Голові спеціалізованої вченої ради Д 64.052.09
61166, м. Харків, пр. Науки, 14,
Харківський національний університет
радіоелектроніки

ВІДГУК
офіційного опонента

професора кафедри інформаційної та кібернетичної безпеки навчально-наукового інституту захисту інформації Державного університету телекомунікацій доктора технічних наук, доцента Семка Віктора Володимировича на дисертаційну роботу Андерса Карлссона на тему "Модель та метод виявлення низькоінтенсивних атак на прикладному рівні", подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – "Телекомунікаційні системи та мережі"

1. Актуальність теми дисертаційної роботи

Атаки на прикладному рівні являють собою найчисленнішу групу, яка використовується для спостереження або несанкціонованого доступу до ресурсів інформаційно-телекомунікаційних систем (ІТС) на мережевому рівні. До них відносяться впровадження вірусів і троянських програм в ІТС, використання вразливостей ОС і прикладних програм, підбір паролів, атаки на веб-додатки.

Однією з найбільш розповсюджених загроз є атака на відмову в обслуговуванні. Ця атака унеможливлює роботу системи, частково або повністю блокує необхідні користувачу ресурси та послуги.

Розробка методів і моделей виявлення низькоінтенсивних атак на прикладному рівні відображає сучасні тенденції щодо забезпечення безпеки функціонування сучасних ІТС, а саме:

- орієнтацію мережевих послуг на забезпечення якості обслуговування;
- збільшення частки інфокомунікаційних систем, що використовують хмарне середовище у якості інфраструктури побудови та надання послуг;
- доступністю мережевих послуг, що залежить від функціональних характеристик і захищеності мереж від різного роду мережевих атак;
- використання інтелектуальних технологій реалізації та управління мережевими атаками на відмову в обслуговуванні;
- використання хмарних технологій, які мають застосовувати новітні моделі та методи виявлення атак на прикладному рівні при створенні комплексів засобів захисту інформації ІТС.

Саме тому створення концептуально нових методів і моделей виявлення низькоінтенсивних атак на прикладному рівні є ***актуальною науковою задачею.***

2. Аналіз основного змісту, наукової новизни та практичної значимості, оцінка достовірності та обґрунтованості результатів

Дисертація складається зі вступу, чотирьох розділів, висновків та списку використаних джерел. Загальний обсяг дисертації становить 130 аркушів, з яких основний зміст роботи розкрито на 110 аркушах.

Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають п.п. 1, 2, 4, паспорту спеціальності 05.12.02 – "Телекомунікаційні системи та мережі" й направлені на дослідження сутності процесів виявлення низькоінтенсивних атак на прикладному рівні, а також розробку науково-методичних основ, технологій та інструментальних засобів виявлення атак, що використовують вразливість відмови в обслуговуванні.

При цьому ***у вступі*** автором обґрунтовано актуальність досліджуваної проблеми та висвітлено її поточний стан, чітко сформульовано мету, котра корелює з темою роботи, та деталізується у завданнях, визначено об'єкт та предмет дослідження та систему використаних в роботі дослідницьких методів та інструментів.

У ***першому розділі*** автором виконано аналіз технологічних рішень та сутності низькоінтенсивних атак типу "відмова в обслуговуванні" на прикладному рівні, виділено їх основні характеристики та сценарії реалізації, проведено дослідження вразливості різних протоколів прикладного рівня до такого класу атак. За результатами аналізу визначено шляхи модифікації досліджених підходів щодо виявлення і прогнозування виникнення Slow-http атак на підставі визначених параметрів функціонування web-серверу.

У ***другому розділі*** автором проведено аналіз особливостей реалізації Slow-http атак, встановлені основні математичні закономірності між параметрами атаки та станом web-серверу, що атакується. Отримані результати дозволили розробити відповідну математичну модель поведінки web-серверу під час атаки, а також визначити розподіл ймовірностей стану web-серверу під час реалізації Slow-http атак різного типу. Адекватність математичної моделі досліджено на імітаційній моделі.

У ***третьому розділі*** розроблено математичну модель прогнозування стану "відмова в обслуговуванні" для web-серверу. Запропонована математична модель базується на аналізі динаміки переходів між станами серверу.

Аналіз засобів моделювання динаміки станів мультисервісних мереж показав, що найбільш прийнятним математичним апаратом для моделювання є ймовірносно-часові графи, що дозволяє зв'язати модель станів web-серверу з динамікою його функціонування, яка визначається набором станів та ймовірнісно-часовими характеристики переходів між ними.

Автором досліджено показники часу переходу web-серверу в стан перевантаження або "відмови в обслуговуванні" в залежності від параметрів, що характеризують атаку за співвідношенням вхідного та вихідного потоків даних.

У ***четвертому розділі*** запропоновано загальний метод виявлення та класифікації slow-http атак на web-сервер та алгоритм його реалізації.

За результатами імітаційного експерименту щодо запропонованого методу виявлення та класифікації атак на web-сервер визначено його ефективність щодо хмарного середовища ІТС на прикладі мультисервісної мережі.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, які сформульовані в дисертації, переконливо окреслена використанням сучасних методів і механізмів захисту мережевих послуг, що використовують хмарне середовище як платформу функціонування ІТС при низькоінтенсивних атаках на відмову в обслуговуванні.

Отримані автором наукові результати у відповідності до поставлених задач досліджень є логічними, не суперечать фундаментальним фізичним і математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків на міжнародних форумах, науково-технічних конференціях та семінарах.

Достовірність отриманих в роботі положень і наукових результатів

підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих припущень та формулюванням умов досліджень, а також математичному і імітаційному моделюванні процесів виявлення низькоінтенсивних атак на прикладному рівні.

Новими науково-обгрунтованими результатами, які:

дістали подальшого розвитку є:

1) апарат ланцюгів Маркова як засіб моделювання сервісів прикладного рівня, на основі використання протоколу транспортного рівня TCP дозволило: *визначити* модель, яка для розрахунку імовірності виникнення атаки на відмову в обслуговуванні використовує інформацію про кількість запитів, що можуть буди оброблені сервісом одночасно, та динаміку їх обслуговування; *забезпечити* можливість розрахувати імовірність переходу сервісу у стан "відмова в обслуговуванні", що відповідає мережевій атаці;

отримані здобувачем вперше є:

2) модель прогнозування часу переходу сервісу у стан "відмова в обслуговуванні", яка базується на використанні апарату імовірносно-часових графів, що дозволило: *визначити* початкові параметри системи; *визначити* статистичні показники роботи сервісу; *розробити* модель, що дозволяє оцінити динаміку зміни станів сервісу; *виявляти* низькоінтенсивні атаки прикладного рівня на відмову в обслуговуванні за рахунок застосування моделі оцінки динаміки зміни станів сервісу;

3) комплексний метод виявлення та класифікації низькоінтенсивних мережевих атак на відмову в обслуговуванні, які реалізуються на прикладному рівні, що дозволило: *виявити* атаки на відмову в обслуговуванні за рахунок розробленої моделі; *врахувати* особливості низькоінтенсивних атак, що реалізуються саме на прикладному рівні; *зменшити* імовірність помилок як першого, так і другого роду у мережевих системах захисту.

Теоретична і наукова цінність та практичне значення одержаних автором наукових результатів полягає в подальшому розвитку теоретичних та практичних методів і моделей підвищення якості надання послуг у мультисервісних мережах за рахунок вдосконалення моделей і показників доступності та захищеності від мережевих атак типу "відмова в обслуговуванні", що реалізуються на прикладному рівні.

Практична цінність дисертації обумовлена позитивним ефектом від використання результатів дисертаційної роботи у складі систем мережевої безпеки хмарного середовища.

Результати роботи використані в навчальному процесі Харківського національного університету радіоелектроніки, та університету ВТН, королівство Швеція.

Оцінка мови та стилю викладання дисертації та автореферату. Дисертація та автореферат написані грамотно, а стиль викладення в них матеріалів досліджень, наукових положень, висновків і рекомендацій відповідає вимогам стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки» й у цілому забезпечує доступність їх сприйняття.

Зміст автореферату відображає основні результати роботи, які приведені в дисертації. Дисертація по тематиці і результатам відповідає паспорту спеціальності 05.12.02 – "Телекомунікаційні системи та мережі".

Повнота викладення наукових результатів дисертації в опублікованих роботах. Основні положення та висновки дисертаційної роботи опубліковано в 19 наукових працях, серед яких 6 статей та 11 матеріалів конференцій. Усі виконані у співавторстві. Всі статті опубліковані в наукових фахових виданнях, 2 з них в іноземному фаховому

виданні. Всі конференції проходили під егідою IEEE, а відповідні матеріали викладені в наукометричних базах Scopus та IEEE Xplore Digital Library. У роботі та авторефераті досить чітко вказано особистий вклад дисертанта при отриманні нових наукових результатів.

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації. Стиль викладення автореферату в цілому забезпечує його доступність та сприйняття. В ньому чітко і лаконічно викладені наукові завдання дослідження та шляхи їх вирішення. З тексту зрозуміла наукова і практична значущість роботи, особистий внесок здобувача.

Недоліки та зауваження.

1) Автором не досить чітко показано переваги щодо використання ланцюгів Маркова в якості апарату моделювання станів web-серверу при вирішенні задачі моделювання сервісів, що надаються у телекомунікаційній мережі, яка використовує хмарне середовище.

2) Автором розроблено модель станів web-серверу, що базується на паралельному обслуговуванні запитів сервером. Такий підхід може буди використаний для розробки моделей будь-якого сервісу, що використовують протокол транспортного рівня TCP.

В дисертаційній роботі автор недостатньо повно розглянув можливості застосування моделі станів web-серверу, яка базується на паралельному обслуговуванні запитів сервером для сервісів прикладного рівня, що використовують таку ж модель з'єднань.

3) Для вирішення задачі прогнозування переходу сервісу у стан "відмова в обслуговуванні" автором використано апарат імовірносно-часових графів. Автор не навів достатнього обґрунтування щодо вибору методів розрахунку переходу системи з одного стану в інший.

4) В першому розділі дисертаційної роботи автор приділяє значну увагу хмарним інфраструктурам і забезпеченню якості саме у таких системах. Однак, при дослідженні ефективності розробленого методу виявлення низькоінтенсивних атак автором проведено експеримент відносно лише одного web-серверу. Проведення експерименту відносно реальної хмарної системи дозволило б більш чітко говорити про ефективність запропонованого автором методу.

5) В тексті роботи та в авторефераті мають місце описки та інколи використовуються терміни і позначення без пояснень, які не є загальновідомими або загальноприйнятими.

Зазначені недоліки суттєво не впливають на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значимості.

3. Відповідність дисертаційної роботи встановленим вимогам та загальний висновок

Дисертаційна робота Андерса Карлссона за темою "Модель та метод виявлення низькоінтенсивних атак на прикладному рівні" є завершеним, одноосібно написаним науковим дослідженням, що:

1) являє собою системне дослідження, проведене з певною метою;

2) має внутрішню єдність і свідчить про особистий внесок автора в науку;

3) розв'язує актуальну задачу, яка має важливу наукову і практичну спрямованість.

За актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота Андерса Карлссона відповідає паспорту спеціальності 05.12.02 – "Телекомунікаційні системи та мережі", а також

вимогам п. 9, 11, 12, «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. №567 (зі змінами) щодо дисертацій на здобуття наукового ступеня кандидата технічних наук, а її автор Андерс Карлссон заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – "Телекомунікаційні системи та мережі".

Офіційний опонент
доктор технічних наук, доцент,
професор кафедри інформаційної та кібернетичної безпеки
навчально-наукового інституту захисту інформації
Державного університету телекомунікацій В.В.Семко

Підпис Семка
засвідчую.
Учений секретар
О.В.Кожем