ВІДГУК
офіційного опонента
на дисертаційне дослідження Давиденка Анатолія Миколайовича
«Методи та моделі адаптивного захисту та розмежування доступу
до розподілених інформаційних ресурсів», представлену на здобуття
наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми. Сучасні методи захисту інформації у кіберпросторі розраховані на стандартну обчислювальну архітектуру, тому при застосуванні для обробки розподіленого інформаційного ресурсу паралельного середовища дуже часто виникає дилема – або втрачати продуктивність, або ризикувати даними, обробляючи їх у відкритому вигляді. Нажаль, інколи своєчасне отримання результатів є не менш критичним, ніж безпека даних.

Тому дослідження та розвиток методів побудови підсистем розмежування доступу, які усувають зазначене протиріччя в системах обробки розподіленого інформаційного ресурсу, є важливою науковою проблемою, а її вирішення має велике державне значення. Отже, це протиріччя, зважаючи на високий ступень загроз, що існує для державних інформаційних ресурсів на теперішній час, робить тему дисертаційного дослідження Давиденка А. М. вельми **актуальною**.

Оцінка обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації, їх достовірність, новизна. Мета дисертаційної роботи полягає у вирішенні важливої науково-прикладної проблеми, сутність якої складає усунення протиріччя між необхідністю високопродуктивної обробки інформаційних ресурсів з обмеженим доступом, паралельна обробка яких висуває високі вимоги до швидкості їх підготовки, але однопотокові механізми розмежування доступу не можуть їх забезпечити.

Досягнення мети автор дисертаційного дослідження проводить шляхом розробки методів та моделей, які здатні узгоджувати продуктивність методів обробки та захисту та адаптувати їх один до одного для високопродуктивного та безпечного існування в розподіленому інформаційному кібердовкіллі.

У процесі такої розробки автором отримано низку нових рішень науково-технічних задач, спрямованих на формування системи розмежування доступу до інформаційних ресурсів людини, суспільства та держави. Вони базуються на використанні моделей захисту, що за допомогою оперативного налаштування процесу контролю розмежування доступу, в тому числі на основі нейронних мереж, дозволило наділити відповідну підсистему захисту властивостями адаптації по відношенню до критеріїв, які визначаються параметрами рівня безпеки системи та параметрами, що характеризують процеси обробки інформації у спеціалізованих розподілених інформаційних системах.

Таким чином маю зазначити, що автором досягнута мета роботи зі забезпечення процесу декомпозиції розмежування доступу до розподілених інформаційних ресурсів, шляхом адаптації системи захисту до поточного стану безпеки кібердовкілля, що обумовлюється вирішенням науково-технічної проблеми, породженою об'єктивним протиріччям між існуючою потребою в багатопотоковому доступі до розподілених інформаційних ресурсів грід-систем, з одного боку, та централізованою однопотоковою архітектурою існуючих засобів захисту, з іншого.

Для досягнення поставленої мети, автором було розв'язано наступні задачі:

– проведено аналіз відомих методів розмежування доступу до ресурсів інформаційних систем та досліджено відповідні математичні моделі з метою виявлення можливостей їх використання для захисту розподілених інформаційних ресурсів;

– удосконалено моделі нейронних мереж для забезпечення керування розмежуванням доступу;

– розроблено метод самоорганізації засобів розмежування доступу;

– розроблено та досліджено основні інформаційні компоненти розширення функціоналу засобів розмежування доступу до інформаційних ресурсів;

– розроблено метод адаптації системи розмежування доступу для розподілених інформаційних ресурсів відповідно до поточного стану безпеки кібердовкілля;

– розроблено методи аналізу стану безпеки систем розмежування доступу;

– розроблено модель та окремі компоненти засобів системи розмежування доступу;

– проведено експериментальні дослідження запропонованих методів, моделей та систем.

На мою думку, об'єкт та предмет дослідження обрані коректно та відповідають поставленій проблемі та задачам, вирішеним та розв'язаним автором.

Вважаю, що **достовірність** наукових результатів, отриманих автором, підтверджується наступними положеннями:

– передумови, які обрані для постановки мети та вирішення задач дисертаційного дослідження, в достатній мірі аргументовані та виключають неоднозначні трактування;

– строгість, коректність та достовірність результатів, які наведені в дисертаційній роботі, адекватні виконаним розрахункам, які базуються на використанні при дослідженнях сучасного математичного апарату;

– коректністю поставлених задач при проведенні експериментальної перевірці отриманих теоретичних результатів;

– відповідністю результатів експериментів теоретичним положенням, набутим при проведенні дисертаційного дослідження;

– науковими публікаціями здобувача основних результатів дисертаційного дослідження, його окремих матеріалів та сформульованих рекомендацій у фахових виданнях за вимогами та переліками МОН України;

– обговоренням результатів на численних міжнародних конференціях та семінарах.

Обґрунтованість наукових методів, положень, висновків дисертаційної роботи визначається коректністю виконаних теоретичних та експериментальних досліджень, практичним застосуванням отриманих результатів, про що свідчить їх широке впровадження у практику, що підтверджується актами впровадження у діяльність державних установ нашої країни. Це дає змогу вважати, що сформульовані в дисертації наукові положення, висновки та рекомендації достатньо повно обґрунтовані здобувачем та викладені в доказовій формі.

У дисертаційному дослідженні автором отримані такі основні **нові наукові результати**:

– *вперше розроблено* структурно-функціональну декомпозиційну модель системи розмежування доступу, яка за рахунок блоків аналізу результатів реалізованого доступу, аналізу ситуації відмови в доступі, критеріїв адаптації засобів захисту відповідно до поточного стану безпеки кібердовкілля та керування засобами захисту системи доступу, дозволяє реалізувати запропонований метод адаптації системи розмежування доступу, шляхом розробки та рекомбінації окремих компонентів системи розмежування доступу до розподілених інформаційних ресурсів;

– *вперше розроблено* структурну модель засобів інформаційного забезпечення системи розмежування доступу, в якій за рахунок сюр'єкції множин ідентифікаторів предметних областей користувачів та об'єктів доступу формуються бієкції та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень;

– *вперше запропоновано* метод адаптації системи розмежування доступу, в якому за рахунок генерування зміни оцінки значень параметрів та регулювання їх кількості при збереженні логіки аналізу, система розмежування доступу набуває нового функціоналу автоматичного інкременту або декременту кількості механізмів захисту при відповідній варіабельності стану безпеки ресурсів інформаційних систем;

– *удосконалено* структурну модель нейрона, в якій за рахунок інтегрування додаткового блоку пам'яті та блоку аналізу, які комутуються до блоку підсумовування вхідних параметрів та формують зворотний зв'язок з функціональними змінними нейрона, реалізується новий функціонал організації контролю даних в системах розмежування доступу;

– *удосконалено* метод аналізу системи розмежування доступу, який за рахунок консолідації оцінок рівня захищеності індивідуальних елементів об'єкта доступу, множини загроз, множини зв'язків із зовнішнім оточенням, функціонального завантаження об'єкта доступу та параметру навантаження обчислювальних ресурсів дозволив отримати комплексну оцінку стану безпеки;

– *отримав подальший розвиток* метод самоорганізації засобів розмежування доступу, в якому за рахунок застосування правила Хебба та відповідної модифікації адаптаційної залежності, для випадку формування вхідних сигналів, які не містять постійної складової, сформовано співвідношення для побудови рекурентного алгоритму на базі односпрямованої нейронної мережі.

Проведені дослідження базуються на сучасних методах математичного та комп'ютерного моделювання для аналізу отриманих результатів, семантичного аналізу та теорії інформації для побудови структурної моделі засобів інформаційного забезпечення системи розмежування доступу та створення окремих інформаційних компонентів, теорії нейронів та нейронних мереж, удосконалення структурної моделі нейрона, теорії навчання, самоорганізації та моделювання нейронних мереж для побудови методу самоорганізації засобів розмежування доступу, багатофакторного та системного аналізу для розробки методу адаптації контролю даних в системах розмежування доступу.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи безпосередньо пов'язана з виконанням 39 НД та ДКР, що проводилися за планами та темами численних державних організацій, установ та підприємств. Їх повний перелік наведено у дисертації та її авторефераті.

Повнота викладення наукових положень, висновків та рекомендацій, сформульованих у дисертаційному дослідженні та опублікованих у працях. За напрямом дисертаційного дослідження здобувачем опубліковано 175 (в авторефераті наведено 57) наукових праць. Із наведених в авторефераті, в тому числі: 1 колективна монографія, 4 наукові статті в міжнародних рецензованих виданнях, що входять в бази даних *Scopus* та *Web of Science*, 2 наукові статті в іноземних наукових журналах, 7 наукових статей у вітчизняних наукових журналах, які входять до інших міжнародних наукометричних баз даних, 26 статей у наукових фахових журналах та збірниках, 2 патенти України, а також матеріали та тези доповідей на 15 конференціях.

Таким чином, результати дисертаційної роботи пройшли достатню апробацію на Всеукраїнських та Міжнародних науково-практичних конференціях, а пе-

рераховані публікації з достатньою повнотою відбивають наукові та практичні результати дисертації.

З праць, які опубліковано у співавторстві, у дисертації використано лише ті результати, які отримані здобувачем самостійно.

За своєю структурою дисертаційна робота складається зі вступу, шести розділів, які містять основні наукові результати, загальних висновків, списку використаної літератури та додатків. Дисертація містить 37 рисунків, 3 таблиці. Список використаних джерел складається з 220 найменувань і займає 22 сторінки. Додатки розміщені на 32 сторінках. Загальний обсяг дисертації складає 347 сторінок, основний текст роботи викладено на 262 сторінках.

Наукове значення дисертаційної роботи полягає в подальшому розвитку теорії захисту інформації в частині, що стосується створення методів розмежування доступу для систем розподіленої обробки інформації, спроможних адаптувати засоби захисту відповідно до поточного стану безпеки кібердовкілля.

Практичне значення дисертації полягає у створенні діючого алгоритмічного та програмного забезпечення модулів, що реалізують побудову механізмів захисту систем розмежування доступу, створення нових структурних рішень та програмних моделей для розмежування доступу до розподілених інформаційних ресурсів.

Аналіз автореферату свідчить про його відповідність матеріалам дисертаційного дослідження та, в цілому, вимогам МОН України.

Дисертація та автореферат написані з дотриманням прийнятої термінології, мовою, зрозумілою для фахівця. Зміст автореферату відповідає змісту дисертаційної роботи та цілком відображає результати проведеного дисертаційного дослідження.

Все це дає змогу позитивно оцінити розглянуте дисертаційне дослідження, відзначити його наукову новизну та практичне значення, самостійність виконання та високий теоретичний рівень. В цілому позитивно оцінюючи дисертаційне дослідження Давиденка А.М., необхідно висловити наступні ***зауваження***:

1. Здобувачем у першому розділі, при проведенні аналізу сучасних сис-

тем розмежування доступу, одержані результати подаються окремо для грід-систем та для класичних моделей розмежування доступу. На мій погляд, такий розподіл за визначеними класифікаційними ознаками не є досить раціональним, оскільки грід-системи можуть використовувати й класичні моделі.

З іншого боку слід відмітити, що при узагальненні результатів стосовно грід-систем (с. 87 дисертації та с. 2 автореферату, відповідно) здобувач прийшов до правильного висновку відносно того, що «однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом».

2. У другому розділі, при формалізації підходу до формування оцінки рівня безпеки системи доступу, здобувачем вводиться низка нових дефініцій. Наприклад «абсолютна», «персональна», «відносна» тощо (с. 131-132, дисертації, с. 14 автореферату, відповідно), які далі вживаються у тексті дисертації. У цілому з цим можна погодитися. Але при введенні нових термінів і понять в усталеній галузі науки, такій як захист інформації та інформаційна безпека, вважається за доцільне визначити їх місця у вже існуючій дефініційній системі або категорійному апараті, що дозволить визначити зв'язки між тим, що вже існує та тим, що пропонується.

3. При висвітленні процедури бієкції ідентифікаторів предметних областей користувача, автор визначає що «Міра непогодженості $u(\phi_1, ..., \phi_m)$ між фрагментами пропозиції Ψ визначається на основі максимальних значень величин суперечливості в кожному із фрагментів ϕ_i.» (с. 207 дисертації, с. 23 автореферату, відповідно). Фактичний вимір цих параметрів вимогає експертної оцінки, але здобувач не акцентує увагу на ряді важливих, на наш погляд, питань, які обов'язково мають бути визначені при використанні методів експертного оцінювання. Це стосується, власне, так званих характеристик самого експерта – його компетенції, кваліфікації, ступеня конформізму тощо; кількості експертів, що залучаються для опитування; методу узгодження експертних оцінок; побудови опитувальних таблиць.

Вважаю це питання принциповим, оскільки обробка даних процедури

експертного оцінювання суттєво впливатиме на міру неузгодженості ідентифікаторів предметних областей користувачів.

4. Не викликає сумніву факт того, що розроблений особисто здобувачем метод адаптації системи розмежування доступу, в якому за рахунок генерування зміни оцінки значень параметрів та регулювання їх кількості при збереженні логіки аналізу, система розмежування доступу набуває нового функціоналу автоматичного інкременту або декременту кількості механізмів захисту при відповідній варіабельності стану безпеки ресурсів інформаційних систем. Даний факт у доказовій формі викладено у п'ятому розділі. Але без введення обмежень на тип інформаційного ресурсу запропонований метод не може розцінюватися як універсальний інструмент, доведення якого до конкретного програмного або програмно-апаратного рішення стане панацеєю для усіх відомих і невідомих типів систем розмежування доступу. Це, на мою думку, не так. Тому слід бути більш коректним у безапеляційному формулюванні висновків.

5. Вважаю, що запропонована у четвертому розділі (с. 193 дисертації та с. 20 автореферату, відповідно) структурна схема засобів інформаційного забезпечення системи безпеки (рис. 4.1) досить повно описує всі необхідні складові типової системи захисту інформації. Схема виглядала би більш виграшно, якби здобувач відокремив би на ній ті компоненти, які відповідають за інформаційне забезпечення предметної області користувача, не за номерами, а більш впізнавано, наприклад – медичне, страхове тощо.

6. У шостому розділі здобувач стверджує, що проведено експериментальне дослідження для підтвердження достовірності отриманих теоретичних положень та практичних результатів. Так, дійсно такі дані приведені. Вони, на мою думку, достовірні. Але при цьому не в повній мірі дотримані (а скоріш за все не показані) процедурні питання проведення експерименту. Мають бути визначені його назва, мета, завдання, план проведення експерименту, спосіб обробки результатів тощо.

7. Зважаючи на достатньо обмежений обсяг автореферату, визначений керівними документами, у дисертації хотілося б побачити не тільки виконання

формальних вимог стосовно формулювання висновків до кожного розділу та до роботи у цілому, а й більш широке висвітлення одержаних результатів. Наприклад, здобувач нічого не каже про те, що ним особисто запропоновано новий підхід до проведення державної експертизі комплексних систем захисту інформації, який значно зменшує час проведення та підвищує якість результатів й ін. Від цього, без сумніву, робота набула б ще більшого наукового та практичного значення.

Зазначені зауваження, більшість з яких носять дискусійний характер, дещо впливають на якість поданої дисертаційної роботи, але їх наявність не знижує практичної, а тим більше, наукової цінності одержаних здобувачем результатів.

Слід зазначити, що дисертаційна робота Давиденка Анатолія Миколайовича «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів» відповідає п. 1 та п. 2 паспорту спеціальності 05.13.21 – системи захисту інформації та профілю спеціалізованої вченої ради Д 26. 062.17.

Викладене дозволяє зробити загальний висновок, що дисертаційне дослідження «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів» є завершеною науковою роботою, що виконана автором особисто на належному рівні, яке вирішує актуальну наукову проблему та має наукову новизну та практичну цінність.

За обсягом досліджень, науковим рівнем, новизною, науковою та практичною цінністю отриманих результатів дисертаційна робота повністю відповідає чинним вимогам до дисертацій на здобуття вченого ступеня доктора технічних наук, які містяться у пп. 9, 10, 12, 13 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 (зі змінами, внесеними згідно Постанови Кабінету Міністрів України № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р., № 567 від 27.07.2016 р., № 943 від 20.11.2019 р.), оскільки в ній запропоноване нове вирішення актуальної науково-практичної проблеми у галузі захисту інформації.

Вважаю, що актуальність розглянутої проблеми, практична та наукова цінність отриманих результатів дають право вважати, що Давиденко Анатолій Миколайович заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент –
головний науковий співробітник
науково-дослідної лабораторії ННІ №2
Національної академії внутрішніх справ
лауреат Державної премії УРСР в галузі науки і техніки
доктор технічних наук, професор,
заслужений професор НАВС **О. В. Рибальський**