Голові спеціалізованої вченої ради
Д 26.861.06 Державного університету
телекомунікацій

вул.Солом'янська, 7, м. Київ

ВІДГУК
офіційного опонента
завідувача кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича,
доктора технічних наук, професора Політанського Леоніда Францовича
на дисертаційну роботу Радівілової Тамари Анатолівни
«Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками»,
представлену на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 «Системи захисту інформації»

Актуальність теми дослідження.

Одним із актуальних питань сьогодення є розвиток інформаційних технологій включаючи розроблення новітніх методів захисту інформації при її передаванні, обробленні та зберіганні в інформаційно-телекомунікаційних системах із забезпеченням належного рівня якості обслуговування.

При цьому слід зауважити, що властивості вхідного трафіку суттєво впливають на безпеку та якість обслуговування і продуктивність комп'ютерних систем.

Однією із таких властивостей трафіку є його самоподібність, що обумовлена поведінкою користувачів у мережі та неоднорідністю ресурсів систем. Самоподібність трафіку обумовлює на порядок вищі затримки та втрати пакетів, ніж для звичайного трафіку. Існуючі методи забезпечення якості та безпеки роботи комп'ютерних систем в умовах кібератак не враховують самопобдібні властивості інформаційних потоків.

Тому вирішення сформульованої в роботі Радівілової Т.А. науково-прикладної проблеми розроблення методів забезпечення безпеки та якості обслуговування в комп'ютерних системах з урахуванням самоподібних властивостей інформаційних потоків в умовах вторгнень та кібератак є актуальним та своєчасним.

Структура, задачі та короткий зміст роботи.

Дисертація складається зі вступу, шести розділів, висновків, списку використаних джерел з 381 найменувань і додатків. Робота містить 300 сторінок основного тексту, 41 таблицю, 123 рисунка.

Метою дисертаційного дослідження є підвищення ефективності методів забезпечення безпеки та якості обслуговування в комп'ютерних системах за рахунок ідентифікації атак із врахуванням самоподібності інформаційних потоків.

Для досягнення поставленої мети автором були розв'язані наступні основні задачі:

- запропоновано концепцію забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками;
- розроблено модель та метод безпечної маршрутизації вхідних самоподібних інформаційних потоків різного класу обслуговування;
- створено модель і метод безпечного балансування вхідних самоподібних інформаційних потоків у комп'ютерних системах та системах виявлення вторгнень;
- створено комплексний метод виявлення атак у комп'ютерній системі на основі поведінкового, сигнатурного та ентропійного аналізі самоподібних потоків; проведено експериментальну верифікацію і практичну реалізацію розроблених методів і моделей.

У вступі обґрунтовано актуальність розв'язуваної наукової проблеми, представлено основні результати аналізу робіт в області розроблення моделей і методів забезпечення безпеки та якості обслуговування в комп'ютерних системах в умовах наявності кібератак, розкрито наукову новизну та практичну цінність отриманих результатів, сформульовані мета і задачі, що необхідно було вирішити для досягнення мети. Наведено відомості про апробацію та публікації результатів досліджень, а також особистий внесок автора.

У першому розділі проведена загальна характеристика стану проблеми забезпечення захисту інформації під час її передавання у комп'ютерних мережах, а також проаналізовано методи виявлення вторгнень. За результатами аналізу встановлено, що в умовах забезпечення безпеки інформації під час її передавання найчастіше не приймаються до уваги самоподібні властивості інформаційних потоків. Розглянуто основні поняття і властивості самоподібного та мультифрактального мережевного трафіку. На підставі аналізу літературних даних визначені напрямки вирішення наукової проблеми та сформульовано задачі наукових досліджень дисертаційної роботи.

Другий розділ дисертаційної роботи присвячений розробці концепції забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками, що працюють в умовах вторгнень та кібератак. Запропоновано удосконалену модель розподіленої комп'ютерної системи, що включає компоненти забезпечення безпеки та управління трафіком і має обмеження на набір характеристик мережі для різних класів обслуговування. На відміну від існуючих запропонована модель розподіленої комп'ютерної системи враховує самоподібність вхідних інформаційних потоків. На базі запропонованої моделі системи було розроблено метод безпечної маршрутизації трафіка з фрактальними властивостями з використанням імітаційного моделювання, проводилася перевірка ефективності роботи запропонованого методу для мереж різної структури та досліджені вихідні параметри якості обслуговування. Отримані дані підтверджують ефективність запропонованого методу безпечної маршрутизації щодо забезпечення безпеки та якості обслуговування.

Третій розділ присвячений опису запропонованої моделі балансувальника комп'ютерної системи, що враховує параметри безпеки розподілу трафіка. На основі моделі розроблено метод безпечного балансування мультифрактального

трафіку, що базується на зовнішніх і внутрішніх системах моніторингу. Розроблений метод забезпечує безпечну передачу інформаційних потоків, рівномірний розподіл навантаження на серверах, високі показники продуктивності, пропускної здатності та відмовостійкості.

У четвертому розділі автором запропонована модель системи виявлення вторгнень, що враховує фрактальні властивості трафіка. На основі запропонованої моделі розроблено метод безпечного балансування фрактального трафіка між сенсорами в мережній системі виявлення вторгнень. Розроблений метод балансування в системі виявлення вторгнень забезпечує рівномірне навантаження з метою ефективного використання ресурсів багатопотокових систем виявлення вторгнень.

П'ятий розділ присвячено подальшому розвитку методів виявлення вторгнень на основі аналізу ентропії пакетів та сигнатур. Ентропійний аналіз протоколів використаний для формування статистичного критерію перевірки приналежності досліджуваного пакету у поточному мережному трафіку до аномального класу, що уможливлює виявлення атак. Для аналізу ефективності роботи методу для виявлення DDoS-атак були проведені експерименти в спеціалізованому середовищі, що підтвердили придатність методу аналізу ентропії для ідентифікації різних типів атак. В розділі розроблено метод аналізу сигнатур, що базується на глибокому аналізі пакетів. Експерименти, в яких використовувалась система виявлення вторгнень Snort, підтвердили перевагу запропонованого алгоритму аналізу сигнатур.

Шостий розділ присвячено подальшому розвитку та класифікації методів виявлення вторгнень на основі машинного навчання із врахуванням мультифрактальних та рекурентних характеристик інформаційного трафіку. Запропоновано комплексний метод виявлення вторгнень, що базується на використанні сукупності алгоритмів аналізу сигнатур, аномалій поведінки мережі та ентропійному аналізі протоколів. В даному випадку мережна система виявлення вторгнень є множиною детекторів і аналізаторів трафіка. Для аналізу результативності запропонованого комплексного методу було проведено імітаційне моделювання з використанням даних з датасетів, які містять в собі неатакований трафік та різні види атак. Результати моделювання підтверджують ефективність запропонованого методу детектування різних типів атак і вторгнень.

Наведені у **висновках** результати досить повно відображають суть дисертаційної роботи і мають практичне втілення.

У додатках наведені документи впровадження результатів дисертації.

Зв'язок роботи з науковими програмами. Обраний напрямок досліджень пов'язаний із виконанням дослідних робіт Харківського національного університету радіоелектроніки у межах договору за замовленням Міністерства освіти і науки України «Автоматизована оптична інформаційно-вимірювальна система для полігонних випробувань керованих та некерованих ракет, артилерійських і реактивних снарядів», що виконується за держзамовленням; угоди про надання гранту Державним департаментом США 2019 р. «Українська обізнаність у сфері кібербезпеки: підтримка низки тренінгів щодо розвитку

кіберзахисту та підвищення обізнаності в Україні»; проекту ТЕМПУС «Навчання експертів наступного покоління з кібербезпеки: нова визнана ЄС програма магістра»; проекту «TRUST – «Назустріч надійній екосистемі забезпечення якості» (TRUST), в яких здобувач виступав виконавцем.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій. Основні теоретичні положення дисертації одержані шляхом коректного застосування засобів теорії прийняття рішень та оптимізації, опису процесів в мережах масового обслуговування, методів теорії комп'ютерних мереж та положень галузі інформаційної безпеки та інфокомунікаційних досліджень. Відповідність та обґрунтованість результатів досліджень підтверджуються граничними переходами до відомих окремих випадків, одержаних в рамках інших теоретичних підходів; апробацією математичних моделей на тестових прикладах, зіставленням отриманих результатів з відомими, достатньою збіжністю аналітичних та експериментальних досліджень, впровадженнями та достатньою кількістю публікацій у виданнях, що входять до переліку фахових видань з технічних наук в Україні; виступами на наукових конференціях національного та світового рівня.

Все це свідчить про високий ступінь достовірності та обґрунтованості результатів дисертації.

Наукова новизна результатів, що отримані у дисертаційній роботі.

Аналіз дисертаційної роботи дозволяє зробити висновок, що автором у процесі досліджень отримані такі нові основні результати:

1. Вперше розроблено концепцію забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками, що працюють в умовах вторгнень та кібератак. Реалізація концепції дозволяє гарантовано забезпечити доступність, конфіденційність та якість обслуговування в комп'ютерних системах із самоподібними інформаційними потоками під час вторгнень та кібератак.

2. Удосконалено модель розподіленої комп'ютерної системи, яка на відміну від існуючих включає компоненти забезпечення безпеки та управління вхідними інформаційними потоками з мультифрактальними властивостями. Запропонована модель містить обмеження на набір характеристик мережі для різних класів обслуговування, що дозволяє розробити методи забезпечення безпеки з урахуванням вимог до якості обслуговування.

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

4. 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.

5. Вперше розроблено метод забезпечення безпечної маршрутизації, 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.

6. 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.

7. 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.

Прикладна цінність дисертації визначається суттєвим підвищенням ефективності інструментальних засобів у вигляді програмних або програмно-апаратних модулів виявлення кібератак у комп'ютерних системах, балансування самоподібними інформаційними потоками в мережних системах виявлення вторгнень та управління трафіком для забезпечення безпеки та якості обслуговування в комп'ютерних системах з самоподібними інформаційними потоками. Автором було розроблено програмну реалізацію комплексного методу виявлення кібератак у комп'ютерній системі, а також прикладне програмне забезпечення для балансування навантаження вузлів мережної системи виявлення вторгнень. В роботі було розроблено спеціалізоване програмне забезпечення, що базується на створених методах і моделях ідентифікації вторгнень, яке дозволило підвищити захищеність інформаційних ресурсів та підвищити якість обслуговування в комп'ютерних системах. Це підтверджується актами впровадження результатів роботи в Харківському державному регіональному науково-технічному центрі з питань технічного захисту інформації, ПрАт Фарлеп-Інвест ТОВ Дайтекс Технолоджіс, АТ БАНКОМЗВ'ЯЗОК, ТОВ WorkNest, ТОВ Владармет, ТОВ Стріт Вей Холідейз, Харківському національному університеті радіоелектроніки.

Рекомендації щодо впровадження результатів дисертації. Перспективи використання результатів є використанні запропонованих моделей та методів при розробленні і впроваджені ефективних інструментальних та програмних засобів для виявлення вторгнень у комп'ютерних системах, а також

балансування та управління трафіком у маршрутизаторах і балансувальниках з метою забезпечення конфіденційності, доступності та якості обслуговування в умовах самоподібних потоків даних в комп'ютерних системах. Отримані автором результати можуть бути корисними при проектуванні мережних систем виявлення вторгнень і передачі даних у інфокомунікаційному середовищі.

Повнота викладення здобувачем основних результатів дисертаційної роботи у публікаціях.

Основні результати досліджень, а також сформульовані у дисертації наукові положення, висновки та рекомендації у повному обсязі викладені у 67 друкованих працях, у тому числі 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.

Отримані результати апробовано на 23 Міжнародних наукових конференціях та форумах, з яких 22 на конференціях, що індексуються базою Scopus. Результати подано у двох монографіях, з яких одна закордонна.

Зазначені наукові роботи були опубліковані після захисту кандидатської дисертації автора, а їх матеріали не включалися до кандидатської дисертації. В працях, які опубліковано у співавторстві, коректно відображено особистий внесок дисертанта, а також забезпечені посилання на публікації інших авторів.

Оцінка мови, стилю та оформлення дисертації і автореферату

Дисертаційну роботу написано українською мовою грамотно, на хорошому стилістичному рівні. Застосована в роботі наукова термінологія є загальновизнаною, стиль викладення результатів теоретичних і практичних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття та використання.

Автореферат відповідає змісту дисертації, написаний грамотно, з використанням сучасної української наукової термінології. Оформлення дисертаційної роботи й автореферату повністю відповідає вимогам державних стандартів України. Зміст автореферату є ідентичний змісту самої дисертації.

Зауваження по роботі.

1. У першому розділі доцільно було б надати опис основних типів телекомунікаційного трафіку і відповідних фрактальних властивостей, якими володіють різні види трафіка.
2. У другому розділі дисертації при розробленні моделі комп'ютерних систем із самоподібними інформаційними потоками автор не врахував особливості оброблення інформації в хмарних системах (час оброблення, навантаження ресурсів та інше).
3. У другому розділі дисертації під час опису методу безпечної маршрутизації самоподібного трафіка в комп'ютерних системах не вказано часові рамки повторного пошуку маршруту передачі даних, а вказано загальні часові характеристики джитеру та затримки даних у мережі.

4. У п'ятому та шостому розділах дисертації шляхом використання методів виявлення вторгнень автор намагається знизити рівень помилкових виявлень вторгнень, але нажаль дослідження в цьому напрямку не проведені у повному обсязі.
5. Різницю між ентропіями класів пакетів в поточному мережевому трафіку та базовим розподілом доцільно було б назвати відносною ентропією, а не умовною (автореферат стор. 19, дисертація стор. 268), оскільки значення $log\frac{\hat{P}(\omega)}{P(\omega)}$ визначає різницю між ентропією отриманого на приймальній стороні системи трафіку від заданого максимального значення ентропії.
6. Пункт 8 (автореферат стор. 20, дисертація стор. 271) сформульований некоректно. Очевидно, що автор приводить дослідження для трьох проміжків часу ΔT і знаходить сумарне значення ентропії пакетів каналу ω. Тобто, замість додати два терміни доцільно було б записати знайти суму ентропій для трьох інтервалів часу, що слідують один за одним.
7. У шостому розділі розглянуто методи бінарної класифікації на основі машинного навчання, які застосовуються для детектування кібератак. У тексті дисертації не вказано, чому були використані тільки нейронні мережі і метод випадкового лісу, в той час як для бінарної класифікації широко застосовуються різні методи, наприклад метод опорних векторів та інші.
8. У шостому розділі дисертації при використанні методів машинного навчання автором не вказано алгоритму формування набору ознак для адекватної роботи обраних методів.
9. У дисертаційній роботі запропоновані методи динамічного балансування самоподібного трафіку як в комп'ютерній системі в цілому, так і окремо в мережній системі виявлення вторгнень, проте не проведений як порівняльний аналіз цих методів, так і притаманні їм характерні відмінності.
10. У дисертаційній роботі аналіз інформаційних потоків проводиться на третьому, четвертому та сьомому рівнях моделі OSI. Доцільно було б дослідити вплив атак на другому рівні моделі OSI.
11. В авторефераті та в дисертації некоректно вказані кількість рисунків та таблиць, які містить дисертація.

Наведені зауваження мають окремий характер, не знижують високий науковий рівень дисертаційної роботи і не впливають на її загальну позитивну оцінку.

Висновок. Розглянувши дисертаційну роботу Радівілової Тамари Анатолівни «Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками», автореферат, опубліковані наукові праці та додаткові матеріали, можна зробити такі висновки:

– дисертація відповідає паспорту спеціальності 05.13.21 – системи захисту інформації;

– тематична спрямованість роботи є актуальною, суспільно корисною й перспективною у плані продовження розпочатих досліджень;

– дисертація є цілісною, завершеною, оригінальною, самостійною кваліфікаційною науковою роботою, в якій отримано нові науково обґрунтовані та практичні результати, що в сукупності вирішують важливу науково-прикладну проблему 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.

Вважаю, що за актуальністю та змістом, характером фактичного матеріалу, ступенем його якісного і кількісного аналізу, рівнем новизни, теоретичної і практичної значущості результатів дослідження для науки і практики, загальним обсягом і якістю оформлення, реалізацією поставлених завдань, обґрунтованістю висновків та повнотою викладання одержаних результатів у публікаціях дисертація Радівілової Т.А. «Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками», відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 зі змінами, затвердженими Постановами Кабінету Міністрів України № 656 від 19 серпня 2015 р. та № 1159 від 30 грудня 2015 р., які висуваються до докторських дисертацій, а Радівілова Тамара Анатолівна заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
завідувач кафедри
радіотехніки та інформаційної безпеки
Чернівецького національного
університету імені Юрія Федьковича,
доктор технічних наук, професор Леонід ПОЛІТАНСЬКИЙ

Підписи Політанського Л. Ф.
засвідчую
Учений секретар
Чернівецького національного університету
імені Юрія Федьковича Наталія ЯКУБОВСЬКА