Голові спеціалізованої вченої ради Д 64.052.09 при Харківському національному університеті радіоелектроніки
61166, м. Харків, пр. Науки, 14

ВІДГУК

офіційного опонента професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, доктора технічних наук, професора Толюпи Сергія Васильовича на дисертацію Андерса Карлссона на тему "Модель та метод виявлення низькоінтенсивних атак на прикладному рівні", подану на здобуття вченого ступеня кандидата технічних наук за спеціальністю 05.12.02 - "Телекомунікаційні системи та мережі"

1. Актуальність теми дисертаційної роботи

Інфокомунікаційні технології глибоко проникають у всі сфери діяльності сучасного суспільства. Системоутворюючою основою інфокомунікаційних систем є телекомунікаційні системи на базі яких будуються мультисервісні мережі, зокрема, ті, що використовують хмарне середовище у якості технологічної платформи.

Сучасні телекомунікаційні системи знаходяться в умовах постійно тиску з боку зловмисників. У теперішній час існує досить велика кількість загроз порушення функціонування телекомунікаційних систем. Одна з найбільших – це мережеві атаки на відмову в обслуговуванні, так звані DOS-атаки. В останній час спостерігається не тільки збільшення їх кількості та потужності, але й підвищення складності та використання нових механізмів, зокрема реалізація на верхніх рівнях моделі OSI. Забезпечення гарантованих параметрів якості обслуговування неможливо без врахування питань мережевої безпеки, зокрема захисту від DOS-атак, що порушують доступність сервісів у мультисервісній мережі.

Здобувач акцентував увагу саме питанню підвищення доступності сервісів у мультисервісній мережі, що використовує хмарне середовище, так як саме доступність сервісу є ключовою характеристикою мультисервісної мережі.

Сучасні засоби захисту мультисервісних мереж мають досить високу ефективність у випадку DOS-атак, що реалізуються на мережевому та канальному рівнях. У той же час, для низькоінтенсивних атак прикладного рівня, що набувають все більшої популярності такі системи майже неефективні. В першу чергу такий стан пов'язаний з особливостями реалізації низькоінтенсивних DOS-атак. Такі атаки майже не викликають підвищення трафіку у мережі. Відповідно й системи захисту, алгоритми яких у першу чергу пов'язані з виявленням аномалій у трафіку, не спрацьовують.

Вирішення вказаних проблем можливо лише при впровадженні нових методів та засобів виявлення низькоінтенсивних атак, що дозволять врахувати особливості їх реалізації.

У зв'язку з цим актуальним є формулювання та вирішення важливої **науково-прикладної задачі**, що пов’язана вдосконаленням систем мережевого захисту за рахунок з розробки моделей та методу виявлення низько інтенсивних DOS-атак, а відповідно й підвищенню доступності сервісів у мультисервісній мережі, що є досить актуальною задачою.

2. Наукова новизна результатів роботи

До основних нових наукових результатів дисертаційної роботи слід віднести:

1. Вперше розроблено модель виявлення низькоінтенсивних атак на відмову в обслуговуванні що реалізуються відносно web-серверу. Використання ланцюгів Маркова для розробки моделі є новизною запропонованого підходу. Розроблена модель дає змогу аналізувати поведінку сервера, що атакується та обчислити ймовірність переходу web-серверу у стан «відмова в обслуговуванні». Застосування розробленої моделі дає можливість запровадити попереджувальні кроки та запобігти стані «відмови в обслуговуванні».

2. Вперше розроблено модель аналізу навантаження web-серверу на основі імовірностно-часових графів. Застосування розробленої моделі дає можливість обчислювати час переходу сервера у стан «відмова в обслуговуванні» та оцінити динаміку реалізації мережевої атаки, а також обрати контрзаходи для зниження її ефективності.

3. Вперше, розроблено метод виявлення та класифікації низькоінтенсивних атак типу «відмова в обслуговуванні» на web-сервіси. На відміну від існуючих розроблений метод базується на аналізі стану захищаємого сервісу, а не пошуку аномалій у мерефевому трафіку.

3. Практична значимість наукових результатів

Практична значимість результатів досліджень полягає в тому, що запропоновані математичні моделі і методи можуть бути використані підчас розробки, підтримки, проектування та впровадження різноманітних мультисервісних хмарних систем. Запропонований метод виявлення та класифікації низькоінтенсивних атак був використаний для захисту хмарної лабораторії ReSeLa, та застосовується для підготовки фахівців у галузі інформаційної безпеки. Матеріали дисертаційної роботи використано в навчальному процесі кафедри інфокомунікаційних систем ХНУРЕ в курсі «Методи колективного захисту інформації».

4. Достовірність отриманих результатів

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується коректним використанням ключових положень добре відомого та апробованого математичного апарату – ланцюгів Маркова, теорії управління багаторівневими системами, теорії множин, теорії графів та поширеними підходами до процесу реплікації та методів балансування навантаження, співпаданням експериментальних результатів з теоретичними.

5. Особистий внесок та реалізація результатів дисертації

5.1 Особистий внесок здобувача.

Усі основні наукові результати, що висвітлено в дисертаційній роботі, згідно списку публікацій, здобувач отримав самостійно. В одній з робіт автором особисто розроблено імітаційну модель низькоінтенсивної атаки прикладного рівня на хмарне середовище, В іншій автором розроблена модель поведінки web-серверу на базі ланцюгів Маркова. В окремій роботі автором розроблена модель, що дозволяє розрахувати час переходу web-сервера у стан «відмова в обслуговуванні». В одній з робіт автором запропоновано метод виявлення та класифікації Slow-http атак на хмарні системи та розроблено модель Slow-http атаки на соціальні мережі.

Таким чином основні результати дисертаційної роботи опубліковані в дев'ятнадцяти наукових працях: одна стаття у закордонному фаховому журналі, п'ять статей у фахових науково-технічних журналах та збірках наукових праць. Апробація результатів дисертації проходила у ході десяти доповідей на міжнародних науково-технічних конференціях, які проходили під егідою IEEE та індексуються в міжнародних наукометричних базах Scopus та IEEE Xplore Digital Library.

5.2 Реалізація результатів досліджень

Запропонований метод виявлення та класифікації низькоінтенсивних атак був використаний для захисту хмарної лабораторії ReSeLa, та застосовується для підготовки фахівців у галузі інформаційної безпеки. Матеріали дисертаційної роботи використано в навчальному процесі кафедри інфокомунікаційних систем ХНУРЕ в курсі «Методи колективного захисту інформації».

6. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

Дисертаційна робота носить завершений характер науково дослідної роботи та подана у вигляді вступу, чотирьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 150 сторінок, в тому числі 130 сторінок основного тексту, 40 рисунків та 8 таблиць на 13 сторінках. Список використаних джерел містить 110 найменувань, викладених на 10 сторінках.

Автореферат дисертаційної роботи в повній мірі відображає наукові та практичні результати, що подані в дисертаційній роботі.

У **вступі** розкрито стан проблем, що досліджуються, обґрунтовано актуальність теми дисертаційної роботи, визначено мету досліджень та ряд науково-практичних задач, що потребують вирішення задля досягнення поставленої мети. Наведено наукову новизну та практичну значимість отриманих результатів. Надано дані щодо апробації отриманих результатів та публікації автора за темою дисертації.

У **першому розділі** проведено аналіз 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. У результаті аналізу було встановлено, що сучасні мультисервісні мережі широко використовують хмарне середовище для організації та надання послуг. Даний вибір в першу чергу обумовлений тим,

що при розробці мультисервісних систем в області інфраструктури основна взаємодія між компонентами виконується або на базі SOA технологій, або REST. В основу обох технологій покладено механізм взаємодії по протоколу HTTP, тобто через web-сервер. Тому саме низькоінтенсивні атаки типу «відмова в обслуговуванні» на web-сервер (Slow-http атаки) є найбільш ефективними засобом, що дозволяє суттєво знизити рівень доступності всього хмарного середовища. Цьому типу атак і було приділено найбільшу увагу з метою з'ясування основних сценаріїв їх реалізації та особливостей впровадження.

Таким чином виникає задача модифікації вищевикладених підходів і використання їх в доповненні з іншими існуючими математичними апаратами що дозволить виявляти і прогнозувати виникнення Slow-http атак, на підставі визначених параметрів web-серверу.

У **другому розділі** проведено аналіз особливостей реалізації Slow-http атак. Встановлені основні математичні закономірності між параметрами атаки та станом web-сервера, що атакується. Це дозволило розробити відповідну математичну модель поведінки сервера під час атаки. Отримано розподіл ймовірностей стану web-серверу під час реалізації Slow-http атак різного типу. Адекватність математичної моделі підтверджено практичним експериментом. Дослідження природи Slow-http атак показали, що в процесі реалізації потік заявок з джерела атаки можна вважати найпростішим. Про це свідчить те, що досліджуваний потік заявок володіє трьома властивостями, характерними для найпростішого потоку: стаціонарність, ординарність і відсутність наслідків.

У **третьому розділі** розроблено математичну модель прогнозування стану «відмова в обслуговуванні» для web-серверу. Модель базується на аналізі динаміки переходів між станами серверу. Аналіз засобів моделювання динаміки станів мультисервісних мереж показав, що найбільш прийнятним засобом є ймовірносно-часові графи. Даний математичний апарат дозволяє зв'язати модель станів системи, що отримана у попередньому розділі з динамікою функціонування системи. Аналіз характеру залежності показав, що вона є нелінійною. Характер нелінійності слід враховувати при визначенні порогових показників спрацьовування системи попередження про атаку.

У **четвертому розділі** розроблено загальний метод виявлення та класифікації slow-http атак на web-сервер. Метод ґрунтується на моделях стану та динаміки функціонування web-сервера. Виконана практична імплементація методу у якості системи виявлення та попередження про мережеву атаку на web-сервер. Ефективність практичної реалізації методу перевірялась при захисті хмарного середовища мультисервісної мережі. Проведений експеримент показав спроможність виявляти slow-http атаки в різних варіантах їх реалізацій та запобігати стану «відмова в обслуговуванні». Розроблені математичні моделі, що дозволяють розраховувати розподіл ймовірностей станів web-серверу в залежності від параметрів вхідного та вихідного потоків можуть буди використані як ядро системи виявлення та протидії мережевим атакам на web-сервери.

У висновках викладено основні результати дисертаційної роботи, розв'язана актуальна науково-прикладна задача, що полягає у підвищенні доступності послуг, що надаються мультисервісною мережею за рахунок вдосконалення іс-

нуючих та розробки нового методу виявлення мережевих атакрозкрито їх наукову та практичну цінність.

За результатами оцінки тексту дисертаційної роботи можна зробити висновок, що твердження та результати, основні висновки, що подані в дисертаційній роботі, сумнівів не викликають. Результати наукових та практичних досліджень дисертаційної роботи Андерса Карлссона вже знайшли практичну реалізацію в захисті хмарної лабораторії ReSeLa, та застосовується для підготовки фахівців у галузі інформаційної безпеки.

7. Мова та стиль викладення наукових положень

Автор дисертації логічно, грамотно й обґрунтовано викладає результати досліджень і отримані ним наукові положення. Текст дисертації та автореферат написані грамотною, лаконічною, науково-технічною мовою. Автореферат ідентичний змісту дисертації, достатньо повно розкриває основні положення дисертаційної роботи.

8. Недоліки та зауваження

В якості основних недоліків та рекомендацій по дисертаційній роботі необхідно відмітити такі:

1. Під час проведення експерименту з дослідження особливостей реалізації низько інтенсивних DOS-атак на web-сервіси автором недостатньо уваги було приділено питанню як саме такі атаки впливають на якість функціонування всього хмарного середовища. Дослідження цього питання підсилило б обґрунтованість дослідження саме цього типу атак.

2. Для аналізу адекватності розробленої моделі web-серверу автором проведено експеримент в при реалізації якого ідентичність отриманих результатів до математичної моделі показана досить поверхнево. Нажаль автором не наведено статистичних параметрів (розмір вибірки, інтервал довіри, статистична похибка), що показують точність отриманих результатів.

3. У вступі та першому розділі автором багато уваги приділено питанням побудови та безпеки хмарних середовищ та мультисервісних мереж що базуються на сервіс-орієнтованій архітектурі (SOA). Однак у подальшому автор сконцентрував свою увагу лише на окремому web-сервісі. На мою думку отримані результати мали б більш вагомий вигляд у разі, якщо б автор більш детально показав вплив низько інтенсивних DOS-атак на всю систему загалом, та як запропонований їм метод підвищує показники якості всієї системи.

4. При розробці моделі прогнозування часу переходу web-сервера у стан «відмова в обслуговуванні» автором отримані досить цікаві результати щодо характеру залежності часу від параметрів атаки, однак чомусь ці результати не в повному обсязі були використані при класифікації типу низько інтенсивної DOS-атаки.

5. В дисертаційній роботі міститься стилістичні погрішності та неточності, наприклад дивись сторінки: 9, 24, 26, 45-50, 58-59, 71, 85, 102, 105, 119.

Вказані недоліки та зауваження не впливають на загальний висновок про дисертаційну роботу.

8. Загальні висновки

8.1 Дисертація Андерса Карлссона є закінченою науково-дослідною роботою, яка містить теоретичне узагальнення та нове рішення важливого науково-практичного завдання, що пов'язане з вдосконаленням систем мережевого захисту за рахунок з розробки моделей та методу виявлення низько інтенсивних DOS-атак, а відповідно й підвищенню доступності сервісів у мультисервісній мережі.

8.2 Дисертаційна робота виконана і оформлена відповідно до вимог, затверджених ВАК України, написана зрозуміло і грамотно, науково-технічна термінологія використовується коректно, структура роботи логічна.

8.3 Здобувач отримав нові наукові результати, що в сукупності та за своїм значенням вносять певний внесок в розвиток систем мережевого захисту, а відповідно й підвищенню доступності сервісів у мультисервісній мережі.

8.4 Зміст дисертації відповідає паспорту спеціальності 05.12.02 - "Телекомунікаційні системи та мережі"

8.5 За науковим рівнем, практичною цінністю, апробацією та публікаціями дисертаційна робота відповідає вимогам пп. 9,11,12,13 "Порядку присудження наукових ступенів", затвердженого постановою КМУ №567 від 24.07.2013 р. (зі змінами, внесеними згідно з Постановами КМУ №656 від 19.08.2015 р., №1159 від 30.12.2015 р. та №567 від 27.07.2016 р.), а її автор – Андерс Карлссон – заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

Офіційний опонент:
професор кафедри кібербезпеки та захисту
інформації Київського національного
університету імені Тараса Шевченка
доктор технічних наук, професор С. В. Толюпа