В І Д Г У К
ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Балакіна Сергія В’ячеславовича
"Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп’ютерній мережі",
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми дисертаційної роботи.

Технічний прогрес зумовив ситуацію, коли більшість інформації не тільки на підприємствах, але і у пересічних користувачів, зберігається і оброблюється на віддалених обчислювальних станціях. Для більш зручної роботи користувачів, оперативного обміну, гнучкого оброблення та зберігання інформації в інфраструктуру підприємств і місць проживання громадян вбудовуються комп'ютерні мережі, які у даний час стали невід'ємною частиною різних сфер діяльності та відпочинку людини. Як наслідок, виникає актуальна проблема захисту таких комп'ютерних мереж, що в свою чергу передбачає розроблення відповідних алгоритмів, методів та засобів виявлення несанкціонованої діяльності у мережах.

Розроблення нових алгоритмів, методів, програмних і апаратних засобів не тільки виявлення несанкціонованих дій в мережах, але і підвищення ефективності виявлення таких дій є актуальною задачею сьогодення. Відповідно, дисертаційні дослідження автора, направленні на вирішення такої науково-прикладної задачі, як підвищення достовірності ідентифікації несанкціонованих дій і атак в комп’ютерній мережі, носять надзвичайно актуальний характер.

Також про актуальність обраної теми можна судити з огляду на участь здобувача у науково-дослідних роботах кафедри комп'ютерних систем та мереж Національного авіаційного університету: НДР № 682-ДБ13 за темою «Розроблення теорії, методів та технологій оптимального управління гарантоздатною комп'ютерною мережею» (номер державної реєстрації 0113U000028), кафедральна НДР № 17/09.01.04 за темою «Системна інтеграція науково-навчального забезпечення другого рівня підготовки фахівців спеціальності 123 – комп’ютерна інженерія».

Оцінка обґрунтованості наукових положень дисертації, їх достовірності та новизни.

Основні наукові положення, результати та висновки, що входять до дисертації, отримані здобувачем самостійно, є новими, достатньо обґрунтованими та підтверджуються даними комп'ютерних експериментів і

апробацією основних положень на міжнародних конференціях, а також впровадженням у виробничу діяльність підприємств для підвищення ефективності діагностування несанкціонованих дій в комп’ютерній мережі.

Достовірність наукових положень, висновків і результатів, отриманих здобувачем, обумовлена коректними та доцільним використанням математичного апарату, методології застосування статистичних методів для оброблення результатів комп'ютерних експериментів при розробленні та оцінці ефективності запропонованих методів.

Наукова новизна результатів дисертації.

Основні наукові положення, висновки та результати, отримані автором і представлені в дисертаційній роботі, прямо пов'язані з метою досліджень та задачами, що вирішуються для її досягнення. До найважливіших наукових результатів належать:

1) Удосконалено модель виявлення несанкціонованих дій в комп'ютерній мережі, в якій розпізнавання відбувається за допомогою аналізу поведінкових ознак, що дає можливість автономно розпізнавати невідомі вторгнення і мінімізувати помилкові спрацьовування;
2) Отримав подальший розвиток метод виявлення вторгнень у комп'ютерні мережі, який базується на використанні операторів штучних імунних мереж для побудови структурованої мережі антитіл, що зі свого боку позитивно впливає на швидкодію і достовірність автономного виявлення як відомих, так і нових вторгнень;
3) Запропоновано модель виявлення вторгнень в комп’ютерній мережі засобами інспектування стану системи на виникнення аномальної поведінки, використовуючи дерево діагностування, що дозволяє відстежувати активність системи й симптомізувати дії користувача, а шляхом введення нових елементів і діапазонів роботи досягається підвищення достовірності виявлення атак;
4) Вперше розроблено метод розпізнавання несанкціонованих дій засобами діагностування на основі операторів теорії Демпстера-Шафера, де на відміну від існуючих пропонується відстежувати часові фрагменти на заданих діапазонах часу і з них, за допомогою операторів злиття, формувати діагнози, за рахунок чого досягатиметься можливість автономного виявлення невідомих системі несанкціонованих дій.

Наукове та практичне значення результатів дисертаційної роботи.

Представлена в роботі сукупність моделей та методів, направлених на виявлення несанкціонованих дій в комп'ютерних мережах за рахунок

розширення можливостей по їх обробці, є важливим теоретичним внеском у наукову спеціальність 05.13.05 – комп'ютерні системи та компоненти відповідно до напрямків досліджень №№ 1 та 6, сформульованих у її паспорті.

Практичне значення отриманих результатів полягає у доведенні наукових результатів до можливості практичного використання у вигляді прикладних програмних засобів, що дадуть можливість підвищити ефективність виявлення несанкціонованих дій в комп'ютерній мережі для забезпечення роботи засобів керування мережею та відповідних систем операційної підтримки. Крім того, наукові результати дисертаційного дослідження використані:

– для підвищення ефективності діагностування несанкціонованих дій в комп'ютерній мережі ТОВ "Газбудсервіс" (акт про впровадження від 26.06.2017 р.);

– для аналізу несанкціонованих дійв комп'ютерній мережі ДП «Короп-пласт» (акт про впровадження від 26.06.2017 р.);

– в навчальному процесі кафедри комп'ютерних систем та мереж Національного авіаційного університету.

Додатковою перевагою запропонованих методів є наявність документів про захист інтелектуальної власності (патенти на корисну модель України № 110330 та № 123634).

Оцінка змісту дисертації.

Дисертаційна робота складається з анотації, вступу, 4 розділів, висновків, списку використаних джерел із 146 найменувань на 15 сторінках та 2 додатків на 10 сторінках. Загальний обсяг дисертації становить 153 сторінки, з них 128 сторінок основного тексту, 22 рисунки та 7 таблиць.

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано мету та завдання дослідження, визначено наукову новизну та практичне значення отриманих результатів, подано інформацію щодо апробацій та публікацій результатів дисертаційної роботи із зазначенням особистого внеску автора у роботах, виконаних у співавторстві.

Перший розділ присвячено огляду сучасного стану в області засобів і методів виявлення несанкціонованих дій і атак в комп'ютерних мережах, аналізу підходів діагностування несанкціонованої активності в комп'ютерній мережі, аналізу і порівнянню засобів і методів підвищення ефективності виявлення несанкціонованих дій і атак в мережах. Результати аналізу та детального огляду дозволили обґрунтувати актуальність досліджень.

Другий розділ присвячено моделі аналізу несанкціонованих дій, яка, застосовуючи поведінковий аналіз даних, може виявити небажані вторгнення

в комп'ютерну мережу. Модель розширено новою функційністю, що дає можливість мінімізувати помилкові спрацювання без потенційного зниження швидкодії системи. Під час виявлення несанкціонованих дій застосовано такі ознаки, які при певних умовах найкраще характеризують події, пов'язані з вторгненнями.

Аналіз моделей штучних імунних мереж дозволив виділити ту модель, яка на основі взаємодії антитіл з різними ступенями подібності дає можливість виявляти вторгнення. Розглянуто та проаналізовано основні імунні оператори, а також обґрунтовано введення додаткових параметрів до моделі для пришвидшення роботи та підвищення загальної продуктивності. Описано підхід до процесу навчання та розпізнавання несанкціонованих дій на основі штучної імунної мережі.

В **третьому розділі** подано модель виявлення несанкціонованих дій, що у своїй основі містить діагностування вторгнень в комп'ютерній мережі та не вимагає постійного оновлення сигнатур. Для моделювання було обрано та обґрунтовано застосування операторів теорії доказів Демпстера–Шейфера для формування відповідного рішення про наявність або відсутність несанкціонованих дій в мережі. Це зумовило виділення тих ознак несанкціонованих дій, які певним чином однозначно характеризують дії зловмисника чи певну атаку. На основі детального аналізу математичних моделей діагностування і алгоритмів виявлення змін визначено параметри процесу діагностування, зокрема алгоритми контролю часових фрагментів і формування даних для визначення симптомів і сигнатур вторгнень. Наведено та обґрунтовано необхідність об'єднання кількох симптомів для отримання точнішого діагнозу.

У **четвертому розділі** автор основну увагу зосередив на питаннях реалізації інструментальних засобів і проведенні експериментальних перевірок результатів досліджень. Зокрема, вибрано інструменти для моделювання і впровадження запропонованих методів з метою підвищення ефективності виявлення несанкціонованих дій і атак в комп'ютерних мережах. Виконано дослідження ефективності методу виявлення несанкціонованих дій і атак в комп'ютерній мережі на основі штучних імунних систем і діагностування.

Висновки по роботі повністю висвітлюють отримані результати та за своїм рівнем відповідають вимогам, які висуваються до результатів дисертаційного дослідження.

Додатки до роботи містять акти про впровадження та використання результатів дисертаційного дослідження.

Повнота викладу основних результатів в опублікованих працях.

Автором опубліковано 14 наукових праць (з них 4 – належать особисто автору), в тому числі 7 статей у наукових виданнях України, 5 праць у збірниках міжнародних та всеукраїнських наукових конференцій, 2 патенти України на корисну модель. Повний перелік опублікованих праць наведено здобувачем у авторефераті та дисертації.

Публікації та автореферат повністю відображають зміст дисертаційної роботи. Аналіз публікацій автора дає змогу зробити висновок про повноту викладу основних наукових положень його дисертаційного дослідження.

Основні результати дисертаційної роботи доповідалися на міжнародних конференціях та друкувалися у їх тезах.

Оцінка оформлення дисертації та автореферату.

Робота написана коректною мовою із використанням сучасної науково-технічної термінології. Стиль викладу матеріалів досліджень, наукових положень і рекомендацій забезпечує їх адекватне і належне сприйняття.

Оформлення автореферату за своїм обсягом, структурою та змістом відповідає чинним вимогам. Зміст автореферату ідентичний змісту основних положень дисертації, автореферат адекватно відображає результати дисертації.

Зауваження до дисертаційної роботи.

При цілком позитивній оцінці роботи, вважаю за необхідне зробити такі зауваження:

– до викладеного змісту:

1) В аналізі слід було навести і порівняти існуючі в світі комерційні та open-source рішення (а не тільки методи і алгоритми) для захисту від атак, зокрема synflood і slowloris, зазначених автором в дисертаційному дослідженні, вказати переваги та недоліки таких рішень.

2) Опису предметної області та відповідних моделей приділено забагато місця. А ось опису власних результатів треба було приділити більше місця, зокрема детальному опису практичної реалізації розроблених методів та результатам оцінювання їхньої ефективності.

3) Зазначені автором в підрозділі 4.4 критерії оцінювання ефективності, як відомо, є дуже чутливими до розміру або складності вхідних даних. Саме тому такі оцінювання проводять на різних за складністю або розміром наборах даних, а середні значення показників ефективності розраховують за результатами багатократних серій експериментів. В роботі автором не чітко описано набори вхідних даних та кількість проведених циклів експериментів.

4) Твердження в розділі 4, що розроблені автором методи перевершують використані у тестуванні антивіруси, є недостатньо обґрунтованими, оскільки не зазначено достатньо вхідних даних, що їх слід було використати або що їх було використано під час комп'ютерного експерименту, зокрема: налаштувань програмних продуктів, апаратних засобів, мережевих протоколів і робочого оточення. Наприклад, які результати експерименту при виявленні атак типу Synflood буде отримано при застосуванні протоколу SCTP і чи взагалі доцільно проводити такий експеримент?

5) В 3.1.5 запропоновано для використання 2 оператори злиття, але необґрунтовано критерії та доцільність їх вибору, не вказано їхні переваги над іншими операторами.

6) В 3.1.7 запропоновано алгоритм "кумулятивної суми", який правильно називається CUSUM, а не CSM.

7) Для чого в алгоритмі функціонування запропонованої системи (рис. 3.3) порівнюють наперед визначені масиви з нормальними і аномальними станами? Слід порівнювати стан системи в конкретний момент часу з цими двома масивами.

8) Фраза в авторефераті та анотації дисертації "Дана робота описує один із варіантів недоліків захисту від несанкціонованих дій у комп’ютерні мережі, який можна впровадити в уже існуючі системи" є некоректною, оскільки робота присвячена одному із варіантів захисту, який можна впровадити.

9) Замість терміну "Штучні нейронні системи" краще використовувати "Штучні нейронні мережі", як більш вживаний і прийнятий у відповідній спільноті.

10) В 3.1.7 при описі алгоритму CUSUM познака μ вказується як середнє відхилення, як "нормальне" середнє відхилення, як очікуване значення і як середнє значення.

– до оформлення роботи:

11) Для уніфікації викладення матеріалу дисертації у розділ 4 слід також було додати висновки до розділу.

12) В авторефераті та дисертації наявні граматичні та орфографічні помилки.

Однак, вказані недоліки не є суттєвими, і не впливають на позитивну оцінку роботи.

Загальний висновок.

В цілому дисертаційна робота Балакіна Сергія В'ячеславовича є завершеним, цілісним, самостійно виконаним науковим дослідженням, містить елементи наукової новизни і важливі практичні результати, які є суттєвими при вирішенні важливої науково-прикладної задачі – розробці моделей і методів підвищення достовірності ідентифікації несанкціонованих дій і атак в комп'ютерній мережі.

Подана робота за своїм змістом, рівнем наукових викладок, системністю досліджень, використаним математичним апаратом та проведеним комп'ютерним експериментом відповідає рівню дисертацій на здобуття наукового ступеня кандидата технічних наук. Вибрану тему дисертації належним чином розкрито, мету досягнуто, завдання в цілому виконані. Тема дисертації відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти, зокрема пунктам 1 та 6 напрямів досліджень за цією спеціальністю.

Вважаю, що дисертаційна робота "Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп'ютерній мережі" відповідає як обраній спеціальності, так і встановленим вимогам до кандидатських дисертацій, зокрема п.п. 9, 11–14 "Порядку присудження наукових ступенів", які ставляться до дисертаційних робіт, поданих на здобуття наукового ступеня кандидата технічних наук, а її автор **Балакін Сергій В'ячеславовича** заслуговує присудження наукового ступеня **кандидата технічних наук** за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент:
провідний науковий співробітник
відділу перетворювачів форми інформації
Інституту кібернетики
ім. В.М. Глушкова НАН України
кандидат технічних наук,
старший науковий співробітник _____ І.Б. Галелюка

Підпис пр.н.с., к.т.н. Галелюки І.Б. засвідчую:

учений секретар Інституту кібернетики
ім. В.М.Глушкова НАНУ, д.ф.-м.н. _____ С.В. Єршов