УДК 621.618:519 **А.О. Аносов**

МОДЕЛЮВАННЯ DDos АТАК НА КОМП'ЮТЕРНІ МЕРЕЖІ ДЛЯ ВИЗНАЧЕННЯ ОЗНАК ЇХ ПРОВЕДЕННЯ

У статті досліджено можливість своєчасного виявлення DDos атак на складні ієрархічні комп'ютерні мережіу процесі обміну інформацією на основі визначення залежності ступеня порушення оперативності інформаційного обміну від коефіцієнтів зниження інтенсивності обслуговування пакетів даних при їх формуванні і передачі та коефіцієнту збільшення інтенсивності звертання серверів до транзакцій, що обумовлені застосуванням DDos атак.Визначено, що факт аномального збільшення інтенсивності звертання робочих станцій (серверів) до транзакцій може бути використаний у якості ознаки проведення DDos атак.

Ключові слова: комп'ютерні мережі, оперативність інформаційного обміну, захищеність комп'ютерних мереж, модель комп'ютерних мереж.

Вступ і постановка задачі

Результати дослідження, проведеного «Лабораторією Касперского» свідчать, що масовані DDos-атаки проти мережевих ресурсів компаній спричиняють збитки в середньому розмірі від 52 до 444 тисяч доларів, залежно від розміру організації, яка потрапила під вплив зловмисників [1], є основним видом порушення функціонування комп'ютерних мереж (КМ)[2,3]. Однак, в багатьох випадках для нанесення досить великих збитків фірмі достатньо забезпечити досягнення необхідного зниження середнього часу обробки даних транзакції та серверах і середнього часу очікування і передачі даних транзакції по Ethernet. Використання такого підходу зловмисником при проведенні DDos-атаки забезпечить скритність впливу тата дозволить отримати керований ефект.Ці питання не дослідженні у повному обсязі. Тому є актуальним дослідити можливість своєчасного виявлення DDos атак у процесі обміну інформацією для обґрунтування раціональних способів захисту від таких атак.

Питання проведення DDos атак на комп'ютерні мережі розглянуті в [1-3]. Моделі елементів складних ієрархічних комп'ютерних мереж розроблені в [4] в умовах здійснення DDos атак. Модель складних ієрархічних комп'ютерних мереж як об'єктів DDos атак розроблена в [5]. Отримані результати [4, 5] створюють наукову базу для практичного дослідження впливу DDos атак на елементи комп'ютерних мереж та своєчасність отримання інформації.

Це робить можливим дослідити на основі розробленої в [4,5] моделі ознаки впливу та визначити підходи до оцінки ефективності виявлення DDos Атак.

На основі розробленої в [5] моделі комп'ютерних мереж дослідити зміни середнього часу обробки даних транзакції у робочій станції та сервері, коефіцієнту K_{no}^{KM} порушення оперативності інформаційного обміну від коефіцієнтів зниження інтенсивності обслуговування пакетів даних при їх формуванні і передачі та коефіцієнту збільшення інтенсивності звертання серверів до транзакцій, що обумовлені застосуванням DDos атак.

Виклад основного матеріалу досліджень

При моделюванні основним показником захищеності комп'ютерних мереж в умовах DDos атак пропонується обрати коефіцієнт $0 \le K_{no}^{KM} < 1$ – порушення оперативності інформаційного обміну [5,6]. Зауважимо, що K_{no}^{KM} по суті визначає ймовірність того, що за результатами застосування DDos атак споживачі отримають потрібну інформацію не своєчасно.

Частковими показниками якості функціонування елементів комп'ютерних мереж в умовах DDos атак пропонується обрати [5,6]:

$\overline{T}_{\text{рс}}, \overline{T}_{\text{с}}$ – середній час обробки даних транзакції у робочій станції та сервері відповідно;

$\overline{T}_{\text{рм}}, \overline{T}_{\text{е}}, \overline{T}_{\text{тпм}}$ – середній час очікування і передачі даних транзакції через радіомережу, Ethernet, пакетами.

Вихідні данні для проведення моделювання визначені виходячи з аналізу технічних характеристик та принципів побудови робочих станцій, серверів та глобальних комп'ютерних мереж.

Для моделювання визначені такі показники:

зниження інтенсивності обслуговування пакетів даних транзакцій при їх формуванні $C_{об\,ф}$ і передачі – $C_{об\,п}$ за рахунок впливу DDos атак;

збільшення інтенсивності $C_{із}$ звертання робочої станції (серверу) до транзакцій, що обумовлені DDos атаками.

Розглянемо приклад моделювання впливу часткових показників елементів комп'ютерних мереж на коефіцієнт $K_{по}^{КМ}$ порушення оперативності інформаційного обміну в умовах DDos атак. Вважаємо, що критерієм захищеності комп'ютерних мереж від DDos атак є забезпечення виконання критерію

$$0 < K_{по}^{КМ} \le K_{нсоі}^{КМ}, \qquad (1)$$

де - $K_{нсоі}^{КМ}$ - значення коефіцієнту $K_{по}^{КМ}$ при якому відбувається несвоєчасне отримання інформаціїдля якісного функціонування офісів.

Потрібно зауважити, що значення $K_{нсоі}^{КМ}$ залежить від сфери діяльності офісів. Наприклад у біржовій діяльності цей коефіцієнт буде невеликий. Такий, що порушення оперативності інформаційного обміну не буде перевищувати декількох хвилин. По суті $K_{нсоі}^{КМ}$ визначає, що отриманні данні втратили свою цінність та достовірність через «старіння».

Дослідження можливості застосування моделей комп'ютерних мереж для оцінки їх захищеності в умовах DDos атак проводились з урахуванням алгоритмів, що запропоновано в [7]. За допомогою розробленої в [5] моделі комп'ютерних радіомереж було досліджено ступень порушення оперативності інформаційного обміну в умовах DDos атак на рівнях "офіс", "філіал", "регіональний офіс", "центральний офіс" в залежності від коефіцієнту збільшення інтенсивності звертання серверів до транзакцій в мережі, проведено моделювання залежності коефіцієнту порушення оперативності інформаційного обміну на рівнях "офіс", "філіал", "регіональний офіс", "центральний офіс" від кількості робочих станцій, серверів, при різних значеннях інтенсивності DDos атак, визначено залежності середнього часу очікування і передачі даних транзакції по шині Ethernet від коефіцієнту збільшення інтенсивності звертання серверів до транзакцій в межах для різних швидкостей передачі даних.

Залежності порушення оперативності інформаційного обміну в умовах DDos атак на рівнях "офіс", "філіал", "регіональний офіс", "центральний офіс"від коефіцієнту збільшення інтенсивності звертання серверів до транзакцій в межах представлені на рис. 1.

Особливістю впливу DDos атак на параметр збільшення інтенсивності звертання робочої станції (серверу) є її експонентний характер від зміни завантаження шини Ethernet. Зокрема, аналіз рис.1 показав, що у діапазоні змін збільшення інтенсивності звертання від 0.1до 0.25 відмічається різке погіршення показника коефіцієнт порушення оперативності інформаційного обміну від 0,2 до 0,999. Це обумовлено наявністю критичного значення навантаження шини Ethernet. При наближенні значень завантаження шини Ethernet до критичного ймовірність несвоєчасного отримання інформації наближається до одиниці.

Тому коефіцієнт збільшення інтенсивності звертання серверів до транзакцій в межах може бути використаний для виявлення факту проведення зловмисникамиDDos атак та прогнозування їх дій та, в залежності від коефіцієнту порушення оперативності

інформаційного обміну для обраної системи, спрогнозувати можливі збитки, а такожвизначити подальші дії щодо нейтралізації атаки.

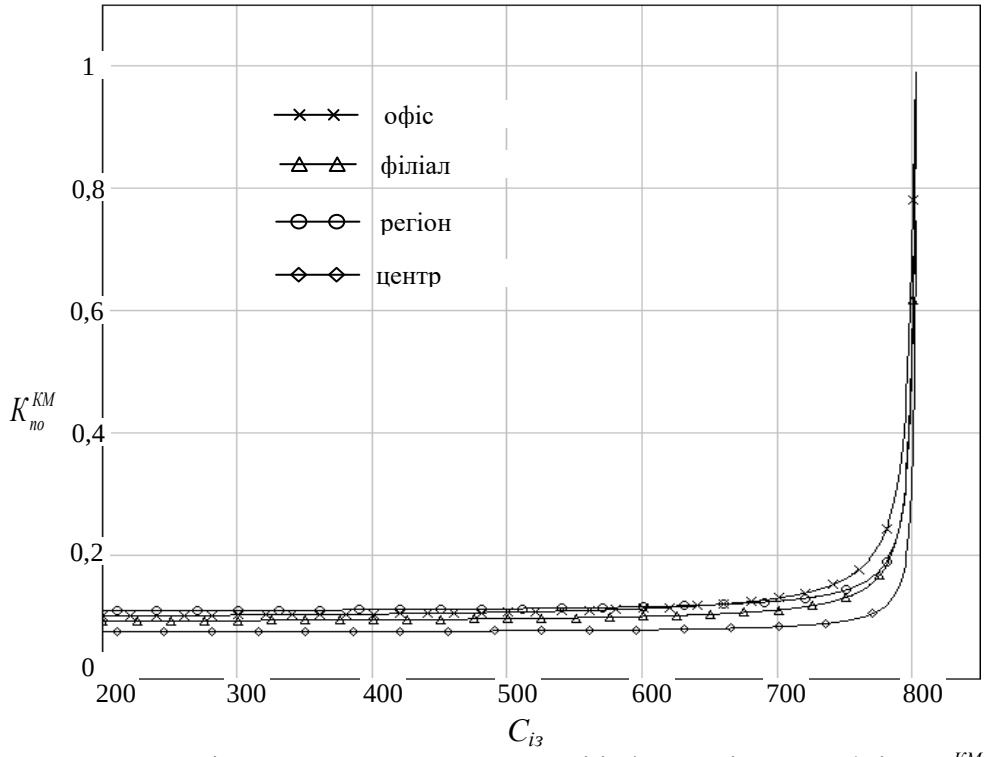

Рис. 1. Залежності порушення оперативності інформаційного обміну $K_{по}^{КМ}$ в умовах DDos атак на рівнях “офіс”, “філіал”, “регіональний офіс”, “центральний офіс” від коефіцієнту збільшення інтенсивності звертання серверів до транзакцій в мережі

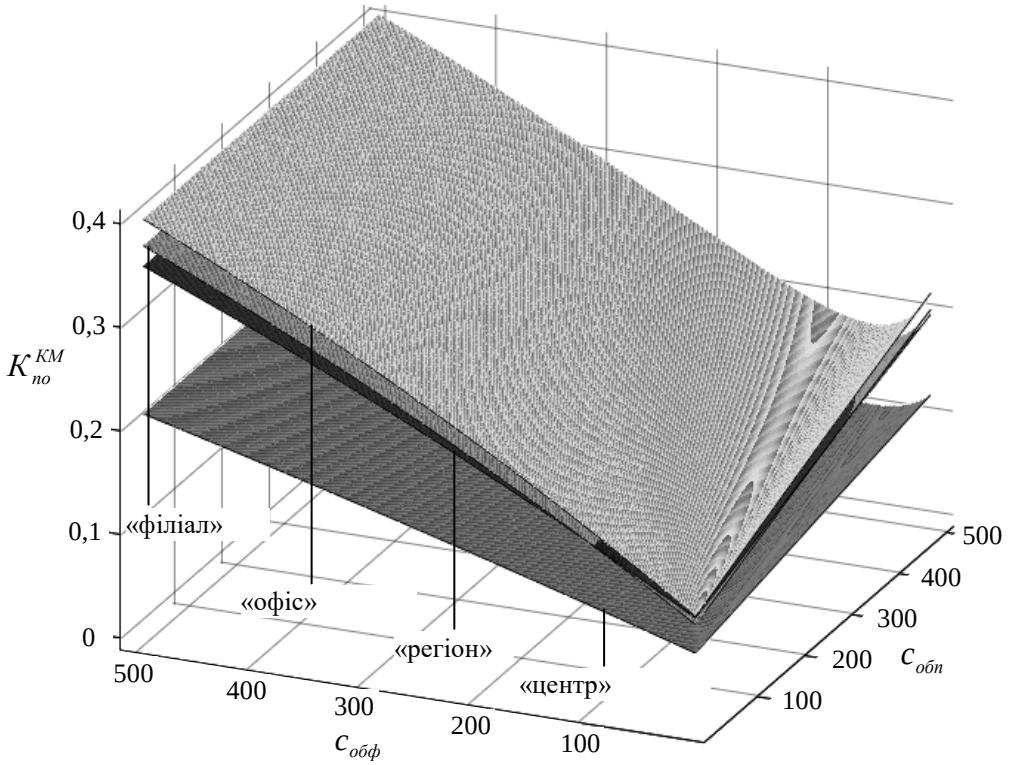

Рис.2. Результати моделювання залежності коефіцієнту $K_{по}^{КМ}$ - порушення оперативності інформаційного обміну на рівнях “офіс”, “філіал”, “регіональний офіс”, “центральний офіс” від кількості робочих станцій, серверів, при різних значеннях інтенсивності DDos атак

Аналіз результатів моделювання показав, що застосування DDos атак, вплив яких спрямований на зниження інтенсивності обслуговування пакетів даних при їх формуванні та при передачі по шині сервера (робочій станції), є найбільш ефективним у нижчих ланках – «офіс», «філіал». При цьому існує множина таких взаємних значень коефіцієнтів зниження інтенсивності обслуговування $C_{об\,ф}$ та $C_{об\,п}$, рис.2, при яких середній час обробки даних транзакції $T_{рс}$ у мережі досягає локального мінімуму. При наближенні значень завантаження шини Ethernet до критичного ймовірність несвоєчасного отримання інформації наближається до одиниці. Тому коефіцієнт $C_{об\,ф}$ та $C_{об\,п}$ збільшення інтенсивності звертання робочих станцій (серверів) до транзакцій в межах мережі може бути використаний для виявлення факту прогнозування та проведення DDos атак При цьому першочерговим об'єктом атаки є процеси формування пакетів даних у серверах мережі.

Узагальнені результати моделювання залежності середнього часу очікування і передачі даних транзакції по шині Ethernet $\overline{T}_{\text{е}}$ від коефіцієнту $C_{із}$ збільшення інтенсивності звертання РС (серверів) до транзакцій в межах ЛОМ для різних значень швидкостей передачі даних приведена на рис. 3.

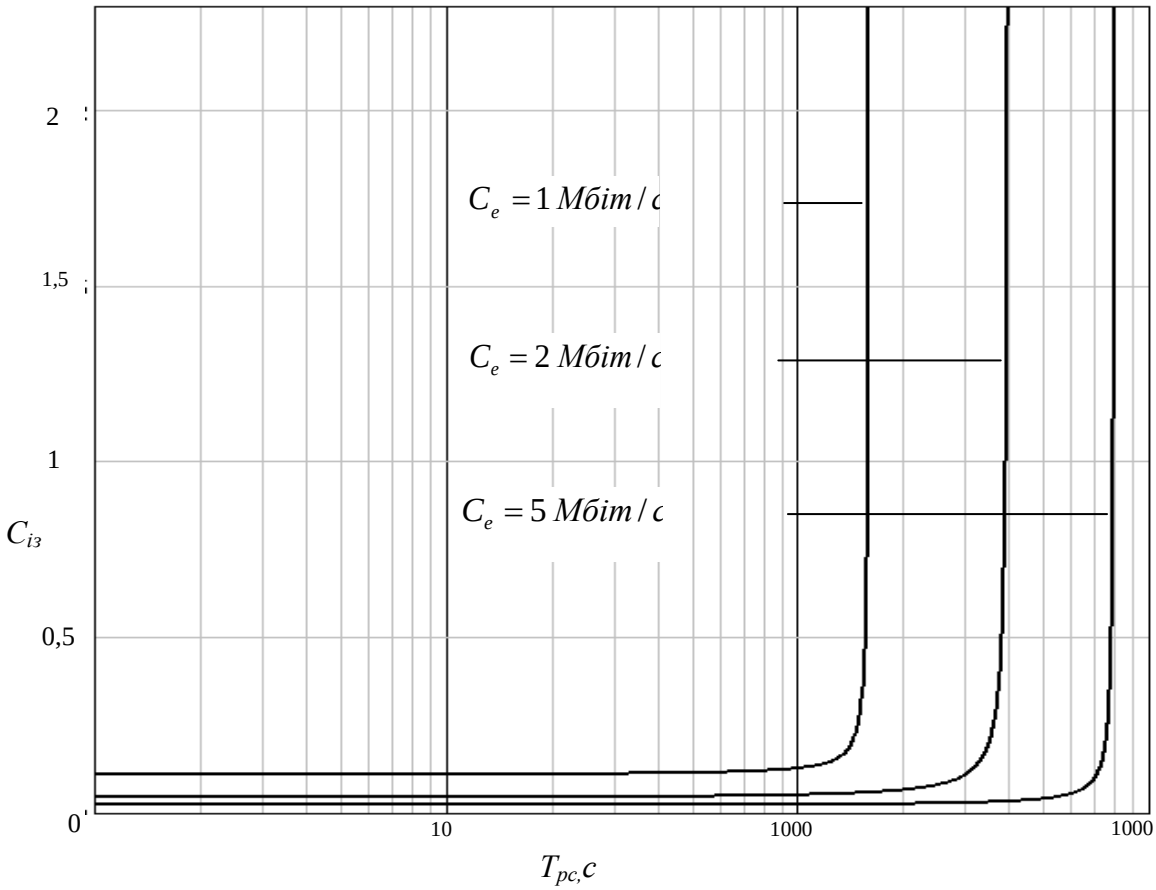

Рис. 3. Залежності середнього часу очікування і передачі даних транзакції по шині Ethernet від коефіцієнту збільшення інтенсивності звертання серверів до транзакцій в межах для різних швидкостей передачі даних

Переломи в графіках обумовлені такими значеннями коефіцієнту збільшення інтенсивності звертання до транзакцій $c_{із}$, при яких завантаження шини

Ethernetнаближається до критичного значення 0,35. При цьому продуктивність шини Ethernet стає критично малою, а середній час очікування і передачі даних транзакції росте необмежено.

Результати, висновки і рекомендації

Аналіз результатів моделювання показав адекватність часткових моделей робочої станції, серверу, шини Ethernet, як об'єктів впливуDDos атак. Отримані результати моделювання не суперечать відомим теоретичним викладкам та результатам натурних експериментів [4-8].

Визначено, що факт збільшення інтенсивності звертання робочих станцій (серверів) до транзакцій 0.1 до 0.25 може бути використаний у якості ознаки проведення DDos атак.

Отримані результати створюють базу для практичної реалізації програмного комплексу завчасного виявлення DDos атак на комп'ютерні мережі комерційної організації.

Напрямком подальших досліджень можна визначити розробку методики раціональних способів завчасного виявлення DDos атак на комп'ютерні мережі та захисту від них.

Література

1.Сайт Лаборатории Касперского [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/analysis

2.Бурячок В.Л. Кіберзлочинність – як одна з найбільших загроз сучасності: прояви і тенденції її поширення, можливі заходи протидії / В.Л. Бурячок, О.А.Ільяшов // Збірник матеріалів Міжвідомчої НПК Національного університету оборони ЗС України, 07.10.2010, № 2(101), 2011, с. 129 - 131

3.Шолохов С. Н. Информационное оружие – новый класс вооружения для дезорганизации автоматизированных систем управления войсками и оружием при проведении информационных наступательных операций / С. М. Шолохов, Г .М. Сидченко С. А. // Сборник научных трудов ХВУ. – Х.: ХВУ. – 2002. – № 1(39). – С. 48 – 53.

4. Шолохов С. М. Програмно-комп'ютерне подавлення комп'ютерної транспортної мережі передачі даних тактичної ланки в операціях (бойових діях) / С. М. Шолохов, Е. В. Лучук // Труди академії. – 2005. – №59 – С. 144–152.

5. Аносов А.О. Математична модель комп'ютерних радіомереж сухопутних об'єднань – об'єктів програмно-комп'ютерного подавлення для забезпечення захисту інформації/ А.О.Аносов, С.М. Шолохов, Ю.А.Гоменюк // Збірник наукових праць А1906, – 2012. – № 76. – С. 78–91.

6. Бурячок В.Л. Показники та критерії надійності функціонування інформаційно-телекомунікаційних систем спеціального призначення / Бурячок В.Л.,К.А. Кураев // Збірник наукових праць в/ч А1906 МО України , 2014, № 38. - С. 34 - 47

7. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // Науково-технічний журнал «Захист інформації» Національного авіаційного університету, № 3, 2011, с. 19 – 27.

8. Лучук Е.В., Дис. канд. техн. наук, К. :НУОУ, 2006, 231 с.

Надійшла 27.08.2015 р. Рецензент: д.т.н., проф. Хорошко В.О.