До спеціалізованої вченої ради Д 26.062.17
Національний авіаційний університет 03058,
м. Київ, просп. Любомира Гузара, 1

ВІДГУК

офіційного опонента
доктора технічних наук, професора Казакової Надії Феліксівні
на дисертаційну роботу 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 дисертації, зв'язок з науковими програмами, планами, темами.

Зі стрімким розвитком інформаційних технологій зростає кількість загроз ресурсам інформаційних систем, що викликає, для забезпечення їх нормального функціонування та попередження вторгнень, необхідність застосування спеціалізованих засобів безпеки. Перспективним напрямком, який активно розвивається у сфері обробки інформації є паралельні високопродуктивні системи обробки розподілених інформаційних ресурсів. Нажаль, застарілі механізмі захисту, які історично вбудовані в операційні системі, не задовольняють вимогам по продуктивності, однопотокові засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи розмежування доступу повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

Таким чином, дисертаційна робота Давиденка Анатолія Миколайовича, виконання якої направлено на вирішення важливої науково-прикладної проблеми, пов'язаної з розробкою ефективних методів побудови систем розмежування доступу до розподіленого інформаційного ресурсу, є актуальною.

Актуальність і практичне значення наукового дослідження підтверджується результатами робіт, що виконувались у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в рамках наступних науково-дослідних тем: НДР «Кріт» «Розробка методів побудови та формального опису критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» № 0101U006700 (2001р.-2004р.). НДР «МодА» «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об'єктів» № 0105U001296 (2005р.-2008р.). НДР «Управление» «Розробка методів і комп'ютерних засобів підтримки прийняття рішень в задачах ситуаційного і технологічного управління в

енергетиці» № 0102U005589 (2002р.-2006р.). НДР «Модель» «Розвиток теорії, розробка нових методів і засобів математичного й комп'ютерного моделювання енергетичних і енергоємних об'єктів, систем і установок» № 0107U001945 (2007р.-2009р.). НДР «МодБ» «Исследование и разработка методов повышения безопасности и эффективности распределенных высокопроизводительных информационных технологий при решении задач энергетики» №0108U010588 (2009р.-2013р.). НДР «МодД» «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р.-2018р.). НДР «МодЕ» «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.-по теперішній час). НДР «ГІБРИД» «Розвиток теорії, розробка методів та засобів реалізації гібридних експертно-моделюючих комп'ютерних систем в задачах комплексного управління перетворенням енергії» № 0112U000050 (2012р.-2016р.). НДР «НОВІНТЕХ» «Розвиток теорії, розробка новітніх інформаційних технологій в задачах комплексного моделювання та управління процесами перетворення та використання енергії» №0117U004347 (2017р.-по теперішній час). НДР «ГРІДІПМЕМОН-11» «Створення грід-системи моніторингу, збору та аналізу даних в енергетичній галузі на базі грід-центру з питань енергетики» №0111U004339 (2011р.-2013р.), згідно Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки. НДР «ГРІДІПМЕМОН-15» «Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ, як ресурсного центра NGI_UA, та створення грід-сервіса централізованого синтезу конфігурацій для апаратних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0115U002876 (2015р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-16» «Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та створення системи централізованого програмування реконфігуровних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0116U006907 (2016р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-18» «Підтримка грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та використання хмарної інфраструктури для централізованого програмування реконфігуровних засобів інформаційної безпеки в енергетичній галузі» №0118U001370 (2018р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-19» «Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та модернізація веб-сервісу централізованого програмування реконфігуровних засобів інформаційної безпеки на базі гріду та хмарної інфраструктури» №0119U001812 (2019р.), згідно Програми

інформатизації НАН України на 2019р. НДР «ГРІДІПМЕМОН-20» «Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та проведення експериментів з системою програмування реконфігуровних засобів на базі гріду та хмарної інфраструктури» №0120U103624 (2020 р.), згідно Програми інформатизації НАН України на 2020 р. Більшість з перерахованих НДР було виконано здобувачем в якості наукового керівника, інші – в якості відповідального виконавця.

Також частка досліджень виконувалась в рамках: Науково-технічної програми «Розвиток системи технічного захисту інформації в Україні», Постанова Кабінету Міністрів України від 21.06.2000 р. №681-009 та програми робіт з організації, стандартизації та сертифікації в галузі ТЗІ, це роботи, які проводились разом з КПІ в інтересах Державної служби спеціального зв'язку та захисту інформації України НДР «РизикМ», договір №239-01 від 15.09.2001р., (2001р.-2007р.).

Результати дисертаційної роботи застосовувалися при проведенні практичних робіт з експертизи технічних систем захисту. Прикладом таких робіт є: експертиза «Комутатор зв'язку КС ТУ У 31016953.001-2000» виробництва ЗАТ «Теком», яка виконувалась за дорученням ДСТСЗІ СБ України Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України договір №241-03 від 26.12.2003р. «Державна експертиза комплексної системи захисту інформації українського академічного грід-вузла Інституту теоретичної фізики НАН України та комплексної системи захисту інформації Центру реєстрації віртуальних організацій» договір №201-13 від 14.06.13р. «Державної експертиза комплексної системи захисту інформації в автоматизованій системі управління персоналом "Кадри" рівня Укрзалізниці» договір №202-13 від 30.08.13р. «Державна експертиза комплексної системи захисту інформації автоматизованої інформаційної системи Президії Національної академії наук України» договір №203-14 від 22.07.14р. «Державна експертиза комплексної системи захисту інформації локальної обчислювальної мережі Управління справами НАН України» договір №207-16 від 30.06.16р. «Державна експертиза комплексної системи захисту інформації Національного Ресурсного центру Інституту кібернетики НАН України ім. В.М. Глушкова» №208-16 від 30.06.16р. «Державна експертиза комплексної системи захисту інформації на об'єкті, що належить Департаменту військово-технічної політики, розвитку озброєння, та військової техніки Міністерства оборони України» договір №149 від 27.06.18р. «Державна експертиза комплексної системи захисту інформації автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України» договір №211-19 від 17.01.19р.

Структура, обсяг та зміст дисертації. Дисертаційна робота складається з анотації, переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел та двох 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.

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.

У вступі обґрунтовано актуальність і доцільність обраної теми дисертаційної роботи; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мета і завдання дослідження; визначено об'єкт, предмет і методи дослідження; окреслені наукова новизна та практичне значення одержаних результатів; зазначений особистий внесок здобувача; вказані апробація результатів дисертації та кількість і характер публікацій.

Перший розділ дисертації присвячено аналізу існуючих методів та моделей розмежування доступу до ресурсів інформаційних систем. Одним з етапів проведеного аналізу є аналіз топології інформаційної безпеки Українського національного гріду. Також проаналізовано розвиток мереж розподіленої обробки та зберігання інформації та один з підходів до побудови систем захисту інформації.

В результаті проведеного аналізу було зроблено висновок про те, що при постійному зростанні продуктивності обчислювальних систем, однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом. На основі даного висновку було запропоновано наділити підсистему захисту властивостями адаптації по відношенню до необхідних критеріїв.

Другий розділ присвячено дослідженню особливостей нейронних моделей і вибору для подальшого аналізу узагальнених ознак класифікації нейронних мереж. Крім того, для подальших досліджень, наведені визначення різних видів оцінки рівня безпеки систем розмежування доступу.

Також в даному розділі виконано удосконалення методу аналізу системи розмежування доступу шляхом консолідації запропонованих складових.

Третій розділ роботи присвячено, в першу чергу, методам навчання нейронних моделей. Наведено процес навчання нейронної мережі, який полягає в формуванні у мережі характеристик необхідних для вирішення завдань, які

характерні для систем керування доступом. Проаналізовано типи таких задач. Виконано обґрунтування вибору необхідних способів навчання нейронної мережі, яка прийнята як базовий засіб для моделювання системи доступу.

Також в даному розділі зроблено висновок, що система керування доступом, відповідно до задач, які вона виконує, складається з підсистеми керування доступом та підсистеми захисту об'єкта від несанкціонованого доступу, доступ до якого забезпечується підсистемою захисту. Після чого формалізовано опис відповідних атак та введені необхідні визначення.

Наступним виконаним кроком був аналіз методів самоорганізації нейронних систем для виконання розпізнавання атак. Також продемонстровано що алгоритми самоорганізації можуть реалізовуватися в процесі функціонування нейронної мережі, при вирішенні тих завдань безпеки, на які дана мережа орієнтована.

Четвертий розділ дисертації присвячено розробці базових інформаційних компонентів, необхідних для розширення засобів захисту системи доступу, з метою опису природною мовою складових частин системи захисту. Для чого було проаналізовано основні інформаційні компоненти та наведено і формалізовано умови їх існування.

Після чого запропонована схема засобів системи розмежування доступу та досліджені взаємозв'язки між семантичними параметрами. Дане дослідження необхідно було для подальшого розширення функціональних можливостей під час виконання контролю доступу.

П'ятий розділ дисертаційної роботи присвячено аналізу основних способів реалізації процесів адаптації, при вирішенні завдань захисту систем доступу. Визначено якими співвідношеннями регламентується процес адаптації в системі керування доступом; розглянуто ряд умов, дотримання яких необхідно в даному випадку; визначено і проаналізовано аспекти, які є загальними для системи, що володіє властивостями адаптації.

Далі було обґрунтовано необхідність формування в межах нейронної мережі спеціалізованих вузлів, які реалізують функції, відповідні до поставленої задачі. Після чого запропонована структура фрагмента нейронної мережі, який використовується для формування всієї мережі, і відрізняється низкою, зазначених в роботі, відмінностей від фрагментів традиційних мереж.

Запропоновані способи реалізації додаткових компонентів нейрона. При цьому, додаткові функціональні входи суматора не пов'язані із загальною класичною структурою нейрона, а забезпечують зв'язок елементів нейрона з додатковими функціональними блоками. Розглянуто призначення цих блоків та принцип їх роботи. Після чого, розроблено функціональну схему фрагмента нейронної мережі.

Шостий розділ присвячено демонстрації та опису розроблених програмних застосунків безпеки систем розмежування доступу та інших розробок, експериментальні дослідження, впровадження та успішне використання яких, підтвердили достовірність теоретичних положень та висновків дисертаційної роботи.

У **висновках** сформульовані основні наукові та практичні результати дисертаційної роботи та наведені дані про їх впровадження.

В **додатках** наведено документи, що підтверджують впровадження результатів дисертаційної роботи, та лістинг розроблених програмних застосунків безпеки систем розмежування доступу та інших розробок.

Ступінь обґрунтованості та достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації підтверджуються коректною постановкою завдань, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, узгодженістю теоретичних положень з результатами експериментальних досліджень, опублікованими науковими працями у фахових виданнях, підтвердженим співробітництвом с Lund University Department of Physics Sweden, результатами проведених, за дорученням ДССЗЗІ СБУ України, державних експертиз комплексних систем захисту, результатами досліджень, що виконувались у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в рамках науково-дослідних тем, під керівництвом здобувача та відповідними актами впровадження у діяльність Інституту кібернетики імені В.М. Глушкова Національної академії наук України, ТОВ «Софтлайн ІТ», НДЦ «Нафтогазбурмаш», Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, а також використанням в навчальному процесі Київського національного університету імені Тараса Шевченка, Національного авіаційного університету для підвищення підготовки фахівців з кібербезпеки.

Наукова новизна результатів роботи. На основі аналізу результатів дослідницької роботи Давиденка А.М., можна зробити висновок, що найбільш суттєвими новими науковими результатами, які представлені ним у дисертації, є наступні:

- удосконалено структурну модель нейрона, в якій завдяки введенню додаткових елементів реалізується новий функціонал організації контролю даних в системах розмежування доступу;
- отримав подальший розвиток метод самоорганізації засобів розмежування доступу, в якому модифікується адаптаційна залежність, для випадку формування вхідних сигналів, які не містять постійної складової, та формується співвідношення для побудови рекурентного алгоритму на базі односпрямованої нейронної мережі;
- вперше розроблено структурну модель засобів інформаційного забезпечення системи розмежування доступу, в якій за рахунок побудови механізму об'єднання множин ідентифікаторів предметних областей користувачів та об'єктів доступу формуються більш складні комплексні множини ідентифікаторів предметних областей та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень;
- вперше запропоновано метод адаптації системи розмежування доступу, в якому шляхом генерування зміни оцінки значень параметрів та регулювання їх

кількості, система розмежування доступу набуває нового функціоналу автоматичного підключення або відключення механізмів захисту при зміні стану безпеки ресурсів інформаційних систем;

• 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;

• вперше розроблено структурно-функціональну модель системи розмежування доступу, яка за рахунок декомпозиції системи на блоки 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, реалізує запропонований метод адаптації системи розмежування доступу.

Теоретичне та практичне значення роботи. Представлені в роботі моделі та методи побудови систем розмежування доступу породжені появою нових типів високопродуктивної обробки інформаційних ресурсів та орієнтовані на створення засобів, що розширюють функціональні можливості сучасних систем розмежування доступу є важливим теоретичним внеском у наукову спеціальність 05.13.21 – «Системи захисту інформації». Практичне значення отриманих результатів полягає у тому, що розроблені в роботі моделі та методи адаптації засобів захисту, використовувались при реалізації систем контролю доступу, окремих механізмів захисту та побудові моделей загроз та порушника в процесі створення систем захисту інформації, а також програм та методик випробувань при проведенні державних експертиз комплексних систем захисту за дорученням ДССЗЗІ СБУ України.

Рекомендації щодо використання результатів, одержаних автором. Теоретичні та практичні результати дисертаційної роботи доцільно використовувати в організаціях як приватного, так і державного секторів, а також в науково-дослідних та навчальних установах України, які займаються теоретичними та практичними питаннями, пов'язаними з розробкою та аналізом ефективності функціонування систем захисту інформації, що обробляється в інформаційних системах. Зокрема, отримані результати можуть бути використані для ефективного вибору існуючих або розширення функціональних можливостей сучасних систем розмежування доступу.

Повнота викладення наукових положень дисертації в опублікованих працях. Основні результати за темою дисертації автором викладено в опублікованих 57 наукових працях. Зокрема, 1 колективна монографія, 4 наукових статті в міжнародних рецензованих виданнях, що входять в бази даних Scopus та Web of Science, 2 наукові статті іноземних наукових журналах, 7 наукових статей у вітчизняних наукових журналах, які входять в інші міжнародні наукометричні бази даних, 26 наукових статей у наукових фахових журналах та збірниках, 2 патенти, 15 матеріалів та тез доповідей конференцій.

За своїм змістом та отриманими результатами дисертаційна робота

відповідає формулі та пунктам напрямів досліджень паспорту спеціальності 05.13.21 - «Системи захисту інформації», а саме: пункту 1 в частині розробки «теоретичних, методологічних, технічних основ створення комплексних систем захисту інформації ... »; пункту 2 в частині розробкою «... архітектури, методології проектування, технології функціонування систем захисту інформації»; пункту 8 в частині «моделювання процесів нападу на інформацію та її захисту». Вона є завершеною кваліфікаційною працею з науковими положеннями, що надані автором для публічного захисту, характеризується внутрішньою єдністю та доводить особистий внесок автора в науку.

При цьому зміст автореферату повністю відображає основні положення дисертаційної роботи.

Зауваження та питання дискусійного характеру.

1. Оскільки з аналізу першого розділу прослідковується недосконаліть і неготовність сучасних систем розмежування доступу адаптуватися в реальному часі до стану кібердовкілля, то автору доцільно було б більш широко розглянути методи розмежування доступу, які використовують керування доступом на основі ролей.

2. При розробці методу аналізу системи розмежування доступу, який за рахунок консолідації оцінок рівня захищеності елементів та параметрів системи дозволив отримати комплексну оцінку стану безпеки, було б доцільно врахувати такі чинники, як узгодженість суджень експертів та рівень їх компетентності.

3. В дисертаційному досліджені метод самоорганізації засобів розмежування доступу, побудовано на основі правил Хебба та Сангера, але не розглянуто, як можна застосувати для цього інші правила, наприклад, сигмоїдальні; або треба було вказати чому обрані саме ці правила.

4. Дисертація має велику кількість об'ємних формул та рисунків, що робить роботу досить великою та складною для сприйняття. Деякі рисунки в авторефераті та дисертації є важкими для сприйняття через їхній розмір та нагромадження.

5. При формуванні наукової новизни, практичної цінності та висновків автор наголошує на розробці великої кількості нових методів, моделей та програмного забезпечення, проте у авторефераті і дисертаційній роботі зазначає про наявність тільки двох патентів. Наявність патентів на всі отримані автором наукові та практичні результати підвищили б вагомість роботи.

6. В роботі присутні стилістичні та орфографічні помилки, котрі, в цілому не впливають на сприйняття роботи.

Зазначені недоліки не є визначальними і тому не зменшують загальної високої оцінки проведеної роботи, наукової та практичної цінності дисертаційної роботи Давиденка Анатолія Миколайовича.

Висновок.

Загалом, робота характеризується внутрішньою єдністю, виконана на належному науковому рівні та є завершеною науковою працею, в якій отримано

нові науково обґрунтовані результати, що в сукупності вирішують науково-прикладну проблему, пов'язану з побудовою систем розмежування доступу, які мають здібності адаптуватися до стану кібердовкілля та збільшувати продуктивність обчислювальної системі за рахунок обґрунтованого зменшення рівня небезпеки.

За актуальністю, науковою новизною, практичною значущістю та сформульованими науковими положеннями вважаю, що дисертаційна робота Давиденка Анатолія Миколайовича «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів» відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 №567 (із змінами), а її автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 - «Системи захисту інформації».

Офіційний опонент
Завідувач кафедри інформаційних технологій
Одеського державного екологічного університету
доктор технічних наук, професор Н.Ф. Казакова
«29» 04 2021 року

Підпис професора Казакової Н.Ф. засвідчую,
Проректор з наукової роботи
Одеського державного екологічного Університету
доктор географічних наук, професор Ю.С.Тучковенко