Голові спеціалізованої вченої ради
Д 26.861.06 Державного університету
телекомунікацій

вул.Солом'янська, 7, м. Київ

ВІДГУК
офіційного опонента

професора кафедри безпеки інформаційних технологій Національного авіаційного університету доктора технічних наук, професора Хорошка Володимира Олексійовича, 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, зв'язок з науковими програмами, планами, темами.

В ході проведених досліджень встановлено, що крім вимог до забезпечення безпеки сучасних комп'ютерних систем, потрібно враховувати вимоги до якості обслуговування, які є класичними функціями сучасних комп'ютерних мереж. При цьому особливо важливо враховувати функціонування систем в умовах постійно зростаючої кількості та ємності атак і вторгнень, які призводять до суттєвої зміни структурних параметрів і властивостей інформаційних потоків та комп'ютерних систем, а також впливають на самоподібність, пропускну здатність, захищеність, керованість тощо. Забезпечення безпеки та якості обслуговування комп'ютерних систем в умовах постійно зростаючої інтенсивності інформаційних потоків та кібератак стає дедалі складнішим завданням. Зважаючи на те, що тема дисертації присвячена вирішенню важливої науково-прикладної проблеми, вважаю її актуальною.

Актуальність теми додатково підтверджується пріоритетами та напрямами забезпечення кібербезпеки України, як передбачено Стратегією кібербезпеки України (затверджена Указом Президента України від 15 березня 2016 року № 96).

Аналіз основного змісту, наукової новизни та практичного значення.

Дисертація складається із вступу, шести розділів, висновків, додатків, списку використаних джерел. У роботі 123 рисунки та 41 таблиця. Загальний обсяг роботи становить 403 сторінки, у тому числі 300 сторінок основного тексту, 31 сторінка з рисунками та таблицями, анотації на 26 сторінках, додатки на 21 сторінці. Список використаних джерел містить 381 найменування, викладених на 50 сторінках.

Зміст роботи відповідає сформульованій науково-прикладній проблемі та поставленим завданням, а їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 05.13.21 «Системи захисту інформації» й спрямовані на розроблення моделей та методів забезпечення безпеки та якості обслуговування комп'ютерних систем.

У вступі автором подано загальну характеристику дисертаційної роботи, обґрунтовано її актуальність, сформульовано мету і завдання досліджень, відображено наукову новизну й практичну цінність отриманих результатів, наведені дані щодо апробації та впровадження.

У першому розділі здобувачем проведено аналіз існуючих методів, які застосовуються в забезпеченні безпеки та якості обслуговування, виявлено протиріччя між зростаючими вимогами до рівня безпеки та якості обслуговування в ході передачі самоподібного трафіка і можливостями існуючих технологічних та теоретичних рішень. Як наслідок, наразі відсутні адекватні моделі та методи забезпечення безпеки та якості обслуговування, які враховують самоподібні властивості інформаційних потоків, в умовах наявності вторгнень та кібератак.

Доведено, що в сучасних наукових працях основна увага приділяється розробці методів, заснованих на використанні динамічних алгоритмів урахування стану системи та на вхідних сповіщеннях. Проте ці методи мають дуже суттєві недоліки в ході дисбалансу роботи системи та наявності вторгнень і сплесків трафіку. В процесі маршрутизації інформаційних потоків питання безпеки розглядаються переважно зі сторони оцінювання ризику уразливостей ресурсів або надійності та живучості. При цьому властивості структури трафіка не враховуються. Це пов'язано з відсутністю адекватних моделей самоподібного трафіка та комп'ютерних систем з точки зору мультифрактальної структури трафіка та його статистичних характеристик.

Виходячи з проведеного аналізу, виникає актуальна науково-прикладна проблема щодо 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. Таким чином, під час розробки нових та модернізації існуючих моделей комп'ютерних систем і методів управління трафіком, актуальним є завдання в ході маршрутизації та балансування трафіка забезпечувати безпечну передачу інформаційних потоків шляхом урахування ймовірності виявлення аномальної поведінки в комп'ютерній системі та інформаційному потоці та властивостей його самоподібності.

Відповідно до поставленої мети, для вирішення науково-прикладної проблеми, в роботі сформульовано такі завдання: розробити концепцію забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками; розробити моделі та методи безпечної маршрутизації, безпечного балансування вхідних самоподібних інформаційних потоків різного класу обслуговування, що враховує їхні мультифрактальні властивості та ймовірність виявлення вторгнень; розробити методи виявлення атак у мережних системах виявлення вторгнень, що засновані на сигнатурному аналізі пакетів, на ентропійному аналізі пакетів, на основі методів машинного навчання; розробити комплексний метод виявлення атак у комп'ютерній системі, що базується на поведінковому, сигнатурному та ентропійному аналізі самоподібних інформаційних потоків; розробити модель і метод балансування вхідних потоків у мережних системах виявлення вторгнень; провести експериментальну верифікацію і практичну реалізацію розроблених методів і моделей з метою підтвердження їхньої ефективності та працездатності.

Другий розділ присвячено розробці концепції 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, а також методом забезпечення безпечної маршрутизації під час передачі самоподібного трафіка та 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.

Удосконалено модель розподіленої комп'ютерної системи, на основі якої було розроблено метод безпечної маршрутизації самоподібного трафіку в комп'ютерних мережах. Модель розподіленої комп'ютерної системи має компоненти забезпечення безпеки, управління трафіком і враховує фрактальні властивості вхідних інформаційних потоків та має обмеження на більш повний набір характеристик мережі для різних класів обслуговування, що дозволяє розробити методи забезпечення безпеки при управлінні трафіком з урахуванням вимог якості обслуговування.

На основі моделі розроблено метод безпечної маршрутизації в комп'ютерній системі, який засновано на врахуванні мультифрактальних властивостей трафіку та параметрів якості обслуговування пріоритетного трафіку, на основі чого обчислюється вартість маршруту для передачі трафіку.

У ***третьому розділі*** дисертації удосконалено метод забезпечення безпеки при динамічному балансуванні самоподібного трафіку в комп'ютерних мережах з врахуванням загальної величини дисбалансу системи, який засновано на моделі балансувальника комп'ютерної системи. В роботі удосконалено модель балансувальника комп'ютерної системи, яка враховує фрактальні властивості трафіку, параметри якості обслуговування для кожного класу обслуговування та параметри безпеки розподілу трафіку. Вузли системи описуються об'ємом ЦПУ та оперативної пам'яті, пропускною здатністю каналів зв'язку та рівнем дисбалансу навантаження. На основі моделі балансувальника удосконалено метод забезпечення безпеки при динамічному балансуванні навантаження, який дає змогу підвищити ступінь безпеки функціонування системи за рахунок спрямування неоднорідних інформаційних потоків на більш безпечні і менш завантажені ресурси. Запропонований метод дозволяє розраховувати завантаження процесора, пам'яті і пропускної здатності каналу потоками різних класів обслуговування для кожного сервера і всієї розподіленої системи та розподіляти самоподібний трафік на основі параметру безпеки розподілу трафіку кожного класу обслуговування та розрахованих значеннях завантаження серверів. Метод впроваджено та завдяки аналізу та врахуванню фрактальних властивостей та параметру безпеки розподілу трафіку забезпечується зниження в 2 рази кількості втрачених даних, що дозволяє до 9

раз знизити кількість атакованого трафіку на серверах, на 16% знизити дисбаланс завантаження системи.

У *четвертому розділі* розроблено метод безпечного балансування фрактального трафіку між сенсорами в мережній системі виявлення вторгнень, який засновано на моделі системи виявлення вторгнень (СВВ). Розроблена модель мережної системи виявлення вторгнень, до параметрів якої належать фрактальні характеристики трафіку та обмеження на час обслуговування різних класів трафіку, дозволяє розробити методи балансування трафіка між детекторами виявлення вторгнень з урахуванням вимог якості обслуговування. На основі розробленої моделі запропоновано метод динамічного балансування трафіку в мережних системах виявлення вторгнень, який враховує ступінь фрактальності трафіка для розрахунку часу глибокої перевірки пакетів, на основі якого розраховується час, потрібний для виявлення атаки, здійснює генерацію і оновлення правил балансування пакетів, що прибувають. Метод балансування навантаження в мережних системах виявлення вторгнень впроваджено, що призвело до збільшення кількості проаналізованих пакетів на 21%, за рахунок чого відсоток виявлених атак збільшився на 14% та зменшився середній час очікування пакетів на 16%.

П'ятий розділ присвячено подальшому розвитку методів ентропійного аналізу протоколів та аналізу сигнатур. Розроблено метод виявлення атак для мережних СВВ, що засновано на глибокому аналізі пакетів за сигнатурами, часі аналізу пакетів та рейтингуванні бази сигнатур за найбільш поширеними атаками. Метод аналізу сигнатур, який використовує глибокий аналіз пакетів для аналізу вмісту трафіку впроваджено, що дозволило ідентифікувати 93% атак та отримати низьку кількість хибнопозитивних спрацьовувань (менше 8%)

Отримав подальший розвиток метод виявлення атак в мережних системах виявлення вторгнень, який засновано на ентропійному аналізі пакетів та статистичних характеристиках трафіку. Ентропійний аналіз використовується для виявлення атак, щоб сформувати статистичний критерій для перевірки приналежності досліджуваного екземпляра до аномального класу. Розроблений метод дозволяє скоротити час виявлення вторгнень та ідентифікувати раніш невідомі атаки. Метод ентропійного аналізу протоколів був впроваджений, що дозволило отримати високі значення точності виявлення атак (близько 94%) і низькі значення хибнопозитивного індексу (близько 12%) для різних типів атак.

У шостому розділі отримав подальший розвиток метод аналізу поведінки трафіку для ідентифікації атак, який засновано на використанні алгоритмів машинного навчання. Метод аналізу поведінки трафіку показав високу точність ідентифікації різних атак при зміні рівня атаки. Результати класифікації показали, що ймовірність виявлення атаки істотно залежить від фрактальних властивостей трафіку, рівня атаки по відношенню до трафіку і варіюється від 0,7 до 0,98. На основі сумісного застосування методів аналізу поведінки трафіку, аналізу протоколів та сигнатурного аналізу розроблено комплексний метод ідентифікації атак. Розроблено симулятор атакованого трафіку, який дозволяє створювати модельну адитивну реалізацію трафіку і атаки, з заданими параметрами, як трафіку, так і атаки. Реалізації атак відповідають відомим існуючим атакам різних типів. Отриманий штучним шляхом трафік атаки, разом з реальним трафіком з датасета, був використаний для проведення машинного навчання. Проведено порівняльний аналіз роботи комплексного метода, який показав високу точність ідентифікації атак при різній інтенсивності трафіку. Комплексний метод впроваджено, що дозволило отримати більш високу точність ідентифікації атак (до 98%), на відміну від існуючих.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації. Обґрунтованість одержаних положень та результатів, отриманих здобувачем, обумовлюється застосуванням відомих методів дослідження на основі системного підходу та теорії інформації із застосуванням математичних моделей і методів статистичного аналізу. Під час дослідження властивостей самоподібності та розрахунку характеристик мережного трафіка та його модельних аналогів використовувались методи фрактального і статистичного аналізу даних. Методи безпечного балансування навантаження необхідні в процесі передачі трафіка. Використання методів безпечної маршрутизації необхідно для передачі трафіка в комп'ютерній системі. Для виявлення та ідентифікації вторгнень та атак використовувались методи класифікації, методи аналізу пакетів, методи ентропійного аналізу та методи аналізу підписів з глибоким аналізом пакетів. Імітаційне моделювання використовувалось для розробки методів забезпечення конфіденційності, цілісності, доступності і запобігання перевантаженню системі, перевірки запропонованих моделей, для аналізу та перевірки достовірності отриманих результатів.

Достовірність одержаних у роботі результатів підтверджується ретельною перевіркою результатів запропонованих моделей і методів забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками, а також ідентичністю результатів експериментальних досліджень з використанням математичного моделювання та збіжністю результатів моделювання з теоретично отриманими результатами.

До основних наукових результатів, які отримані в дисертаційній роботі, на мій погляд, 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. 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.

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.

Удосконалено метод забезпечення безпеки мережі при динамічному балансуванні навантаження з самоподібним трафіком, який, на відміну від

існуючих, відрізняється застосуванням моделі балансувальника комп'ютерної мережі з урахуванням параметрів безпеки розподілу трафіка і мультифрактальних властивостей трафіка. Реалізація зазначеного методу дозволяє зменшити завантаженість ресурсів комп'ютерної системи за рахунок спрямування безпечних неоднорідних інформаційних потоків на безпечні та менш завантажені ресурси.

Теоретична і наукова цінність та практичне значення одержаних автором наукових результатів.

Практичне значення отриманих результатів полягає в тому, що отримані теоретичні положення та методи доцільно використовувати 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 та 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 викладення дисертації та автореферату.

Дисертація і автореферат написані грамотно. Стиль викладення метеріалів дослідження, а саме наукових положень і рекомендацій, відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора наук. Дисертація являє собою наукову працю, яка мітить 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.

Повнота викладення наукових результатів дисертації в опублікованих роботах.

Основні результати дисертаційної роботи Радівілової Т.А. повністю викладені у 67 наукових працях, з них 36 статтях, 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. Також результати дисертаційних досліджень знайшли відображення в 29 матеріалах та тезах доповідей опублікованих у матеріалах міжнародних наукових конференціях та форумах, що індексуються базою Scopus. Також результати подано у двох монографіях, з яких одна закордонна. Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації.

Зауваження до дисертаційної роботи.

1. Оскільки забезпечення безпеки залежить від поточного стану системи та аналізу захищеності комп'ютерної системи доцільно було б зосередитись на виявленні слабких ланок, несправностей, ізоляції загроз безпеки з метою зменшення ризиків та ймовірності реалізації загроз інформаційній безпеці.

2. Оскільки в дисертаційній роботі запропоновано метод безпечного балансування інформаційних потоків в комп'ютерних системах та метод безпечного балансування в системах виявлення вторгнень, який залежить від часу обробки інформації та самоподібних властивостей інформаційних потоків то, на мою думку, доцільно було б об'єднати обидва методи в один. Це дозволило б скоротити перелік методів та полегшити сприйняття викладених матеріалів.

3. Не повною мірою наведено методи обчислення мультифрактальних і фрактальних параметрів, їхні недоліки та переваги. Також не наведено точність обчислення мультифрактальних параметрів запропонованими методами.

4. Так як в дисертаційній роботі запропоновано методи машинного навчання для обчислення поведінки мережі щодо виявлення вторгнень: нейронні мережі та випадкового лісу. Але, на мій погляд, також було б доцільно використовувати метод глибокої нейронної мережі та порівняти його із наведеними методами.

5. В дисертаційній роботі автор вирішує задачі безпечного управління інформаційними потоками та виявлення вторгнень, то було б доцільно описати комплексну систему захисту інформації починаючи з прийняття потоку на вході

у комп'ютерну систему та безпечне його обслуговування до кінцевого користувача.

Зазначені недоліки не є принциповими та не впливають на загальну позитивну оцінку дисертаційної роботи Радівілової Т.А.

Висновок.

Дисертація Радівілової Тамари Анатоліївни є завершеною, логічно побудованою, одноосібно написаною працею, в якій вирішена науково-прикладна проблема 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.

Дисертаційна робота за актуальністю теми, обґрунтованістю та достовірністю наукових положень, новизною досліджень і практичною цінністю отриманих результатів відповідає п.п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 року № 567 (зі змінами). Дисертація відповідає спеціальності 05.13.21 – системи захисту інформації, а її авторка, Радівілова Тамара Анатоліївна заслуговує присудження їй наукового ступеня доктора технічних наук.

Офіційний опонент

Доктор технічних наук професор,
Професор кафедри безпеки інформаційних
технологій, факультету кібербезпеки,
комп'ютерної і програмної інженерії
Національного Авіаційного університету В.О. Хорошко

Підпис Хорошка В.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Логенький