Голові спеціалізованої вченої ради 26.062.17
при Національному авіаційному університеті
03058, м. Київ, пр. Любомири Гузара 1

ВІДГУК
офіційного опонента
професора кафедри кібербезпеки та математичного моделювання
Національного університету «Чернігівська політехніка»,
доктора технічних наук, професора Шелеста Михайла Євгеновича
на дисертаційну роботу Давиденка Анатолія Миколайовича
«Методи та моделі адаптивного захисту та розмежування доступу
до розподілених інформаційних ресурсів»,
представлену на здобуття наукового ступеню доктора технічних наук
за спеціальністю 05.13.21 – « Системи захисту інформації»

Актуальність теми дисертаційної роботи. В сучасному суспільстві відбувається значне зростання обсягів інформації, що накопичується, зберігається та оброблюється в інформаційних систем. Концентрація інформації в єдиних базах даних різного призначення та різке розширення кола користувачів, що працюють з нею, породжують проблему безпечного функціонування систем доступу до інформації. Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних ІТ призводять до постійного збільшення різноманітності методів зламу захисту і, як наслідок, до порушень політики доступу з метою несанкціонованого ознайомлення, модифікації або знищення інформаційного ресурсу. Для запобігання цьому створюються системи розмежування доступу, які є невід'ємною частиною будь-якої сучасної системи безпеки, а світова тенденція свідчить про те, що автентифікація та визначення прав доступу користувачів, є обов'язковою функцією операційної системи та застосовується в різному програмному забезпеченні. Виникає потреба розширення функціональних можливостей таких систем за рахунок впровадження методів забезпечення декомпозиції процесу доступу.

Таким чином, існує певна проблема, яка обумовлена об'єктивним протиріччям між, з одного боку, потребою в багатопотоковому доступі до розподілених інформаційних ресурсів систем, а, з іншого, - централізованою однопотоковою архітектурою існуючих засобів захисту, що обумовлює актуальність теми дисертаційної роботи Давиденка А.М.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, що проводились при виконанні дисертаційної роботи, виконувались у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України у 2001-2020 роках в рамках більш ніж 15 науково-дослідних робіт та науково-технічних програм, зокрема:

- НДР «Кріт» «Розробка методів побудови та формального опису критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» № 0101U006700 (2001-2004 р.);
- НДР «МодД» «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014-2018 р.);
- НДР «МодЕ» «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.-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-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;
- науково-технічної програми «Розвиток системи технічного захисту інформації в Україні» (Постанова Кабінету Міністрів України від 21.06.2000 р. №681-009);
- НДР «Ризик-М» (2001р.-2007р.) щодо програми робіт з організації, стандартизації та сертифікації в галузі ТЗІ в інтересах ДССЗЗІ України (договір №239-01 від 15.09.2001 р.

У більшості вказаних робіт автор дисертації був науковим керівником чи відповідальним виконавцем.

Формулювання наукових задач, які необхідно вирішити для досягнення поставленої мети. Метою дисертаційного дослідження є забезпечення процесу декомпозиції розмежування доступу до розподілених інформаційних ресурсів, шляхом адаптації системи захисту до поточного стану безпеки кібер-

середовища. У якості об'єкту дисертаційного дослідження обрано процес захисту та розмежування доступу до інформаційних ресурсів, а предметом дослідження стали методи і моделі адаптивного захисту та розмежування доступу до ресурсів інформаційних систем.

Для досягнення поставленої мети було поставлено наступні задачі:

- аналіз відомих методів розмежування доступу до ресурсів інформаційних систем та дослідити відповідні математичні моделі з метою виявлення можливостей їх використання для захисту розподілених інформаційних ресурсів;
- удосконалення моделі нейронних мереж для забезпечення керування розмежуванням доступу;
- розробка методу самоорганізації засобів розмежування доступу;
- розробка та дослідження основних інформаційних компонент розширення функціоналу засобів розмежування доступу до інформаційних ресурсів;
- розробка методу адаптації системи розмежування доступу для розподілених інформаційних ресурсів відповідно до поточного стану безпеки кіберсередовища;
- розробка методу аналізу стану безпеки систем розмежування доступу;
- розробка моделі та окремих компонентів засобів системи розмежування доступу.

Оцінка змісту дисертації, її завершеності як єдиного цілого і оформлення. Дисертація складається з анотації, списку скорочень, вступу, шести розділів, загальних висновків, списку використаних джерел до кожного розділу та двох додатків. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам.

У вступі обґрунтовано актуальність теми дисертаційної роботи, показано зв'язок роботи з науковими темами, сформульовано мету та задачі досліджень, наведено методи дослідження, викладено наукову новизну та практичне значення одержаних результатів, зазначено особистий внесок здобувача та наведено відомості про впровадження, апробації, структуру роботи.

У першому розділі розглянуто теоретичні основи використання моделей розмежування доступу у розподілених інформаційних системах, проведено аналіз дослідного зразка спеціалізованої розподіленої інформаційної системи грід-сайту PIMEE ARC в складі Українського національного гріду, визначено параметри й властивості, які є критичними при його використанні у задачах, що розв'язуються.

У другому розділі наведено необхідні теоретичні особливості нейронних моделей та обрано узагальнені ознаки класифікації нейронних мереж для їх подальшого аналізу. Для введення визначеності в міркуваннях про рівень безпеки системи доступу розглянуто визначення абсолютної, персональної та відносної оцінки рівня безпеки системи розмежування доступу.

Удосконалено метод аналізу системи розмежування доступу, шляхом консолідації оцінки рівня захищеності індивідуальних елементів об'єкта доступу, множини загроз, множини зав'язків із зовнішнім оточенням, функціонального завантаження об'єкта доступу та параметру навантаження обчислювальних ресурсів.

В третьому розділі наведено теоретичні особливості методів навчання нейронних моделей.

В першу чергу розглянуті завдання розпізнання нових атак і завдання збільшення ефективності розпізнання атак, яке використовує сигнатури атак, на основі використання такої властивості нейронних мереж, як властивість її самоорганізації, яка є вищим за рівнем методів зміни можливостей мережі в порівнянні з методами навчання.

Підбір ваги вхідного вектору реалізується відповідно до нормалізованих правил Хебба, для випадку коли кількість нейронів відповідає кількості складових використовується правило Сангера. Розглянуто алгоритми самоорганізації на базі рекурентних співвідношень, які визначені вище згаданими правилами. Визначено схему підключення нейронної мережі для випадку коли сигнали статично незалежні.

Четвертий розділ присвячено розробці засобів інформаційного забезпечення системи безпеки.

В роботі розглядається інформаційна система, побудована на описах предметних областей, які описують інтерпретацію даних, що використовуються у всіх фрагментах системи розмежування доступу. Тому в даному розділі розглянуто основні інформаційні компоненти, які необхідні для вирішення задач інформаційного забезпечення системи безпеки.

Проведено аналіз: словників, що містять опис базових елементів предметних областей; системи синтаксичних правил формування описів інтерпретації базових елементів; системи семантичних параметрів, які характеризують особливості інтерпретації базових елементів і інших компонентів; системи семантичних правил, які регламентують способи побудови опису інтерпретації елемен-

тів, що використовуються при функціонуванні системи; системи правил перетворення описів компонентів системи.

Визначені умови виміру зміни рівня абстракції між двома описами предметних областей, умови виміру величини зміни рівня абстракції, умови зміни величини рівня абстракції між двома послідовно розглянутими описами предметної області.

Введено наступні семантичні параметри, які характеризують семантику інформаційних засобів системи, які допускають текстове відображення природною мовою: семантична значимість елемента; семантична ефективність елемента; суперечливість фрагмента; погодженість фрагментів у пропозиції; рівень конфліктності пропозицій. Розглянуто способи визначення їхніх числових значень.

На основі проведеного аналізу запропоновано структурну модель засобів інформаційного забезпечення системи розмежування доступу, завдяки якій формуються об'єднання множин ідентифікаторів предметної області користувачів та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень.

У п'ятому розділі розглянуті основні способи реалізації процесів адаптації при вирішенні задач захисту систем доступу.

Наведено визначення процесу адаптації, розглянута низка умов, які повинні виконуватися для того, щоб могли реалізовуватися дії в системі розмежування доступу, що класифікуються як дії процесів адаптації. Цими умовами є: умова зміни оцінки параметра в системі розмежування доступу; умова ініціалізації процесу адаптації, яка відповідає випадку модифікації граничних значень контрольованих параметрів і відноситься до випадку реалізації в системі розмежування доступу граничних алгоритмів контролю доступу. Важливою особливістю процесів адаптації системи розмежування доступу є зміна кількості параметрів, які реалізуються в системі. Показані цілі процесів адаптації, які розділені на: локальні цілі; інтегральні цілі; умовні або виділені цілі.

Показано що процеси адаптації, які приводять до певних змін в системі розмежування доступу, повинні реалізовуватися тільки в певні періоди часу функціонування. При цьому, можливі наступні режими реалізації процесів адаптації: автономний спосіб реалізації процесу адаптації системи розмежування доступу; сполучений спосіб реалізації процесів адаптації.

Запропоновано використання нейронних мереж для організації процесу адаптації. У межах нейронної мережі повинні формуватися спеціалізовані вузли, що реалізують функції: ініціації процесів адаптації; контролю часу функціонування;

аналізу умов завершення локального процесу адаптації; зв'язку фрагментів локальних процесів адаптації з інтегральними умовами узагальненого процесу адаптації в рамках всієї системі розмежування доступу. Запропоновано здійснювати вибір критеріїв адаптації базуюсь на поняттях теорії перспектив.

У межах розглянутого підходу, запропоновано модифікацію фрагменту нейронної мережі, що використовується для формування всієї мережі, відрізняється рядом особливостей від фрагментів традиційних мереж. Ці особливості полягають у наступному: класичний суматор, що є базовим елементом нейрона, має додаткові функціональні входи; крім суматора і вузла, який реалізує функцію активації, до складу нейрона входить блок оцінки критеріїв адаптації; до складу фрагмента нейронної мережі включається елемент збереження ознак історії розвитку відповідного фрагмента.

У шостому розділі описана апробація методів та моделей розмежування доступу до інформаційних ресурсів.

У висновках стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

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

Таким чином, усі положення, які винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів.

Наукова новизна одержаних автором результатів. У результаті виконання дисертаційної роботи набув подальшого розвитку науковий напрям, пов'язаний із розробленням методології створення систем розмежування доступу до розподілених інформаційних ресурсів. Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації такі:

– *удосконалено* структурну модель нейрона, в якій за рахунок інтегрування додаткового блоку пам'яті та блоку аналізу, що 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;

– *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;

– *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* 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 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 кіберсередовище 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.

Практичне значення отриманих результатів. Практична цінність роботи обумовлена тим, що використання запропонованих в ній моделей, методів, конкретних рішень і рекомендацій дозволяє створювати більш досконалі, порівняно з відомими, програмні засоби розмежування доступу, які можуть застосовуватися як розширювачі функціональних можливостей сучасних систем розмежування доступу до розподілених інформаційних ресурсів.

Розроблені в роботі моделі та методи адаптації засобів захисту, використовувались при реалізації систем контролю доступу, окремих механізмів захисту та побудові

моделей загроз та порушника, а також програм та методик випробувань при проведенні державних експертиз комплексних систем захисту за дорученням ДССЗЗІ СБУ України, зокрема: державної експертизи 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 експертизи 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.); державної експертизи 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.), тощо.

Результати дисертаційних досліджень впроваджено 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, Центральному науково-дослідному інституту озброєння та військової техніки Збройних Сил України, а також використовувалась в навчальному процесі Київського національного університету імені Тараса Шевченка, Національного авіаційного університету для підвищення підготовки фахівців з кібербезпеки.

Рекомендації щодо використання результатів дисертації. Цінність дисертаційної роботи для науки. Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної проблеми в теорії побудови та використання систем розмежування доступу. Змістовний аспект запропонованого рішення, який спрямований на узгодження продуктивності підсистем захисту та обробки інформації, що забезпечує розширення функціональних можливостей сучасних систем розмежування доступу, не був відомий раніше.

Запропоновані у роботі моделі, методи та алгоритми можуть бути використані при побудові систем розмежування доступу, як складових комплексних систем захисту від кібератак розподілених інформаційних ресурсів.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій, що захищаються. Наукові положення, викладені у дисертаційній роботі, є достатньо обґрунтованими за рахунок використання апробованих математичних методів та елементів теорій, а саме: методів математичного та комп'ютерного моделювання, семантичного аналізу та теорії інформації, теорії нейронів та нейронних

мереж, багатофакторного та системного аналізу.

Достовірність основних наукових результатів роботи підтверджується наведеною у 2–6 розділах роботи системою формальних методів і правил, що не містять принципових помилок, а також низкою прикладів і збіжністю результатів експериментальних досліджень, отриманих під час програмної реалізації алгоритмів забезпечення безпеки систем розмежування доступу.

Ідентичність змісту автореферату й основних положень дисертації. Автореферат дисертації за своїм змістом з необхідною повнотою відповідає викладеним у дисертаційній роботі результатам, в ньому ідентично відображено загальну характеристику, основній зміст та висновки роботи. Стиль викладення автореферату в цілому забезпечує повноту та доступність сприйняття. Наукові задачі дослідження та шляхи їх вирішення викладені чітко і лаконічно. З тексту зрозуміла наукова і практична значущість роботи та особистий внесок здобувача.

Відповідність теми і змісту дисертації паспорту спеціальності, за якою вона подана на захист. Тема дисертації та її зміст відповідають формулі й галузі досліджень відповідно до положень, що викладені у паспорті спеціальності 05.13.21 – «Системи захисту інформації».

Повнота викладення основних результатів дисертації та їх апробація. Основні результати дисертації достатньо повно відображені в 57 наукових працях, серед яких зокрема: 1 монографія, 4 статті у міжнародних рецензованих виданнях, що входять до бази даних Scopus, 7 наукових статей у вітчизняних наукових журналах, що входять в інші міжнародні наукометричні бази даних, 26 статті у наукових фахових журналах та збірниках України, 2 наукові статті у закордонних фахових наукових журналах, 2 патенти України. Основні положення дисертаційної роботи пройшли достатню апробацію на міжнародних науково-практичних конференціях та семінарах в Україні і закордоном та опубліковані у 15 матеріалах і тезах доповідей конференцій. В авторефераті і дисертації наведено дані щодо конкретного особистого вкладу здобувача.

Таким чином, кількість опублікувань результатів роботи та їх якість відповідає вимогам ВАК України до докторських дисертацій.

Зауваження щодо змісту і оформлення дисертації.

1. Аналізуючи поточний стан методів та моделей розмежування доступу до ресурсів інформаційних систем, автор відзначає, що « … однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом». Було б доцільно навести

кількісні оцінки продуктивності механізмів захисту, а не обмежуватися лише оцінкою продуктивності систем обробки розподілених інформаційних ресурсів.

У завершенні першого розділу хотілось побачити формалізовану постановку наукової проблеми, яка б логічно витікала з результатів аналізу досліджень за темою дисертації.

2. При побудові матриці доступу для різних типів паралельних систем обробки даних автор не дає оцінки розмірності матриці Md_{prj}. Доцільно було б навести конкретні приклади розрахунку міри близькості ξmpr, а не обмежуватися посиланням на структуру множин OtcAplInGR чи OtcAplOutGR.

3. Не зрозуміло, чому при вирішенні задач протидії атакам на систему керування доступом автор розглядає тільки сигнатурні методи. Також у відзначенні 3.1 має бути посилання на формулу (3.2) а не (3.1), як указано автором. Враховуючі вище згадане при доказі твердження 3.1 треба було вказати, що доказ є дійснім тільки у випадку сигнатурного аналізу атак на систему керування розмежуванням доступу.

4. На структурній схемі засобів інформаційного забезпечення системи розмежування доступу (рис. 4.1) між блоком семантичного словника SS та підсистемою інформаційного забезпечення предметної області користувача PIOPOn присутні стрілки зустрічного напряму. Нажаль з тексту дисертації незрозуміло навіщо це потрібне.

5. Процеси еволюційного розвитку S_C розглянуто автором на якісному рівні. Доцільно було б навести конкретні приклади процесів деградації, стабілізуючих процесів, катастрофічних процесів, а не обмежуватися їх формальним описом.

6. На сторінці 230, аналізуючи запропонований метод адаптації, наведено перелік необхідних для його реалізації параметрів. З тексту дисертації незрозуміло чи є цей перелік повним, але автор стверджує «Наведені параметри, які аналізуються, при реалізації процесів адаптації, не є параметрами самого процесу адаптації, а характеризують компоненти або дані SD, які піддаються змінам», тому доцільно було навести клас систем розмежування доступу для якого він є релевантним.

7. Незрозуміло, навіщо автором введено без визначення та обґрунтування новий термін ***кібердовкілля*** замість сталого ***кіберпростір***, який вже багато років використовується у наукових працях даної сфери досліджень. Під довкіллям, як правило, вважають навколишнє природне середовище – всі живі та неживі об'єкти, що *природно* існують на Землі або в деякій її частині.

Крім того, у авторефераті та дисертації зустрічаються стилістичні, синтаксичні та орфографічні помилки.

Загальна оцінка дисертації. Дисертаційна робота Давиденка Анатолія Миколайовича «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів» є завершеним науковим дослідженням, що характеризується єдністю змісту, містить нові наукові положення та обґрунтовані теоретичні результати, які підтверджено результатами проведених експериментів та відповідними документами щодо впровадження, та вирішують важливу науково-прикладну проблему, пов'язану з побудовою систем розмежування доступу, яка здатна адаптуватися до поточного стану кіберсередовища.

Усі результати, що виносяться на захист є достовірними та отримані автором особисто.

Вважаю, що за актуальністю обраної теми, обсягом і рівнем теоретичних і експериментальних досліджень, достовірністю та обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики. Дисертаційна робота задовольняє вимогам п.10,13,14 «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. №567 (із змінами, внесеними згідно з Постановами 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., №607 від 15.07.2020 р.), а її автор, **Давиденко Анатолій Миколайович**, ***заслуговує присудження наукового ступеню доктора технічних наук*** за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент -

професор кафедри кібербезпеки та математичного моделювання
Національного університету «Чернігівська політехніка»,
заслужений діяч науки і техніки України,
лауреат Державної премії України в галузі науки і техніки,
д. т. н., професор М. Шелест
«29» квітня 2021 року

Підпис Шелеста М. Ф. засвідчую
Ректор
О.О. Ковалевець