Голові спеціалізованої вченої ради
Д 26.861.06 Державного університету
інформаційно-комунікаційних
технологій
вул. Солом'янська, 7, м. Київ

**ВІДГУК**
**офіційного опонента**

професора кафедри засобів захисту інформації ДНП «ДУ Київський авіаційний інститут» доктора технічних наук, професора Хорошка Володимира Олексійовича, 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»

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

Інформація стає більш важливим ресурсом, ніж матеріальні або енергетичні ресурси. Аналіз функціонування програмних засобів та систем захисту інформації, показав, що проблема побудови системи захисту інформації в кіберфізичних системах, є дуже широкою та багатогранною. Нарівні з підвищенням показників надійності систем захисту інформації, забезпеченням виявлення впливів, розпізнавання загроз системи захисту інформації побудова методологічних основ захисту інформації в кіберфізичних системах є необхідним і першочерговим завданням.

Тому здобувач запропонував розробити моделі захисту та удосконалити захисту інформації в кіберфізичних системах. Отже, розробка науково-методичного апарату захисту інформації в кіберфізичних системах є актуальною науковою проблемою, що має теоретичне і практичне значення.

Зважаючи на те, що тема дисертації «Моделі і методи захисту інформації в кіберфізичних системах» Погасія С.С. присвячена вирішенню важливої науково-прикладної проблеми, вважаю її актуальною.

Актуальність теми додатково підтверджується завданням оперативного реагування інформаційним загрозам, як передбачено Доктриною інформаційної безпеки України (затверджена Указом Президента України від 25 лютого 2017 року № 47/2017).

**Аналіз основного змісту, наукової новизни та практичного значення.**

Дисертація складається зі вступу, п'яти розділів, висновків, додатків та списку використаних джерел, Структура та обсяг дисертації. Дисертація складається зі вступу, 5 розділів, висновків, списку використаних джерел з 229 найменувань на 21 сторінці. Повний обсяг дисертації 301 сторінка, з них 275 сторінок основного тексту.

Зміст роботи відповідає сформульованій науково-прикладної проблемі та поставленим завданням, а їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 05.13.21 «Системи захисту інформації»

У *вступі* автором обгрунтовано актуальність теми дисертації, сформульовано науково–прикладну проблему, мету, об'єкт, предмет, завдання дослідження, наукову новизну одержаних результатів, практичне значення результатів, зв'язок роботи з науковими програмами, планами, темами досліджень Національного технічного університету «Харківський політехнічний інститут» та Державного університету інформаційно-комунікаційних технологій.

У *першому розділі* здобувачем здійснено аналіз існуючих методів захисту інформації. Проведено аналіз вітчизняної та зарубіжної наукової літератури за темою дисертаційної роботи. Розглянуто існуючі загрози інформаційних ресурсів у кіберфізичних системах. Проаналізовано сучасний стан проблеми захисту інформаційних ресурсів у кіберфізичних системах. Здійснено постановку проблеми дослідження.

Проведені дослідження показали відсутність цілісної концепції захисту інформації у CPS. Виходячи з чого пошук шляхів вирішення проблеми захисту CPS остається актуальною проблемою. Шляхом вирішення цей проблеми є шлях розробки нових концептуальних підходів та загальної концепції захисту інформації у CPS. Існуючі методики та моделі захисту не складають єдину концепцію комплексного забезпечення захисту інформації, яка б поєднувала теоретичні методи, методики, моделі та технологічні підходи до захисту інформації у соціальних мережах.

Виходячи з проведеного аналізу, виникає науково-прикладна проблема щодо розробки методології підвищення рівня захищеності інформаційних ресурсів у кіберфізичних системах. Тому потрібно розробити методологію захисту інформації у кіберфізичних системах.

Таким чином, при розробці нових або модернізації існуючих методів та методик захисту інформації потрібно застосовувати комплексний підхід до розробки алгоритму захисту інформації.

Проведені дослідження ґрунтуються на теоретично обґрунтованих та практично апробованих методах теорії множин (формалізовано загрози безпеки інформаційних ресурсів, здійснено їх класифікацію, визначено вимоги і повноту забезпечення безпеки інформаційних ресурсів), теорії криптографії, теорії кодування та теорії скінченних полів Галуа (використано при розробці гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах та обґрунтуванні їх стійкості), теорії ймовірностей і математичної статистики (використано для дослідження властивостей гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування класифікатора загроз), математичної логіки і теорії автоматів (для оцінювання енергетичних затрат при практичній реалізації гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах, побудові серверної частини програмно-апаратного комплексу), системного аналізу (для ієрархічного подання кіберфізичних систем), законах синергії (для побудови моделі загроз, дослідження її впливу на систему безпеки інформаційних ресурсів).

Доведено, що після рішення завдань розробки та удосконалення моделей та методик захисту інформації буде розроблено методологічні основи захисту захисту інформації в кіберфізичних системах.

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

Оцінка рівня загроз неможлива без оцінки можливостей самих нападників (зловмисників, кіберзлочинців тощо). Від їхньої "компетентності", обчислювальних ресурсів, часових характеристик, їхньої вмотивованості багато в чому залежить можливість реалізації загрози. Таким чином, невід'ємною частиною аналізу загроз є розробка моделі "небезпеки" порушника. Такий підхід дає змогу сформувати безліч загроз залежно від можливостей нападників, сформувати безліч можливих впливів, оцінити стан превентивних засобів захисту. Для формування вагових коефіцієнтів "небезпеки" порушників пропонується використовувати таку класифікацію порушників.

Доведено, що однією з особливостей CPS є відсутність забезпечення захисту інформації в елементах інфраструктури, передача сигналів від датчиків/сенсорів відкритими каналами, і забезпечення управління та адміністрування на основі хмарних технологій. Це істотно знижує можливості формування контуру безпеки, і

призводить до збільшення критичних точок для реалізації кібератак. За таких умов оцінювання безпеки необхідно проводити в офлайн-режимі, що дає змогу враховувати динаміку, як кіберзагроз, з одного боку, так і можливість засобів захисту протистояти їм. Аналіз результатів моделювання дає змогу зробити доволі загальний висновок, що в умовах обмежених фінансових коштів, які спрямовуються на розробку та впровадження нових засобів, що забезпечують послуги безпеки, їхній розподіл має здійснюватися таким чином. Визначається той із коефіцієнтів, зміна якого призводить до більш істотних змін з точки зору рівня безпеки. З'ясовується найбільш значущий фактор, який призводить до змін розглянутого коефіцієнта. Визначаються заходи, що призводять до подібних змін. У роботі наведено порівняльні результати аналізу практичного використання методу оцінювання стану безпеки CPS на основі моделі Лотки-Вольтерри:

У *третьому розділі* навеена розробка підходу до забезпечення захисту каналу зв'язку на основі постквантових алгоритмів

Створення сучасних синтезованих мереж ґрунтується на гібридізації технологій бездротових мобільних та SCPS на основі IoT. Доведено, що основою забезпечення основних послуг безпеки: конфіденційності, цілісності та автентичності даних є закриття каналів зв'язку CCIS/ CPSS (SCADA) програмними (програмно-апаратними) застосунками на основі постквантових криптосистем – ССС Мак-Еліса та Нідеррайтера з урахуванням ступені конфіденційності (секретності) інформації та/або інформаційних потоків. Крім забезпечення послуг безпеки на основі ССС Мак-Еліса та Нідеррайтера забезпечується необхідний рівень оперативності (швидкість крипто-перетворень в ССС порівнянна з перетворенням сучасних симетричних алгоритмів шифрування), вірогідності за рахунок використання методів завадостійкого кодування. Такий підхід дозволить враховувати можливість масштабування та створення об'єднаних з хмарними технологіями мереж. За рахунок використання концепції двоконтурної системи безпеки, формується об'єктивна оцінка потокового стану CCIS / CPSS (SCADA). Головною частиною запропонованих механізмів послуг безпеки є сервер генерації ключових послідовностей, в якому формуються OTP-ключі для використання в програмних та/або програмно-апаратних застосунках CCIS / CPSS (SCADA). З метою забезпечення необхідного рівня безпеки для передачі ключових послідовностей (OTP-ключів) використовується ССС Нідеррайтера, в програмних та або програмно-апаратних застосунках CCIS / CPSS (SCADA) пропонується використовувати ССС Мак-Еліса. Такий підхід дозволить значно підвищити рівень безпеки в mesh-мережах на основі смарт-технологій та мобільних безпровідних Інтернет-каналів.

*Четвертий розділ* присвячено розробці математичної моделі та методики захисту. Розвиток технологій IoT з низьким споживанням енергії та високим покриттям є однією з ключових тенденцій у сфері IoT. Ця область технологій продовжує еволюціонувати і розвиватися, і наступні напрямки її розвитку особливо актуальні. Розроблена концепція захисту CPS яка позбавлена недоліків існуючих систем, та перевершує їх за наступними параметрами:

- швидкості виявлення радіосигналів атак, це робиться за рахунок проведення декілька сканувань радіодіапазону за один і той же час;
- чутливості, вимірювання проводиться двома різними за принципом дії пристроями;
- завадостійкістю, тому що апаратним та програмним способом прибираються шуми та завади радіодіапазону;
- здатністю розпізнавати випадкові радіосигнали, які можуть бути радіосигналами атак на систему, за рахунок використання нового принципу розпізнавання радіосигналів;

- здатністю створення захищених каналів або передачі захищеної інформації при передачі інформаційних та керуючих сигналів від виконуючих пристроїв до сервера сховища та обробки інформації.

Здатністю створення захищених каналів або передачі захищеної інформації при передачі інформаційних та керуючих сигналів від виконуючих пристроїв до сервера сховища та обробки інформації, це основний напрямок концепції. Тому що гарантований механізм передачі керуючій інформації дозволяє надійно працювати CPS. Розроблена концепція процесу захисту CPS, практично, за усіма параметрами суттєво опереджає існуючі системи захисту інформації. Запропонована концепція побудована на збалансованому співвідношенні системи захисту інформації при передачі кіберпростором та системи безпеки інформації у цілому.

*П'ятий розділ* присвячений оцінці та визначенню ефективності захисту даних з урахуванням одночасно дії багатьох параметрів мережі. Крім того, в розділі розроблено рекомендацій щодо застосування отриманих наукових положень та результатів. Визначено переваги розробленої методології та проведено оцінку достовірності запропонованих наукових результатів.

**Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації.** Обґрунтованість одержаних положень та результатів, отриманих здобувачем, обумовлюється застосуванням відомих методів дослідження на основі системного підходу та теорії складних систем із застосуванням математичних моделей і методів дискретної математики. Теоретичні основи будуються з використанням теорії випадкових графів, теорії ймовірностей, аналітичного моделювання та дискретної оптимізації. Методи теорії ймовірності використані для розробки методів аналізу ймовірності виявлення і достовірності розпізнавання атак на кіберфізичні системи.

**Достовірність одержаних у роботі результатів** підтверджується ретельною перевіркою результатів експериментальних досліджень з використанням математичного моделювання та збіжністю результатів моделювання з теоретично отриманими результатами.

До **основних наукових результатів,** які отримані в дисертаційної роботі, можна віднести:

1. Вперше розроблено концепцію побудови багатоконтурної системи захисту кіберфізичних систем, яка за рахунок інтеграції: методу забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів програмно-апаратного комплексу; методу забезпечення закриття каналу мобільного «Інтернету» і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дає можливість створити ефективні системи захисту інформації в кіберфізичних системах та відкрити новий напрямок у побудові системи захисту інформаційних ресурсів внутрішнього та зовнішнього контуру безпеки фізичної платформи та платформи управління кіберфізичних систем.

2. Вперше розроблено математичну модель безпеки кіберфізичних систем, яка на підставі розробленої концепції за рахунок врахування вагового коефіцієнту, що відображає можливості порушника, час та ймовірності реалізації загрози, дозволяє своєчасно визначити спрямованість загроз, врахувати обчислювальні ресурси нападників.

3. Вперше розроблено метод забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів кіберфізичних систем в якому за рахунок використання гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах, дозволяє зменшити складність формування (лінійного перетворення) та розкодування у криптограмі, забезпечити достовірність OTP-паролів в протоколі автентифікації в умовах дії гібридних загроз.

4. Набув подальшого розвитку метод забезпечення закриття голосового каналу мобільного «Інтернету», в якому за рахунок використання алгоритмів постквантової криптографії у крипто-кодових конструкціях Нідеррайтера на еліптичних кодах підвищується стійкість протоколів послуг безпеки у структурі технологій LTE та забезпечується високий рівень захищеності голосового каналу мобільного зв'язку.

5. Удосконалено класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем, який за рахунок врахування рівня критичності загроз, відношення загрози до складової безпеки, послуги безпеки, впливу загрози відповідно до регуляторів та оцінки фінансових можливостей порушника дозволяє оцінювати гібридність загроз та відкриває новий підхід побудови діючих та перспективних систем захисту інформаційних ресурсів кіберфізичних систем.

6. Вперше розроблено методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка за рахунок використання концепції побудови багатоконтурної системи безпеки, методу забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів, методу забезпечення закриття каналу мобільного «Інтернету» і каналу циркуляцію інформації та математичної моделі з урахуванням класифікатора загроз дозволяє відкрити новий емерджентний підхід побудови діючих та перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

**Теоретична і наукова цінність та практичне значення одержаних автором наукових результатів.**

Наукова цінність основних положень дисертації полягає у розробці концепції, моделей і методів безпеки кіберфізичних систем та методології створення системи безпеки кіберфізичних систем, в основу яких покладено концепцію побудови багатоконтурної системи безпеки, які базуються на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах.

Практична цінність роботи полягає в тому, що:

1. Запропоновано методика застосування класифікатора загроз безпеки інформаційних ресурсів (електронний доступ: http://skl.khpi.edu.ua), яка дозволяє в он-лайн режимі здійснювати об'єктивну оцінку загроз, визначення критичних точок інфраструктури кіберфізичних систем, можливості превентивних заходів, та формувати оцінку потокового стану захищеності.

2. Запропоновано програмно-апаратний комплекс на основі мікроконтролерів, який забезпечує автономне управління елементами кіберфізичної системи, закриття каналів зв'язку (як дротових, так й бездротових на основі крипто-кодових конструкціях Нідеррайтера на LDPC-кодах).

3. Розроблений практичний протокол LoRa, якій забезпечує циркуляцію інформації у кіберфізичних системах з забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу та дозволяє аналізувати ефективність функціонування системи захисту кіберфізичних систем.

4. Впровадження розроблених методів забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів кіберфізичних систем на гібридних крипто-кодових конструкціях Нідеррайтера забезпечує зменшення складності формування (лінійного перетворення) та розкодування у криптограмі.

**Оцінка мови та стилю викладення дисертації та автореферату.**

Дисертація і автореферат написані грамотно. Стиль викладення матеріалів дослідження, а саме наукових положень, висновків і рекомендацій, відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора наук. Дисертація являє собою наукову працю, яка містить сукупність наукових положень та результатів, виставлених автором для публічного захисту, має внутрішню єдність та свідчить про особистий внесок автора у науку.

Оформлення дисертації та автореферату відповідає вимогам Державних стандартів України. Текст дисертації та автореферату написані правильною технічною мовою, ясно та зрозуміло.

Зміст автореферату повністю відображає основні результати досліджень, які подані в дисертації.

**Повнота викладення наукових результатів дисертації в опублікованих роботах.**

Основні результати дисертаційної роботи Погасія С.С. повністю викладені в 44 наукових працях, з них, 27 наукових статей, одна монографія, у тому числі, 8 статей у виданнях, яке індексується у науково-метричній базі Scopus, Також результати дисертаційних досліджень знайшли відображення в 17 матеріалах та тез доповідей опубліковано у матеріалах міжнародних і всеукраїнських наукових конференцій.

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації.

**Недоліки.**

1. З автореферату стр. 10 та дисертаційної роботи стр. 46, не зрозуміло яким чином кіберфізичні системи відрізняються від смарт систем.

2. З дисертаційної роботи стр. 95 та автореферату стр. 15 не зрозуміло, чому саме ці категорії зловмисників необхідно враховувати для побудови багатоконтурних систем захисту інформації.

3. З автореферату рис 3. та дисертаційної роботи п.2.2, не зрозуміло яким чином визначені рівні безпеки та показники α, β,γ в запропонованих моделях. Яким чином забезпечується підвищення рівня захищеності кіберфізичних систем з урахування моделей на основі моделі Лотки-Вольтерри.

4. З автореферату стр. 21-25 та дисертаційної роботи п.3.3, не зрозуміло, чому обрана конструкція Нідеррайтера, та яким чином необхідно визначити яку саме модель криптокодовоїї конструкції Нідеррайтера необхідно використовувати для забезпечення послуг безпеки в кіберфізичних системах.

5. З дисертаційної роботи п 4.3. та автореферату стр. 27.,чому вибраний протокол в якості дослідження протокол Lora, а не протокол KNX, який на сьогоднішній час використовується в кіберфізичних системах для забезпечення безпеки.

6. Було би за доцільно при верифікації методики виявлення радіосигналів небезпечних сигналів, якими можуть бути сигнали незаконного втручання у кіберфізичну систему навести приклади таких сигналів за спектром або за амплітудою. Це би покращило розуміння досягнених результатів.

7. При формуванні моделей превентивних заходів на основі моделі Лотки – Вольтерри на стр. 238 наведені коефіцієнти моделі які враховують синергізм і гібридність сучасних загроз. Ці коефіцієнти можуть змінюватися, але у роботі дисертант такий варіант не розглянув, що не у повної мірі надає відповідь для оцінки стійкості кібкерфізічної системи. Робота виглядала би більш переконливою при наявності таких досліджень.

Зазначені недоліки, безумовно, дещо звужують поле досліджень, але не є визначальними і тому не зменшують загальної високої оцінки проведеної роботи, наукової та практичної цінності дисертації.

**Висновок.**

Дисертаційна робота Погасія Сергія Сергійовича є кваліфікаційною науковою працею, що містить нові науково обґрунтовані результати проведених особисто здобувачем досліджень, які у галузі систем захисту інформації в сукупності вирішують актуальну науково-прикладну проблему щодо розробки методології підвищення ефективності захисту інформаційних ресурсів у кіберфізичних системах.

Сформульована в дисертації мета досліджень досягнута. Дисертація та автореферат повністю відповідають паспорту спеціальності 05.13.21 «Системи захисту інформації» та вимогам, які висуваються до дисертацій на здобуття наукового ступеня доктора наук згідно з «Порядком присудження наукових ступенів».

За зроблений внесок у підвищення рівня інформаційного захисту підприємств та державних установ в умовах впливу зовнішніх і внутрішніх загроз в інформаційної сфері, подальший розвиток в дисертації науко-методичного забезпечення виявлення, розпізнавання та локалізації цифрових засобів негласного отримання інформації та одержані при цьому вагомі теоретичні й практичні результати, вважаю, що Погасій Сергій Сергійович заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Офіційний опонент
Професор кафедри засобів захисту інформації
Факультету комп'ютерних наук та технологій
ДНП «ДУ Київський авіаційний інститут»

доктор технічних наук, професор

«20» 11 2024 року

В.О. Хорошко

Підпис Хорошка В.О.
засвідчую
Вчений секретар
Державного некомерційного підприємства „Державний Київський авіаційний інститут"