Голові спеціалізованої вченої ради
Д 26.861.06 Державного університету
телекомунікацій

вул.Солом'янська, 7, м. Київ

ВІДГУК

офіційного опонента

доктора технічних наук, старшого наукового співробітника, начальника кафедри захисту інформації та кіберзахисту Військового інституту телекомунікацій та інформатизації імені Героїв Крут,
Міністерство оборони України,
Чевардіна Владислава Євгенійовича
на дисертаційну роботу Радівілової Тамари Анатоліївни на тему
«Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками»
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – Системи захисту інформації

Актуальність теми дисертації та вирішуваної науково-прикладної проблеми.

Критично важливим ресурсом в рамках держави, організації, індивідуума, якому необхідно забезпечити безпеку, надійність та своєчасність передачі, є інформація, яка циркулює в комп'ютерних системах різного призначення. Ці системи є невід'ємною частиною сучасного життя. Можливість несанкціонованого впливу на інформацію розглядається як пряма загроза інтересам як держави, так і індивідуума. Тому системи захисту інформації

(антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень тощо), стали невід'ємною частиною інформаційно-комунікаційних мереж. Однак ці мережні системи недосконалі й мають множину проблем, пов'язаних з їх побудовою, розгортанням управлінням, масштабуванням і підтримкою. Всі зміни в конфігурації мережі та в операційних системах її елементів повинні враховуватись в системах виявлення вторгнень та неналежна якість обслуговування інформаційних потоків призводить до появи вразливостей в безпеці систем. Тобто, механізми забезпечення безпеки та якості обслуговування залежать один від одного та властивостей вхідних інформаційних потоків. Таким чином дисертаційна робота Радівілової Тамари Анатоліївни присвячена вирішенню науково-прикладної проблеми щодо розробки моделей та методів забезпечення безпеки та якості обслуговування в комп'ютерних системах з урахуванням самоподібних властивостей інформаційних потоків в умовах наявності вторгнень та кібератак є актуальною.

Загальна характеристика дисертаційної роботи. Дисертаційна робота складається з анотації, вступу, шести розділів, загальних висновків, додатків, списку використаних джерел (381 найменування). Загальний обсяг роботи становить 403 сторінки, у тому числі 300 сторінок основного тексту. Зміст роботи відповідає сформульованій науково-прикладній проблемі. Робота має чітку послідовність постановки задач, а їх рішення є суттю та змістом виконаних досліджень, що відповідають паспорту спеціальності 05.13.21 – Системи захисту інформації.

Достовірність наукових положень, висновків і рекомендацій, отриманих в дисертації, підтверджено результатами проведених досліджень, коректністю застосування математичного апарату, можливих обмежень і припущень при розробленні моделей та методів забезпечення безпеки та управління інформаційними потоками із самоподібними властивостями в умовах кібератак. Додатково достовірність отриманих наукових результатів

експериментально підтверджено їх використанням у діяльності Харківського державного регіонального науково-технічного центру з питань технічного захисту інформації (акт впровадження від 11.12.2019), АТ БАНКОМЗВ'ЯЗОК (акт впровадження від 25.06.2019), при створені програмного комплекса ідентифікації вторгнень, та у навчальному процесі в Харківському національному університеті радіоелектроніки (акт впровадження від 16.04.2019), що підтверджується відповідними актами впровадження.

До **основних нових наукових результатів**, які отримані в дисертаційній роботі, можна віднести такі:

Вперше розроблено концепцію забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками, які працюють в умовах вторгнень та кібератак. Дана концепція базується на моделі розподіленої комп'ютерної системи, яка включає компоненти забезпечення безпеки та управління самоподібними інформаційними потоками, у поєднанні з методом забезпечення безпеки в ході динамічного балансування навантаження в комп'ютерних системах та в системах виявлення вторгнень з урахуванням мультифрактальних властивостей трафіка; методом забезпечення безпечної маршрутизації під час передачі самоподібного трафіка; методом виявлення вторгнень, що базується на використанні аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів. Реалізація концепції у програмному комплексі дозволяє гарантовано забезпечити доступність, конфіденційність та якість обслуговування в комп'ютерних системах із самоподібними інформаційними потоками під час вторгнень та кібератак.

Вперше розроблено метод динамічного балансування трафіка, який базується на моделі мережної системи виявлення вторгнень, що враховує мультифрактальні властивості трафіка та обмеження на час обслуговування різних класів трафіка. Реалізація методу динамічного балансування трафіка

зменшує час обробки інформаційних потоків з метою виявлення вторгнень та їх розподілення на менш завантажені ресурси системи.

Вперше розроблено комплексний метод виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Це дозволяє підвищити як достовірність, так і точність виявлення вторгнень, та уможливлює раннє виявлення вторгнень в широкому діапазоні кібератак на систему.

Набули подальшого розвитку методи виявлення вторгнень на основі аналізу сигнатур, який враховує дані глибокого аналізу пакетів та рейтингування бази сигнатур; аналізу ентропії пакетів, який базується на розрахунку умовної ентропії та статистичних характеристиках даних пакетів; на основі машинного навчання, які базуються на мультифрактальних та рекурентних характеристиках трафіка, що дозволяє скоротити час виявлення вторгнень і збільшує швидкість та точність виявлення вторгнень, уможливлює виявлення вторгнення при низькому рівні кібератак.

Вперше розроблено метод забезпечення безпечної маршрутизації під час передачі самоподібного трафіка, який базується на мультифрактальних властивостях трафіка та параметрах якості обслуговування різнопріоритетного трафіка, що дозволяє зменшити завантаженість ресурсів комп'ютерної системи за рахунок спрямування безпечних інформаційних потоків різного класу обслуговування на безпечні і менш завантажені ресурси.

Набули подальшого розвитку методи виявлення вторгнень на основі аналізу сигнатур, який враховує дані глибокого аналізу пакетів та рейтингування бази сигнатур; аналізу ентропії пакетів, який базується на розрахунку умовної ентропії та статистичних характеристиках даних пакетів; на основі машинного навчання, які базуються на мультифрактальних та рекурентних характеристиках трафіка, що дозволяє скоротити час виявлення вторгнень і збільшує швидкість та

точність виявлення вторгнень, уможливлює виявлення вторгнення при низькому рівні кібератак.

Теоретична і наукова цінність та практичне значення одержаних атором наукових результатів. Проведений аналіз показав, що результати дісертаційної роботи Радівілової Т.А. відображено у науково-дослідних роботах Харківського національного університету радіоелектроніки «Автоматизована оптична інформаційно-вимірювальна система для полігонних випробувань керованих та некерованих ракет, артилерійських і реактивних снарядів» (Міністерства освіти і науки України номер державної реєстрації ДР №01190U001405), угоди про надання гранту: S-LMAQM-18-GR-2301 Державним департаментом США 2019 р. «Українська обізнаність у сфері кібербезпеки: підтримка низки тренінгів щодо розвитку кіберзахисту та підвищення обізнаності в Україні»; проекту ТЕМПУС 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR «Навчання експертів наступного покоління з кібербезпеки: нова визнана ЄС програма магістра» ENGENSEC.

Теоретична і наукова цінність отриманих автором результатів полягає в тому, що вони в сукупності є внеском у вирішення проблеми забезпечення доступності, конфіденційності та якості обслуговування в комп'ютерних системах з урахуванням самоподібних властивостей інформаційних потоків в умовах наявності вторгнень та кібератак. Практичне значення отриманих результатів формує підґрунтя для розробки і впровадження ефективних засобів виявлення кібератак у комп'ютерних системах, балансування самоподібними інформаційними потоками в мережних СВВ та управління трафіком у маршрутизаторах і балансувальниках для забезпечення конфіденційності, цілісності, доступності та якості обслуговування в умовах неоднорідних потоків та обмеженості ресурсів комп'ютерних систем. Реалізація запропонованих моделей та методів дозволяє створити програмну реалізацію комплексного методу виявлення кібератак у комп'ютерній системі, яку засновано на

поведінковому, сигнатурному та ентропійному аналізі самоподібних інформаційних потоків; створити прикладне програмне забезпечення для балансування навантаження вузлів мережної системи виявлення вторгнень; підвищити точність, швидкість, своєчасність ідентифікації кібератак, захищеність інформаційних ресурсів та якість обслуговування в комп'ютерних системах та знизити завантаження вузлів.

Оцінка мови та стилю викладання дисертації та автореферату. Дисертація й автореферат написані достатньо грамотно. Стиль викладення матеріалів дослідження, а саме – наукових положень, висновків і рекомендацій, відповідає вимогам ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила офрмлення» й Вимогам до офрмлення дисертацій, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. №40 та у цілому забезпечує доступність їх сприйняття.

Зміст автореферату повністю відображає основні результати роботи, які приведені в дисертації. В ньому чітко і лаконічно викладені часткові наукові завдання дослідження та шляхи їх вирішення. З тексту зрозуміла наукова і практична значущість роботи, особистий внесок здобувача.

Повнота викладення наукових результатів дисертації в опублікованих роботах. Основні положення та висновки дисертаційної роботи опубліковано в 67 наукових працях. Серед них 36 статті, серед яких 20 статей у наукових фахових виданнях України та 16 статей у закордонних фахових виданнях, з яких чотири статті індексуються наукометричними базами Scopus / Web of Science. Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації.

Дискусійні положення та зауваження щодо дисертаційного дослідження:

1. В дисертаційній роботі припущено багато помилок в оформленні елементів роботи. Так, в ході тексту навіть в одному абзаці автором допускається

повторення тексту (стор. 59), в роботі зустрічаються скорочення, які не є загальноприйнятими і які не перелічені в списку скорочень та не розкриті в тексті, на стор. 88 в формулі 1.1 зустрічається позначення Low{} – значення якого не визначено, під час роздрукування тексту роботи автор не звернув увагу на нечитаємість деяких символів на ПК на якому здійснювався друк (стор. 87, 88, 91, …), в тексті дисертації двічі зустрічається викладення мети та завдань дисертаційного дослідження, не узгоджені закінчення слів і тому не зрозумілі речення при розгляді функціонування CoPP (стор. 132, пп.4, 5), в формулі 2.1 (стор. 142) не визначено параметр *f*, він також не зустрічався раніше, деякі матеріали викладені в дисертації взяті зі статей автора, але під час переносу не виплавлено самопосилання на "статтю" (стор. 148).

2. З постановки науково-прикладної проблеми (стор. 38) та мети досліджень (стор. 40) не зрозуміло який обрано об'єкт дослідження, для якого "забезпечення безпеки" підвищується, а також чому в роботі до "безпеки" відносяться тільки "доступність" та "конфіденційність, без "цілісності"?

3. Виходячи зі сформульованих практичних значень і зазначених наукових результатів не зрозуміло яким чином отримані результати впливають на конфіденційність, і чому саме конфіденційність забезпечується?

4. У вступі застосовується не зрозуміле словосполучення без визначення значення "контроль заборони доступу", але зовсім не використовується загальноприйняте поняття "контроль доступу";

5. Не зрозуміло чому в постановці завдань використовується минулий час? Задачі на момент постановки мети вже були вирішені? Тоді втрачається новизна (стор. 40).

6. В ході переліку атак проти систем виявлення вторгнень не зрозуміле використання пунктів:

- Можливість обробки трафіка з високою інтенсивністю трафіка.
- Можливість співвідносити події.

- Здатність виявляти ніколи раніше не бачені напади, атаки нульового дня".

- Можливість ідентифікації атак.

- Можливість визначення успіху в атаці.

- Перевірка ємності для мережних систем виявлення атак.

- Продуктивність. (В тексті пункту загалі про системи виявлення атак не йдеться).

7. Не зрозуміло чому автор у пп. 1.1 "Аналіз параметрів безпеки та якості обслуговування мережі" із засобів захисту мережі розглядає лише "системи виявлення вторгнень", а не бере до уваги, наприклад, "міжмережні екрани", які на продуктивність мережі здійснюють більший вплив, або "систем запобігання вторгнень" результатом роботи яких при хибнопозитивному спрацюванні може бути блокування трафіку;

8. Автором невдало використовується словосполучення "інформаційна атака" при розгляді здійснення впливу на маршрутизатори. Вважаю, що краще у випадку атак на телекомунікаційне обладнання використовувати термін "кібератака" або просто "атака" (стор. 57);

9. Вважаю не доречним використовувати фразу ""найнебезпечніша вразливість" будь-яких інформаційних систем – людина" (стор. 57). Варто було би використати фразу "джерело найбільшої кількості інцидентів із кібербезпеки – людина";

10. Автор стверджує про наявність не існуючих функцій у таких мережних пристроїв як "балансувальник". На скільки відомо, то балансувальники не можуть захистити від "впровадження SQL" та "міжсайтового скриптинга", це функції IDPS, але автором не вказана можливость протидій балансувальником небезпечному класу атак – DDOS. Також автором в таб. 1.1. "Порівняння балансуваньників" не наведено функцій захисту про які стверджувалося раніше;

11. Не зрозумілий перехід автора після порівняння балансувальників на "хмарні сервіси" в підрозділі "Надійний моніторинг і аудит" (стор. 62);

12. Автором використовуються незв'язні речення позбавлені усілякого змісту. Наприклад: в контексті функціонування систем виявлення вторгнень на стор. 72 присутнє речення: "*Якщо датчики виявляють будь-яку шкідливу активність, він відповідає зловмисному пакету проти бази даних підписів атак.*". Складається враження, що автором було здійснено автоматичний переклад якогось матеріалу і після не прочитано його зміст. Такий випадок не поодинокий в тексті.

13. Автором стверджується, що "датчик може здійснювати різні дії залежно від того, як вони налаштовані. Наприклад, датчик може скинути TCP-з'єднання, надіславши FIN, змінити список контролю доступу на маршрутизаторі шлюзу або брандмауєрі …", але на скільки відомо, що системи виявлення вторгнення обмежуються лише оповіщенням, а дії здійснюють вже системи протидії вторгненням (IPS), або ж гібриди IDS та IPS – IDPS;

14. На рис. 1.2. (стор. 73) з легенди не зрозуміло яка ж лінія вказує на інтерфейс управління, а яка на інтерфейс моніторингу;

15. В тексті приводиться те що "маршрутизатори зазнають атак таких як: … соціальна інженерія" (стор. 124) – але атаки з використанням соціальної інженерії застосовуються для впливу на користувачів.

16. З опису методу безпечної маршрутизації при передачі мультифрактального трафіку видно, що автор вважає що трафік від зловмисників має невеликі значення параметру H та передається маршрутами з більшою вартістю, але в роботі не показано виходячи з чого автором взято припущення віднесення зловмисного трафіку саме до трафіку з малим H;

17. Автор чомусь системам DLP (Data Leak Protection, систем захисту від витоку інформації) приписує функцію "запобігання втратам інформації", а потім в тому ж реченні повертається до вірної функції "запобігання витоку" (стор. 158).

18. На рис. 3.4., 3.5., 3,6, не зрозуміло який показник яким кольором вимірюється та не зрозуміло в яких одиницях проводиться відображення на осях.

19. Піддаються сумніву використання "агрегованих критеріїв якості виявлення атак", які невідомо як розраховуються "на основі множини проведених експериментів та результатів подальшого виявлення вторгнень будь-яким методом виявлення вторгнень та/або аналізатором трафіку на основі характеристик трафіку" (стор. 148). На сторінці 190 використовуються "агреговані критерії якості виявлення атак" з приведенням їх значень, але не зрозуміло на основі чого зроблені висновки про інтервали значень цих "агрегованих критеріїв якості виявлення атак".

20. На рисунку 4.3 в класифікації систем виявлення вторгнень не зрозуміла класифікація "за способом збору інформації", а саме зустрічаються понятійні повтори та відхилення від розуміння "способу збору інформації" і їх переплутування з рівнем роботи відповідно моделі OSI/ISO-7, також з рисунку переплутуються різні способи класифікації та понять методів та способів, наприклад, "за способом виявлення вторгнень" – "виявлення аномалій" і за "методом виявлення атак" – "метод аномалій".

21. Не зрозуміла необхідність приведення автором рисунку 4.5. В тексті ніякого пояснення до рисунку не приведено, в наявності лише посилання на нього. З самого рисунку не зрозумілий об'єкт зображений на рисунку "схема балансування …" на якій зображені елементи з незрозумілими зв'язками взаємодії.

22. Не зовсім зрозуміло, що основна увага в роботі автором звернута на процеси маршрутизації, але робота подана за спеціальністю 05.13.21 "Системи захисту інформації".

Вказані недоліки дещо знижують сприйняття роботи, але принципово не знижують цінність отриманих наукових та практичних результатів. Наявність недоліків не впливає на загальний позитивний висновок щодо дисертації.

Відповідність дисертаційної роботи встановленим вимогам та загальний висновок.

Дисертаційна робота Радівілової Тамари Анатоліївни на тему «Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками» є кваліфікаційною науковою працею, що містить нові науково обґрунтовані результати проведених особисто здобувачем досліджень, які в галузі інформаційної безпеки у своїй сукупності вирішують важливу науково-прикладну проблему розробки моделей та методів забезпечення безпеки (доступності, конфіденційності) та якості обслуговування в комп'ютерних системах з урахуванням самоподібних властивостей інформаційних потоків в умовах наявності вторгнень та кібератак.

Дисертація та автореферат повністю відповідають паспорту спеціальності 05.13.21 – Системи захисту інформації, які висуваються до дисертацій на здобуття наукового ступеня доктора наук, а також п.п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 року № 567 (зі змінами). Автореферат та дисертація ідентичні один одному. Вважаю, що Радівілова Тамара Анатоліївна заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
начальник кафедри захисту інформації та кіберзахисту Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Міністерство оборони України,
докт. техн. наук, с. н. с. В. ЧЕВАРДІН
11.01. 2021

..АЧАЛЬНИК ВПС
П\П-К С.ЛИСЕНКО