Голові спеціалізованої
вченої ради Д 64.050.14
Національного технічного університету
«Харківський політехнічний інститут»

м. Харків, Україна, вул. Кирпичова, 2,
61002

ВІДГУК

офіційного опонента – завідувача кафедри вищої математики Державного університету телекомунікацій доктора технічних наук, професора Барабаша Олега Володимировича на дисертацію Мартовицького Віталія Олександровича «Моделі та метод виявлення аномалій функціонування комп'ютерних систем на основі технології машинного навчання», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти»

Актуальність теми дисертації. Ефективність надання інформаційних послуг багато в чому визначається надійністю, інформаційної та функціональною безпекою комп'ютерних систем і мереж, що досягаються при реалізації комплексу програмно-апаратних засобів оперативного і тестового контролю, спрямованих на виявлення та мінімізацію наслідків кібернетичних впливів як навмисного, так і випадкового характеру. Для комп'ютерних систем з метою підвищення готовності до безпечного виконання запитів і мінімізації небезпечних станів порушення захищеності, що істотно знижують рентабельність надання інформаційних послуг, виникає потреба в створені системи моніторингу стану функціонування комп'ютерних систем для виявлення порушень захищеності в результаті внутрішніх та зовнішніх кібернетичних впливів.

Система моніторингу не тільки змінює уявлення про систему експлуатації, переходячи від збору даних параметрів окремих станцій до параметрів експлуатації всієї мережі, а також автоматизує безліч рутинних процесів зі збору та обробки параметрів розподіленої комп'ютерної системи.

Таким чином, актуальним є *наукове завдання*, що полягає в розробці моделей та методів виявлення аномалій функціонування комп'ютерних

систем на основі технології машинного навчання. Вирішенню даного наукового завдання і присвячена дисертаційна робота Мартовицького В.О.

Зв'язок роботи з науковими програмами та планами. Дисертаційна робота виконувалась у відповідності до Плану наукової та науково-технічної діяльності Харківського національного університету радіоелектроніки. Зокрема, у дисертації використані результати проведених автором досліджень в рамках науково-дослідних робіт: " Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання ", (номер державної реєстрації 0117U003916), " Методи, системи та засоби криптографічного захисту інформації з гарантованим рівнем стійкості та підвищеною швидкодією " (номер державної реєстрації 0115U002431), " Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання " (номер державної реєстрації 0118U000832) .

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації. Викладені в дисертаційній роботі наукові положення є повністю обґрунтованими, а відповідність запропонованих автором теоретичних положень та математичних моделей підтверджується відповідними даними проведених експериментів та підтверджують результати запропонованих моделей та методу. Отримані результатів моделювання відповідають теоретичним висновкам роботи і повністю підтверджують їх, коректно застосовані методи теорії множин, методи оптимізації, теорії складних систем та теорії багатоагентних систем.

Достовірність одержаних в роботі результатів підтверджується обґрунтованими теоретичними твердженнями та оцінку ефективності запропонованої системи моніторингу для виявлення аномального поведінки мережного трафіку на основі множини параметрів мережевих з'єднань *{NW}*, що реалізується шляхом аналізу вхідного трафіку за допомогою ансамблю класифікаторів. Де було проведено експериментальне дослідження ефективності роботи запропонованої моделі виявлення аномальної поведінки, результати якого наведені в табл. 4.1 (розділ 4, п. 3).

Одержані у роботі результати мають чітке наукове тлумачення і не суперечать відомим даним.

Наукова новизна одержаних результатів:

1) Вперше запропоновано модель класифікації стану системи, яка ґрунтується на структурному представлені показників функціональності розподілених комп'ютерних систем, що дозволяє виділити множину станів у залежності від функціональних завдань, розмежувати процеси цільового функціонування системи та інтерфейсні процеси взаємодії з мережною інфраструктурою та використовувати їх у методах інтелектуального аналізу для виявлення аномалій функціонування розподілених комп'ютерних систем.

2) Отримала подальшого розвитку мультиагентна модель системи збору і зберігання інформації, що побудована на основі агентів, метою яких є надання користувачеві або інформаційній системі більш високого рівня інформації про стан мережної інфраструктури, отриманої в результаті збору та інтелектуальної обробки параметрів, що дозволило зменшити навантаження на мережу за рахунок застосування запропонованого протоколу обміну інформацією між агентами.

3) Удосконалено метод класифікації стану мережі на основі статистичних параметрів за рахунок рівномірної вибірки об'єктів із поверненням для формування навчальних вибірок, що дозволяє адаптувати процес навчання ансамбля класифікаторів до розмірів навчальної вибірки.

Практичне значення одержаних автором наукових результатів.

Викладені у роботі запропоновано модель класифікації стану системи, яка ґрунтується на структурному представлені показників функціональності розподілених комп'ютерних систем, удосконалено мультиагентну модель системи збору і зберігання інформації, що побудована на основі агентів, що забезпечує роботу з множиною різнорідних джерел, шляхом їх інтегрування для отримання більш повного збору інформації та метод класифікації стану мережі на основі статистичних параметрів, який дозволяє виявляти кібернетичні впливи на мережу, що є важливим теоретичним внеском у наукову спеціальність 05.13.05 – «Комп'ютерні системи та компоненти». Отримані наукові результати мають важливе практичне значення, що визначається можливістю виявлення аномалій функціонування в інформаційно-комунікаційній мережі розподілених комп'ютерних систем під час внутрішніх та зовнішніх кібернетичких впливів на систему.

Основні результати дисертаційної роботи були апробовані:

– при розробці перспективних систем передачі даних в «Центральне конструкторське бюро «ПРОТОН»»;

– у ході стратегічних командно-штабних навчань «Непохитна стійкість-2017» Розрахунково-аналітичним центром Збройних Сил України;

– в навчальному процесі Харківського національного університету радіоелектроніки при проведенні лабораторних робіт з дисципліни «Технології виявлення загроз в комп'ютерних мережах» для студентів усіх форм навчання спеціальності 123 «Комп'ютерна інженерія».

Подальші дослідження доцільно спрямувати на вдосконалення та покращення методу оцінки стану обчислювального вузла та стану запущених завдань в комп'ютерній системі.

Повнота викладення основних результатів дисертації в публікаціях.

Основні результати дисертаційної роботи з необхідною повнотою відображені в 13 наукових працях, з них: 6 статей у наукових фахових виданнях України, включених до міжнародних наукометричних баз (з них 2 внесені до міжнародної наукометричної бази даних SCOPUS), 7 публікацій у матеріалах міжнародних наукових конференцій (з них 1 внесена до міжнародної наукометричної бази даних SCOPUS).

Оцінка змісту дисертації, відповідність встановленим вимогам до оформлення. Дисертація Мартовицького В.О. являє собою одноосібно написану кваліфікаційну наукову працю, яка містить сукупність результатів та наукових положень, поданих автором для публічного захисту, має достатній ступінь завершеності, структурованість, логічну внутрішню цілісність і свідчить про наявний особистий внесок автора у науку.

Дисертація та автореферат написані грамотною науково-технічною мовою з використанням загальноприйнятих наукових термінів, визначень та понять, достатньо ясно та зрозуміло. Матеріали досліджень викладені логічно та послідовно. Стиль їх викладення не суперечить методології наукових досліджень. Висновки достатньо конкретні та відображають основні результати досліджень.

Дисертацію достатньо добре ілюстровано. Винесені на захист наукові результати викладено вичерпно. Використані в роботі терміни, визначення та поняття відповідають діючим Державним стандартам України.

Відповідність змісту автореферату основним положенням дисертації. За структурою, змістом та оформленням автореферат відповідає встановленим вимогам та загальноприйнятому стилю його викладення. Зміст автореферату ідентичний основним положенням дисертації, у ньому достатньо повно і точно відображені основні результати досліджень, що детально подані в дисертації.

Недоліки та зауваження.

1. Розділ 1 дисертації має назву «Аналіз сучасного стану підходів виявлення аномалій в комп'ютерних системах», але саме аномалій стосується лише підрозділ 1.3.2, до того ж стосовно лише атак у відповідних системах виявлення. Окрім цього, у розділі 1 автор намагався виконати аналіз критеріїв порівняння методів виявлення атак. На жаль автор обмежився множиною існуючих критеріїв оцінки і не запропонував комплексного показника оцінки ефективності.

2. У розділі 2 дисертації виконано розробку моделі моніторингу аномалій та наведено структуру моделі моніторингу розподіленої комп'ютерної системи кластерної архітектури для виявлення аномальних подій (рис. 2.12). Однак, в дисертації під час опису структури даної моделі не вистачає відомостей щодо співвідношення наведених елементів, а також характеру взаємозв'язків та множин параметрів, що передаються між ними. Також невідомим залишається зв'язок між «параметри мережі» (рис. 2.12) та «множина параметрів мережних з'єднань» (вираз 2.2), що є описом до структури моделі.

3. Виходячи із назв підрозділів розділу 3, автор розробляв метод класифікації аномалій (підрозділ 3.2 «Метод до класифікації стану мережі на основі статистичних параметрів для виявлення аномалії в інформаційній структурі обчислювальної системи»). При цьому в підрозділі 3.2.2 «Метод класифікації стану мережі на основі модифікованого алгоритму стекинга» автор докладно зосередився на наведені алгоритмів, що привело до ускладнення системного розуміння методу. Доцільно було б навести системне представлення методу, вхідні та вихідні параметри методу, а після цього навести відповідні алгоритми.

4. Із опису запропонованого автором модифікованого алгоритму стекінга (крок 2) незрозуміло, як отримати розбиття множини X на K підмножин, що пересікаються.

5. У розділі 4 дисертації автор декларує технологію мониторингу стану функціонування розподілених інформаційних систем. При цьому, термін «Технологія» присутнє лише у назві розділу. В тексті розділу відсутні будь-які пояснення. Експериментальні результати у підрозділі 4.3 доцільно було б навести у графічній формі, а також навести кількісні оцінки аномальності трафіку.

Разом із тим, вказані недоліки не знижують цінності та практичного значення одержаних в дисертаційній роботі наукових результатів і, внаслідок цього, її позитивну оцінку в цілому.

Висновок. Дисертаційна робота Мартовицького В.О. є кваліфікаційною науковою працею, яка містить нові науково обґрунтовані результати проведених автором досліджень, що в сукупності вирішують актуальне наукове завдання, сутність якого полягає в розробці моделей та методів виявлення аномалій функціонування комп'ютерних систем на основі технології машинного навчання. Дисертаційна робота має зазначену наукову новизну та практичну значимість, відповідає вимогам п.п. 9, 11, 12 «Порядку присудження наукових ступенів», які висуваються до кандидатських дисертацій, а її автор, Мартовицький Віталій Олександрович, заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти».

Завідувач кафедри вищої математики
Державного університету телекомунікацій
доктор технічних наук, професор О.В. Барабаш
"24" вересня 2019 року

Підпис професора Барабаша О.В. засвідчую
Учений секретар вченої ради
Державного університету телекомунікацій О.В. Попов