернет-речей та смарт-технологій сформували кіберфізичні системи, які практично поєднуються з об'єктами критичної інфраструктури, та формують національну безпеку держави. Стрімке зростання обчислювальних можливостей не тільки значно поширюють спектр цифрових послуг, збільшують швидкість та об'єми передачі даних, а також формують низку проблем серед яких забезпечення безпеки є найголовнішою. В умовах зростання обчислювальних та фінансових можливостей кіберзлочинців та кібертерористів формуються цільові (змішані) атаки з ознаками синергізму та гібридності, що потребує негайного підвищення рівня захищеності структури кіберфізичних систем, а також висуває більш жорсткі вимоги до систем захисту інформації в умовах появи повномасштабного квантового комп'ютера (постквантового періоду). В таких умовах розв'язання проблеми щодо розробки методології підвищення ефективності захисту інформаційних ресурсів у кіберфізичних системах є своєчасним та актуальним.

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

Тематика дисертаційної роботи та отримані результати безпосередньо відповідають пріоритетності розвитку інформаційних та комунікаційних технологій в Україні. Згідно із Законом України «Про пріоритетні напрями розвитку науки і техніки» № 2623–III від 11.07.2001; зі змінами, внесеними згідно із Законом України «Про інформацію» №2658–XII від 02.10.1992; Законом України «Про доступ до публічної інформації» № 2939–VI від 13.01.2011; Законом України «Про захист даних» № 4452–VI від 23.02.2012.

Ця робота є частиною досліджень в рамках у госпрозрахункової науково-дослідної роботи «Моделі і методи захисту інформації в кіберфізичних системах» (Державний реєстраційний номер 0121U114233, ХНЕУ, м. Харків), яку виконував Харківський національний економічний університет імені Семена Кузнеця у 2020 р., частиною досліджень науково-дослідницької роботи «Геоінформаційні і інтелектуальні технології підтримки прийняття рішень в задачах оцінки та прогнозування екологічної безпеки територій» (Державний реєстраційний номер 0119U03671, ОДЕКУ м. Одеса), яку виконував Одеський Державний екологічний університет у 2023-2024 рр., частиною досліджень науково-дослідницької роботи «Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі» (Державний реєстраційний номер 0123U101020, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет «Харківський політехнічний інститут» 2023-2025рр., частиною досліджень науково-дослідницької роботи «Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кібер-просторі» (Державний реєстраційний номер 0123U101018, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет «Харківський політехнічний інститут» 2023–2025рр.

3. Наукова новизна одержаних результатів

Вперше розроблені концепція побудови багатоконтурної системи захисту кіберфізичних систем, математична модель безпеки кіберфізичних систем, метод забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів кіберфізичних систем на гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах, методологія побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка за рахунок

використання концепції побудови багатоконтурної системи безпеки, методу забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів, методу забезпечення закриття каналу мобільного Інтернету і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дозволяє відкрити новий емерджентний підхід побудови наявних і перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

Удосконалено класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем.

Набув подальшого розвитку метод забезпечення закриття голосового каналу мобільного Інтернету.

4. Практичне значення одержаних результатів.

Запропоновано методику застосування класифікатора загроз безпеки інформаційних ресурсів (електронний доступ: http://skl.khpi.edu.ua), програмно-апаратний комплекс на основі мікроконтролерів, якій забезпечує автономне управління елементами кіберфізичної системи, закриття каналів зв'язку (як дротових, так й бездротових на основі крипто-кодових конструкціях Нідеррайтера на LDPC-кодах). Розроблений практичний протокол LoRa, якій забезпечує циркуляцію інформації в кіберфізичних системах із забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу та дозволяє аналізувати ефективність функціонування системи захисту кіберфізичних систем.

Результати досліджень прийняті до впровадження в Державному підприємстві «Науково-технічний комплекс «Імпульс»(акт від 07.12.2021р.), в ТОВ «Мікрокрипт Текнолоджіс» (акт від 07.12.2023р.), в ТОВ «Сайфер ІТ» (акт від 10.01.24. в навчальному процесі кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут» при викладанні дисципліни «Основи побудови та захисту мікропроцесорних систем», «Інтернет речей та сервісів» для студентів спеціальності 125 «Кібербезпека» денної форми навчання (акт від 16.09.2022 р.).

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація та автореферат у цілому відповідають вимогам, які висуваються до його оформлення відповідно до «Порядку присудження наукових ступенів» затвердженого Постановою Кабінету Міністрів України

№ 1197 від 17 листопада 2021 р. та не відхиляються від вимог ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення» й «Вимог до оформлення дисертації» затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. У цілому зміст дисертації та автореферату викладено послідовно та логічно.

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

Дисертація присвячена вирішенню об'єктивного протиріччя з одного боку відсутності нових теоретичних підходів до забезпечення захисту інформаційних ресурсів у кіберфізичних системах в умовах появи повномасштабного квантового комп'ютеру, з іншого – відсутністю цілісної науково обґрунтованої методології побудови системи безпеки інформаційних ресурсів у кіберфізичних системах з багатоконтурною інфраструктурою.

Розв'язання даного сперечання дозволяє підвищити рівень захищеності інформаційних ресурсів у кіберфізичних системах.

Обґрунтованість одержаних положень та результатів, отриманих здобувачем, обумовлюється застосуванням відомих методів теорії множин і теорії ймовірностей, теорії скінченних полів Галуа та теорії кодування, системного підходу та теорії складних систем із застосуванням математичних моделей і методів дискретної математики.

Вірогідність одержаних у роботі результатів підтверджується ретельною перевіркою результатів, а також збіжністю результатів моделювання з теоретично отриманими результатами.

6. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Погасія С.С. достатньо повно викладені в 44 наукові праці, із них 27 наукових статей у фахових виданнях. Одна монографія та вісім статей опубліковані в науковому виданні, що входить до науково-метричної бази Scopus. Також 17 праць опубліковано в матеріалах наукових конференцій, з них вісім, що входять до науково-метричної бази Scopus.

Назва дисертації відповідає її змісту. Дисертація та автореферат оформлені згідно з вимогами МОН України. Науковий рівень дисертації відповідає вимогам «Порядку присудження наукових ступенів» затвердженого Постановою Кабінету Міністрів України від від 17 листопада 2021 р. № 1197, а зміст – паспорту спеціальності 05.13.21 – системи захисту інформації.

Загальна характеристика структури та змісту дисертаційної роботи.

Структура та обсяг дисертації відповідають вимогам паспорту спеціальності 05.13.21 «Системи захисту інформації», та складається зі вступу, 5 розділів, висновків, списку використаних джерел. Повний обсяг дисертації 330 сторінок, з них 261 сторінок основного тексту, у дисертації використано 255 джерел.

У **вступі** автором обґрунтовано актуальність теми дисертації, сформульовано науково-прикладну проблему. Визначені мета, об'єкт, предмет, часткові завдання дослідження, наукова новизна результатів дослідження, практичне значення результатів, а також зв'язок з науковими програмами, планами, темами досліджень Національного технічного університету «Харківський політехнічний інститут».

У **першому розділі** здобувачем здійснено аналіз існуючих методів захисту інформації на основі глибокого аналізу наукової літератури за темою дисертаційної роботи. Розглянуто можливі цільові атаки з ознаками синергізму та гібридності на структуру, та інформаційні ресурси кіберфізичних систем. Сформована постановка проблеми дослідження.

Другий розділ присвячений розробці моделей захисту інформації в кіберфізичних системах на основі моделі Лотки-Вольтерри.

Оцінка рівня загроз неможлива без оцінки можливостей самих нападників (зловмисників, кіберзлочинців тощо). Від їх «компетентності», обчислювальних ресурсів, часових характеристик, їх вмотивованості багато в чому залежить можливість реалізації загрози. При цьому запропонований удосконалений класифікатор загроз, який ураховує не тільки ознаки гібридності та синергізму можливих цільових атак, а також надає оцінку їх впливу на зовнішній та внутрішній контури системи захисту. Запропоновані моделі систем безпеки на основі моделі Лотки-Вольтерри забезпечують об'єктивну оцінку еволюційного розвитку як сучасних технологій, так й можливі вектори «розвитку» цільових (змішаних) атак.

В **третьому розділі** дисертації розглядаються, запропоновані автором, методи забезпечення послуг безпеки на основі крипто-кодові конструкції Нідеррайтера різних типів та модифікацій. Для забезпечення послуг безпеки у кіберфізичних системах пропонується використовувати постквантові алгоритми – крипто-кодові конструкції Нідеррайтера на основі LDPC-кодів із заподіянням збитку на основі запропонованих моделей побудови постквантових алгоритмів

забезпечення послуг безпеки. Приведені доказові результати дослідження стійкості та властивостей запропонованих криптосистем на основі крипто-кодові конструкції Нідеррайтера.

В **четвертому розділі** запропоновані комплексний показник оцінювання функціональної ефективності передачі інформації кіберфізичних систем, математична модель та методика захисту технологій IoT з низьким споживанням енергії та високим покриттям є однією з ключових тенденцій у сфері IoT, які також є основою сучасних кіберфізичних систем з одного боку, з іншого – критичною точкою будь-якої інфраструктури кіберфізичних систем. Запропонована концепція побудови багатоконтурної системи захисту базується на збалансованому співвідношенні системи захисту інформації при передачі кіберпростором і системи безпеки інформації у цілому.

В **п'ятому розділі** наведені результати практичної реалізації серверного програмно-апаратного комплексу в кіберфізичних системах та аналіз ефективності функціонування системи захисту CPS. Крім того, у розділі розроблено рекомендацій щодо застосування отриманих наукових положень і результатів. На основі методів і моделей побудови багатоконтурних систем безпеки, а також механізмів забезпечення основних послуг безпеки на основі постквантових алгоритмів –крипто-кодових конструкцій Нідеррайтера на LDPC-кодах запропонована нова методологія побудови системи безпеки інформаційних ресурсів на основі методів і моделей побудови багатоконтурних систем безпеки, яка забезпечує визначений рівень безпеки у постквантовий період.

8. Ідентичність змісту автореферату та основних положень дисертації

Зміст автореферату є ідентичним до дисертаційної роботи та не містить інформації, яка відсутня у самій роботі. Текст автореферату повною мірою розкриває наукову та практичну цінність дисертації. Висновки в авторефераті збігаються з висновками по роботі.

Загальні висновки дисертаційної роботи узгоджуються з метою і завданнями дослідження. За результатами дисертаційного дослідження зроблено шістнадцять висновків, які повністю відповідають поставленим завданням. Отримані результати характеризуються науковою новизною та практичною цінністю, обґрунтовані теоретично та підтверджені експериментальними дослідженнями. В цілому дисертація Погасія Сергія

Сергійовича є завершеним і повним дослідженням, яке містить теоретичні розробки високого рівня та відповідні їм експериментальні перевірки.

9. Зауваження до дисертаційної роботи.

1. Під час обґрунтування науково-прикладної проблеми щодо розробки моделей та методів захисту інформації в кіберфізичних системах, автору необхідно було більш чітко описати протиріччя, які виникають при захисті інформації в кіберфізичних системах, особливо на об'єктах критичної інфраструктури та можливостями наукових методів й моделей, що реалізовані в існуючих системах захисту інформації, наприклад стандарт KNX. На мою думку, в розділі 5 доцільно було б сформувати порівняльну таблицю з існуючими та запропонованими методами і методиками, які використовуються в системах захисту інформації кіберфізичних систем.

2. В дисертаційній роботі автор розв'язує науково-прикладну проблему щодо розробки методологічних основ захисту інформації в кіберфізичних системах, але не враховує особливості наявних класів вузькоспеціалізованих засобів захисту мобільних мереж та можливості перехоплення інформації в мережах на основі смарт- та мобільних (бездротових) технологій за допомогою комплексів радіомоніторингу та скануючих приймачів.

3. В дисертаційної роботі розглядається удосконалений класифікатор, але в авторефераті математичного опису його не наведено, тому не зовсім зрозуміло, що саме покращено/удосконалено та за рахунок чого.

4. В дисертаційної роботі п. 2.4 досліджується «небезпечність» зловмисника, але не зрозуміло яким чином це впливає при побудові математичних моделей захисту на основі моделі Лотки-Вольтери. На мій погляд, це необхідно враховувати під час формування вагових коефіцієнтів «хіжаків» (зловмисників), а також їх фінансових та обчислювальних можливостей.

5. З тексту дисертації залишається відкритим питання щодо практичної можливості реалізації запропонованих протоколів на основі протоколу Lora (яка архітектура, вхідні параметри процесорів необхідні) при їх використані у смарт-технологіях кіберфізичних систем.

6. В дисертаційної роботі запропонована нова методологія побудови системи захисту інформації в кіберфізичних системах на основі багатоконтурності, але не зрозуміло, яким чином та за рахунок чого комплексний показник ефективності збільшується на 10 % (автореферат рис.

12, 13 й табл. 2), та яким чином це впливає на підвищення рівня захищеності, особливо у постквантовий період.

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

10. Загальний висновок на дисертаційну роботу.

За обсягом проведених досліджень, їх теоретичним рівнем, актуальністю розглянутої проблеми та значенням одержаних результатів для науки та практики дисертаційна робота Погасія Сергія Сергійовича «Моделі і методи захисту інформації в кіберфізичних системах» є завершеною науковою працею, в якій виконано теоретичне узагальнення і запропоновано нове вирішення актуальної науково-прикладної проблеми, що полягає у розробки моделей і методів захисту інформації в кіберфізичних системах, яка є внеском у теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації, зокрема інформації, що зберігається, оброблюється й передається в комп'ютерних системах і мережах та в математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів.

Матеріали дисертації опубліковано достатньою мірою, висновки роботи відображають її результати.

Автореферат достатньою мірою відповідає змісту дисертаційної роботи, оформлення дисертації та автореферату в цілому відповідає нормативним вимогам. Дисертаційна робота повністю відповідає паспорту спеціальності 05.13.21 – системи захисту інформації та вимогам, які висуваються до дисертацій на здобуття наукового ступеня доктора наук, а також пп. 7, 9 «Порядку присудження наукових ступенів» від 17.11.21 р., а її автор, Погасій Сергій Сергійович, заслуговує присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Офіційний опонент
Завідувачка кафедри інформаційних технологій
Одеського національного університету
ім. І. І. Мечнікова, д.т.н., проф. Надія КАЗАКОВА

Особистий підпис Н. Казакової
ЗАСВІДЧУЮ
ДИРЕКТОР ВІДДІЛУ КАДРІВ

Підпис громад. Надії Казакової
посада Зав. кафедри
ЗАВІРЯЮ:
Проректор ОНУ імені І. І. Мечникова
Запорожченко О. В.