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

вул. Солом'янська, 7, м. Київ

ВІДГУК
офіційного опонента

професора кафедри систем та технологій кібербезпеки, доктора технічних наук, професора Казмірчук Світлани Володимирівни, 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.

Актуальність теми дисертаційної роботи «Моделі і методи захисту інформації в кіберфізичних системах» визначається сучасними викликами, які виникають у зв'язку зі швидким розвитком кіберфізичних систем у різних сферах: від промисловості та транспорту до охорони здоров'я та енергетики. Ці системи забезпечують тісну інтеграцію фізичних процесів із цифровими технологіями, що дозволяє підвищувати ефективність управління, автоматизації та моніторингу. Однак поряд із цим збільшується ймовірність кібератак, що спричиняють значні загрози безпеці інформації, а також можуть порушувати нормальне функціонування фізичних процесів. Таким чином, забезпечення надійного захисту інформації в кіберфізичних системах об'єктів критичної інфраструктури є однією з ключових умов для сталого розвитку цифрової економіки та суспільства в цілому.

Не тільки зростання кількості кіберінцидентів, а й зростання їх складнощі призводить до необхідності підвищення безпеки. Основною причиною ескалації кібератак по відношенню до кіберфізичних систем таких, як CPS може бути те, що більшість систем управління експлуатують стандартні рішення. Також більшість традиційних методів захисту інформації виявляються малоефективними або непридатними для застосування в CPS, оскільки вони не враховують специфіку тісної інтеграції фізичних і кіберкомпонентів, динамічний характер систем, обмеження обчислювальних ресурсів і необхідність роботи в режимі реального часу. В результаті CPS стають більш уразливими до кіберзагроз, ніж будь-коли раніше.

Оскільки масштаб і природа CPS критичних інфраструктур не дозволяють проводити експерименти, основна увага досліджень у напрямку підвищення рівня захищеності, усвідомлення критичних інфраструктур та їх

взаємозв'язків, властивостей і стійкості до зловмисних дій, що виникають, повинна бути спрямована на побудову моделей та їх використання.

Тому, дослідження, спрямоване на формування концепції побудови систем безпеки, в основі яких лежить множина моделей, що описують різні сторони об'єктів критичної інфраструктури, є дуже важливе, яка дозволяє забезпечити безпеку та надійність системи. А тема дисертації «Моделі і методи захисту інформації в кіберфізичних системах» є актуальною в сучасних умовах.

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).

2. Аналіз основного змісту, наукової новизни і практичної цінності, достовірності та обґрунтованості результатів.

Аналіз основного змісту, наукової новизни та практичної цінності

Дисертація складається з анотації, вступу, 5 розділів, висновків, списку використаних джерел з 255 найменувань на 29 сторінках та додатків на 33 сторінках. Повний обсяг якої становить 330 сторінок друкованого тексту, з них 261 сторінок основного матеріалу.

За своїм змістом дисертаційна робота Погасія С.С. відповідає чинним вимогам щодо оформлення дисертацій на здобуття наукового ступеня доктора технічних наук, 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* обґрунтовано 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. Визначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації.

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, автор прийшов до висновку, що існує науково-прикладна проблема щодо розробки методології підвищення рівня захищеності інформаційних ресурсів у кіберфізичних системах, і тому потрібно розробити методологію захисту інформації у кіберфізичних системах. Доведено, що вирішення сформульованих автором завдань розробки та удосконалення моделей та методів захисту інформації дозволить здійснити розробку методології захисту інформації в кіберфізичних системах.

Другий розділ присвячено розробці моделей захисту інформації в кіберфізичних системах на основі моделі Лотки-Вольтерри. Показано, що 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* наведена розробка підходу до забезпечення захисту каналу зв'язку на основі постквантових алгоритмів. Створення сучасних синтезованих мереж ґрунтується на гібридизації 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 порівняння 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. 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. Основною ідеєю концепції є здатністю створення захищених каналів або передачі захищеної інформації при передачі інформаційних та керуючих сигналів від виконуючих пристроїв до сервера сховища та обробки інформації. Наголошується, що саме 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.

Новизна одержаних 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, та які базуються на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах.

В рамках проведених досліджень для досягнення мети автором особисто отримані наступні нові наукові результати:

1) вперше розроблено концепцію побудови багатоконтурної системи захисту кіберфізичних систем, яка 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 дозволяє своєчасно визначити спрямованість загроз, врахувати обчислювальні ресурси нападників;

3) вперше розроблено метод забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів кіберфізичних систем, який 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 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 враховую рівень критичності загроз, відношення загрози до складової безпеки, послуги безпеки, вплив загрози відповідно до регуляторів та оцінки фінансових можливостей порушника, що дозволяє оцінювати гібридність загроз та відкриває новий підхід побудови перспективних систем захисту інформаційних ресурсів кіберфізичних систем;

6) вперше розроблено методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка відкриває новий підхід побудови перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

Практичне значення одержаних автором наукових результатів.

Практична цінність роботи полягає в наступному.

1. Запропонована 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, якій забезпечує автономне управління елементами кіберфізичної системи, закриття каналів

зв'язку (як дротових, так й бездротових на основі крипто-кодових конструкцій Нідеррайтера на LDPC-кодах).

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

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

Ступінь достовірності й обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Обґрунтованість одержаних положень та результатів, отриманих здобувачем, ґрунтуються на теоретично обґрунтованих та практично апробованих методах теорії множин, теорії криптографії, теорії кодування та теорії скінченних полів Галуа, теорії ймовірностей і математичної статистики, експертного оцінювання, математичної логіки і теорії автоматів, системного аналізу, законах синергії.

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

Оцінка мови, стилю та змісту дисертації, відповідність встановленим вимогам щодо оформлення.

Оформлення дисертації та автореферату відповідає вимогам Державних стандартів України. Дисертація і автореферат написані грамотною технічною мовою, ясно та зрозуміло. 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, підготовлених автором для публічного захисту, має внутрішню єдність та свідчить про особистий внесок автора у науку.

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

Повнота викладу наукових результатів дисертації в публікаціях. 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.

Зауваження та недоліки до тексту дисертації

1) В роботі зазначено, що мета дисертаційної роботи полягає у підвищенні ефективності захищеності інформації, а в загальному висновку (пункт 11) автор констатує, що – мета досліджень щодо підвищення рівня захищеності інформації та всі часткові завдання вирішені повністю. Оскільки, ефективність захищеності інформації відображається за допомогою комплексних показників, доцільно б було розкрити в роботі, що саме автор вкладає в це поняття.

2) В описі предмета дослідження здобувач зазначає моделі і методи захисту інформації у кіберфізичних системах, але в першому розділі в пп. 1.1 проводить аналіз загроз інформаційної безпеки в кіберфізичній системі та в подальшому використовує це для удосконалення класифікатора загроз.

3) В дисертаційній роботі автор вирішує актуальну науково-прикладну проблему щодо розробки моделей і методів захисту інформації в кіберфізичних системах. Виходячи з такої назви роботи, мета роботи повинна полягати саме в розробці моделей та методів, що дозволяють підвищити захищеність кіберфізичних систем.

4) В авторефераті стверджується, що «оцінка рівня загроз неможлива без оцінки можливостей самих нападників (зловмисників, кіберзлочинців тощо)» (стор 14 автореферату). Таке твердження є суперечним. Доцільно було б розглядати співвідношення можливостей злочинців та «жертв», тим більш, що формалізація цього положення наведена далі.

5) З дисертаційної роботи та автореферату не зрозуміло, яким чином використання моделі Лоткі-Вольтери, яка описує динаміку взаємодії злочинця та жертви, дозволяє підвищити рівень захищеності кіберфізичних систем. Також не зовсім зрозуміло, яким чином результати, отримані при використанні моделі Лоткі-Вольтери (розділ 2), знайшли практичне використання у наступних розділах.

6) У переліку наукової новизни роботи значено, що вперше розроблено методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем (п.6). Але в авторефераті не наведено ніяких даних (крім загальних тверджень), щодо такої методології, наприклад, її структура, склад, взаємозв'язки між компонентами. Це викликає питання до узгодження зазначеної наукової новизни та структурних компонентів роботи, де розкривається розроблена методологія.

7) В авторефераті недостатньо приділено увагу розробленню методики забезпечення відмовостійкості, яка є необхідною при побудові автоматизованої системи пеленгації та радіомоніторингу, та обумовлюється можливими відмовами у роботі антено-фідерної системи. Зазначена характеристика є важливою, оскільки елементи антено-фідерної системи передбачається встановлювати поза межами будівель і не завжди в умовах, придатних для тривалої безперервної роботи.

8) У загальних висновках і у новизні заначено, що використання методології побудови системи безпеки інформаційних ресурсів кіберфізичних систем, дозволило підвищити ефективність захисту

інформаційних ресурсів кіберфізичних систем на 5%, але не зазначено у порівняні з чим.

Проте, зазначені недоліки не є визначальними і тому не знижують цінності дисертаційної роботи, її науково-теоретичного і практичного значення та загальної позитивної оцінки.

3. Загальний висновок по роботі.

Дисертаційна робота Погасія Сергія Сергійовича є завершеною кваліфікаційною науковою працею та свідчить про особистий внесок автора в науку. Робота містить нові науково обґрунтовані результати проведених особисто здобувачем досліджень, які у галузі систем захисту інформації в сукупності вирішують актуальну науково-прикладну проблему 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 чинним вимогам п. 6-9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженому постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197, які висуваються до дисертацій, а її автор, Погасій Сергій Сергійович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Офіційний опонент:
Професор кафедри систем та
технологій кібербезпеки
Державного університету
інформаційно-комунікаційних технологій,
доктор технічних наук, професор С. В. Казмірчук

«21» 11 2024 року

Підпис Казмірчук С.В. засвідчую
Проректор з навчальної роботи Артур ГУДМАНЯН