Отже, запропоноване програмне забезпечення дає змогу кількісно змоделювати матеріальну, хвилеводну і дисперсію профіля показника заломлення, та виявити умови, за яких можна виготовити оптичні волокна з нульовою дисперсією.

1. Арчер Т., Уайтчепел Э. Visual C++ .NET. Библия пользователя / пер с англ. – М.: Издательский дом «Вильямс», 2003. 2. Дмитриев А. Л. Оптические системы передачи информации: учеб. пособие. – СПб: СПбГУИТМО, 2007. 3. Стерлинг Д.Дж. Техническое руководство по волоконной оптике. – М.: ЛОРИ, 1998. 4. Убайдуллаев Р.Р. Волоконно-оптические сети. – М.: Эко-Трендз, 2001.

УДК 621.391

О.І. Сиротинський, І.С. Беляєв, Т.А. Максимюк, М.І. Олексін
Національний університет "Львівська політехніка"

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД МЕРЕЖЕВИХ DDOS АТАК НА ОСНОВІ МАРКІВСЬКОЇ МОДЕЛІ ПОВЕДІНКИ БОТНЕТУ

Запропоновано приховану марківську модель DDoS атаки, яка являє собою результат двох випадкових процесів і забезпечує можливість визначення характеру поведінки ботів у інформаційній мережі. Це дає змогу ефективно визначати вразливі місця за рахунок декомпозиції мережі на окремі частини, що є необхідним для визначення найменш захищених її ланок. Модель дозволяє враховувати розміри, топологію та протоколи маршрутизації досліджуваної мережі. На основі цієї моделі розроблено алгоритм відбиття атаки шляхом аналізу вхідного трафіку при появі аномальних властивостей в мережі.

Ключові слова: ddos, мережева атака, ботнет.

The paper presents a hidden Markov model of network DDoS attack, which represents a result of two random processes. The advantage of the proposed model is a possibility of determination of bots behaviour in the information network. Such determination allows us to effectively identify weak spots by decomposition of the network into separated parts. Besides, this model allows considering additional factors, such as size, topology, and network routing protocols in the analized network. Designed algorithm, which is based on this model, repels attacks by analyzing incoming traffic during appearance of anomalous properties in the network.

Key words: ddos, network attack, botnet.

Вступ. Сьогодні, у зв'язку із інтенсивним розвитком інформаційних технологій, більшість людей не може уявити свого життя без сучасних засобів інфокомунікацій. Саме тому проблеми інформаційної безпеки є надзвичайно актуальними та важливими. Вони вимагають поглибленого аналізу та вивчення, адже із розвитком інформаційних технологій розвиваються і методи та види атак в інформаційному просторі.

Інформаційні системи створюються для надання певних послуг, тому, якщо внаслідок деяких обставин надати ці послуги неможливо, це завдає збитків всім суб'єктам інформаційних відносин. З позиції інформаційної безпеки основною загрозою доступності є мережеві атаки типу «розподілена відмова від обслуговування», або, як їх ще називають, DDoS (Distributed Denial of Service) атаки [1]. Мета таких атак – частково або повністю паралізувати роботу атакованого вузла мережі або ж усієї

мережі. Оскільки це спричиняє зниження якості отримуваних користувачем послуг, чи взагалі унеможливлює отримання будь-яких послуг, то важливим завданням є розроблення методів для забезпечення захисту від мережевих атак.

Для того, щоб підійти до методики виконання такого завдання, необхідно дослідити властивості мережевих атак з позиції інформаційної системи, що атакується, та з погляду мережі хостів, які беруть участь у атаці [2, 3]. Це дозволить здійснити оцінку впливу DDoS атак на корпоративну мережу залежно від потужності та типу атаки.

В результаті проведення аналізу мережевих атак різних типів розроблено приховану марківську модель мережевої DDoS атаки на основі теорії динамічного хаосу. Враховуючи критерії розподілу навантаження, сформовано алгоритм захисту від мережевих атак типу “розподілена відмова від обслуговування”.

Аналіз мережевих атак типу «розподілена відмова від обслуговування». DDoS атака – це атака на обчислювальну систему з метою вивести її ресурси з ладу, зробити недоступними для користувачів. DDoS атаки організовуються за допомогою ботнетів (botnet) – мережі інфікованих хостів (ботів). Схематично атака виглядає приблизно так: на вибрану жертвою інформаційну систему надходить величезна кількість помилкових запитів з сотень, тисяч хостів з різних кінців світу. В результаті цього сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів.

Коротко суть мережевої атаки можна описати так: через керуючу консоль зловмисник зв’язується з головними серверами ботнету, з яких безпосередньо відправляються команди інфікованим хостам, що формують сотні запитів різних типів, якими атакується вузол-мішень. Архітектура кластера DDoS наведена на рис.1.

Рис. 1. Архітектура кластера DDoS

Математична модель DDoS атаки. Оскільки поведінка ботів є нелінійним псевдовипадковим процесом, ботнет описується як система з динамічним хаосом [4]. Така система характеризується неконтрольованою динамікою та чутливістю до первинного стану. Під первинним станом розуміють множину хостів, які заражені безпосередньо зловмисником. Після зараження динаміка ботнету стає неконтрольованою і залежить лише від співвідношень первинної множини

ботів з іншими хостами в мережі. Випадкові стани окремо взятого хоста – дискретні (уражений або неуражений), а процес DDoS атаки є неперервним в часі [5]. У цьому випадку для аналізу такого процесу можна застосувати приховану марківську модель, що зображена на рис. 2.

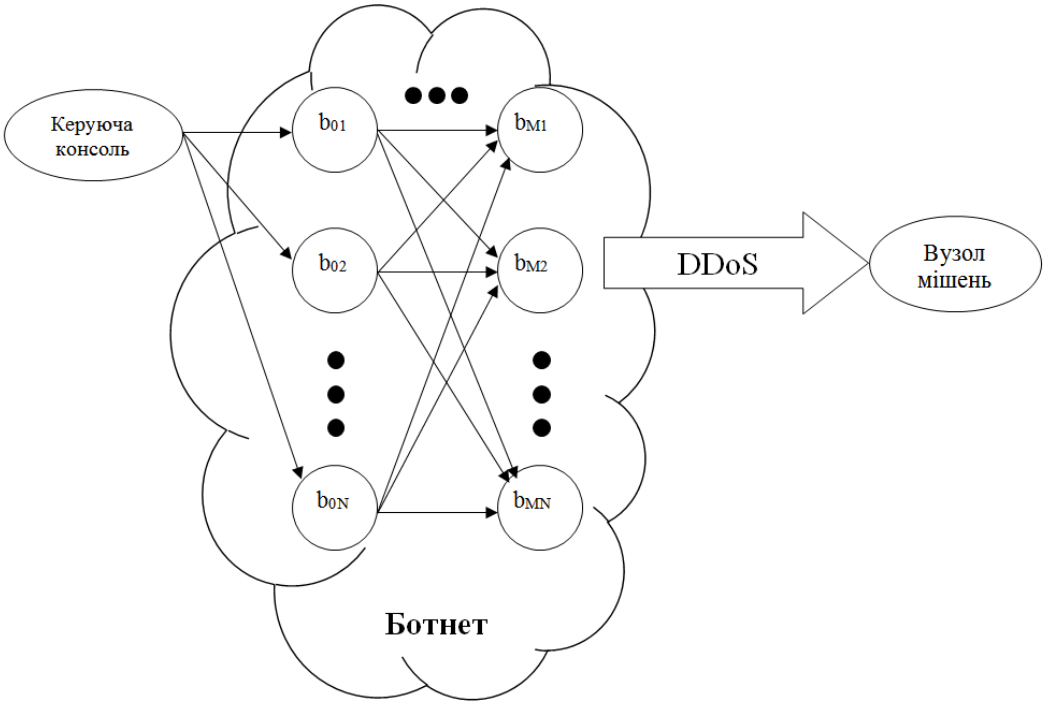

Рис. 2. Графічне представлення марківської моделі ботнету

Зловмисник через керуючу консоль уражає декілька хостів, створюючи первинний вектор з N ботів. Кожен бот характеризується коефіцієнтом b_{ij}, який визначають за формулою:

$$b_{ij} = 0.5 \cdot \lfloor f(C_{ij}, P_{ij}) \rfloor , \quad (1)$$

де C_{ij} – пропускна здатність зовнішнього каналу хоста; P_{ij} – продуктивність ЕОМ.

$$P = A \cdot F_{CPU} + B \cdot M_{RAM} , \quad (2)$$

де F_{CPU} – тактова частота центрального процесора; M_{RAM} – об'єм оперативної пам'яті A,B – коефіцієнти, значення яких вибирають відповідно до типу атаки ($A+B=1$).

Розглянемо впорядковану множину станів ботнету X_0, X_1, X_2, …, X_k як марківський процес загибелі та розмноження для випадку, коли боти не тільки атакують ціль, а й інфікують інші хости, встановлюючи на них свої копію, тобто роблячи їх ботами. В момент часу t_k система перебуває в стані X_k, а переходи можуть здійснюватись лише між сусідніми станами. На рис. 3 показано переходи станів ботнету, як частковий випадок байєсівського ланцюга. Суцільними лініями показано перехід у разі зростання кількості ботів, а штриховими, відповідно, у разі зменшення.

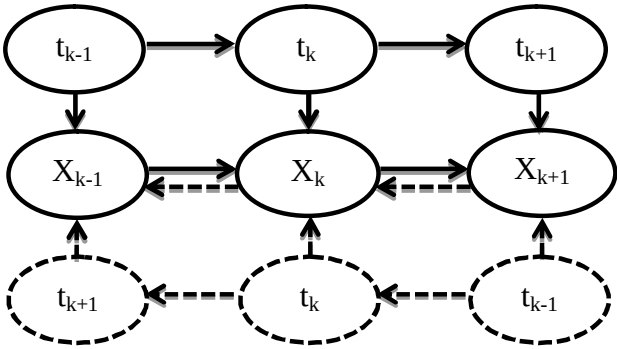

Рис. 3. Перехід станів ботнету

Як видно на рисунку, зі стану X_k можливий перехід лише в стан X_{k-1}, або в стан X_{k+1}. Аналізуючи чисельність ботнету приймемо, що стан X_k відповідає кількості ботів, яка дорівнює k. Тоді перехід системи із стану X_k в стан X_{k+1} відбувається при підключенні одного хоста до ботнету, а перехід в стан X_{k-1}, — у випадку від'єднання хоста від ботнету.

Нехай $p(t_1)$ – апріорна ймовірність наявності лише одного хоста. Тоді ймовірність перебування системи в стані X_k запишемо як $p(x_k \mid t_k)$,при $p(t_k \mid t_{k-1})$. Потужність кластера DDoS в момент часу t_k розраховують за такою формулою:

$$l_k = \prod_k r\left(x_k \mid t_k\right) r\left(t_k \mid t_{k-1}\right) \sum_{i=0}^{M} \sum_{j=1}^{N} b_{ij}. \quad (3)$$

Запропонована марківська модель – це результат двох випадкових процесів. Перший процес – прихований, оскільки описує динаміку поведінки ботів у мережі, яку неможливо зареєструвати. Проте його можна охарактеризувати за допомогою другого випадкового процесу, що являє собою конкретну послідовність значень інтенсивності атаки у фіксовані моменти часу t_k: $\lambda_k = \lambda_1, \lambda_2 \ldots \lambda_N$ (запитів/с).

Розроблення алгоритму для захисту від мережевих DDoS атак. На основі цієї моделі розроблено алгоритм відбиття атаки шляхом аналізу вхідного трафіку при появі аномальних властивостей в мережі (рис. 4) [6]. Він створює масив MasIP, у якому зберігаються IP адреси, що здійснюють запити до ресурсів мережі, та кількість запитів з цих адрес за секунду. Алгоритм дає змогу розділити права доступу до мережі для аномального трафіку та легітимних користувачів.

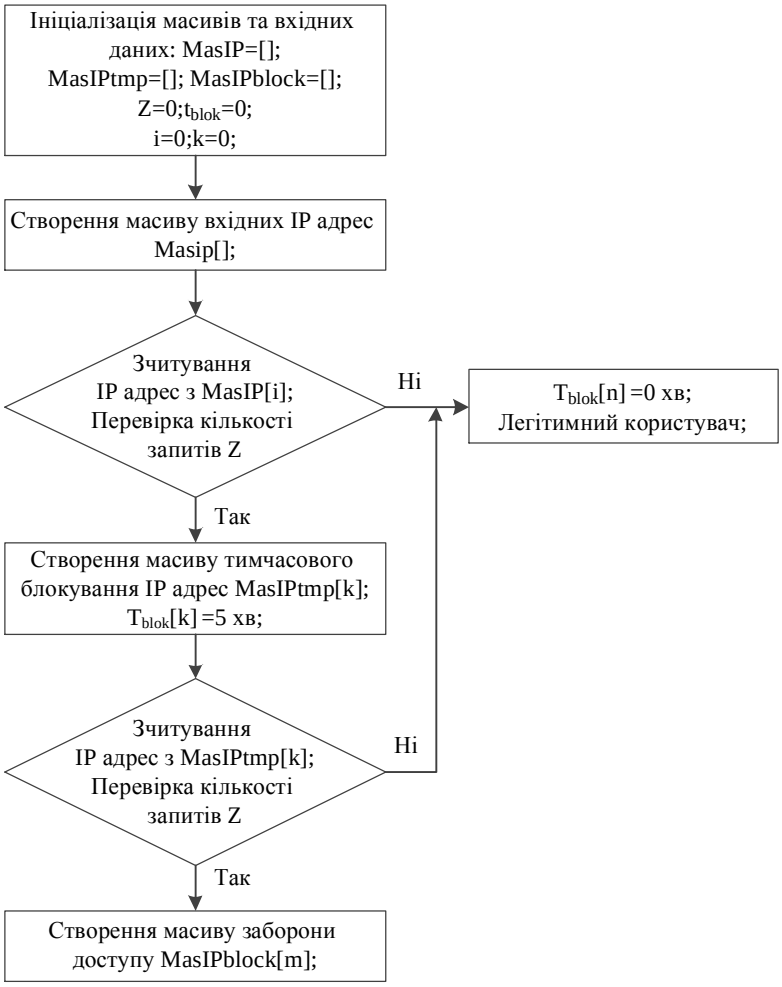

Рис. 4. Алгоритм аналізу вхідного мережевого трафіку для захисту від атак типу «розподілена відмова від обслуговування»

За умови генерації хостом великої кількість запитів Z (значення критерію вибирають залежно від потужності та типу інформаційної системи) він автоматично блокується на певний час (Tblok[k]=5 хв) і його адресу заносять в масив MasIPtmp. Хости, що генерують менше за Z запитів, вважаються легітимними користувачами і отримують доступ до інформаційних ресурсів мережі. Через час Tblok[k] елементи масиву MasIPtmp аналізуються повторно.

Якщо під час повторного аналізу хост і далі продовжує здійснювати велику кількість запитів до мережі, він вважається інфікованим хостом і заноситься в масив MasIPblock, ресурси мережі усі запити від нього відкидають. Значення гранично допустимої кількості запитів з однієї IP адреси за одиницю часу та період блокування вибрані експериментально, як оптимальні для аналізованої мережі. Залежно від потужності атаки та серверного обладнання, значення змінних алгоритму можна корегувати.

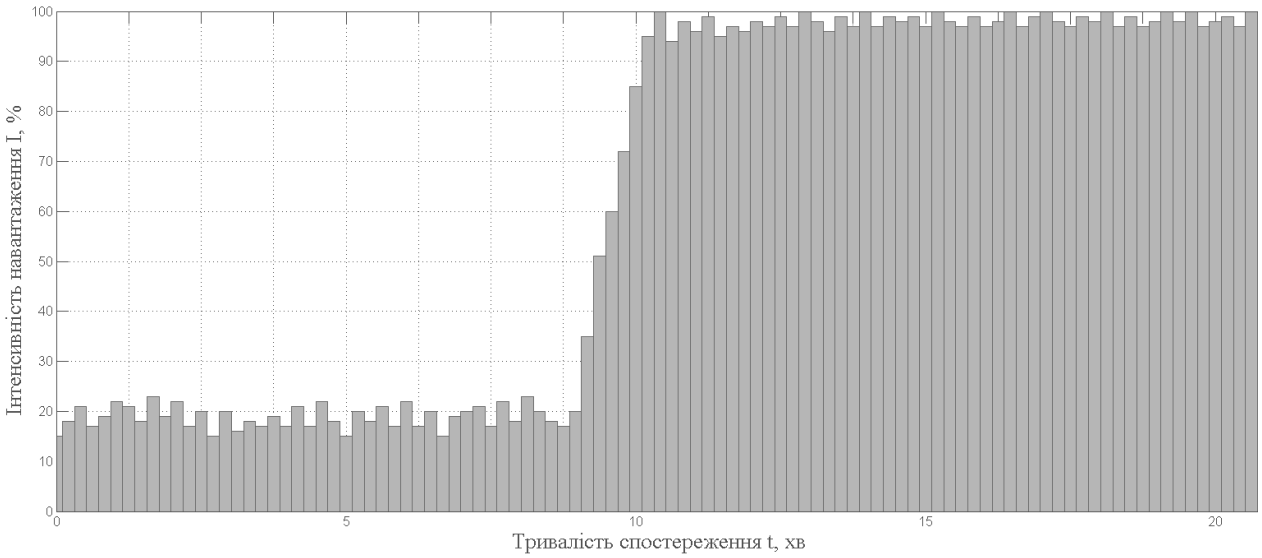

Рис. 5. Навантаження мережі під час DDoS атаки

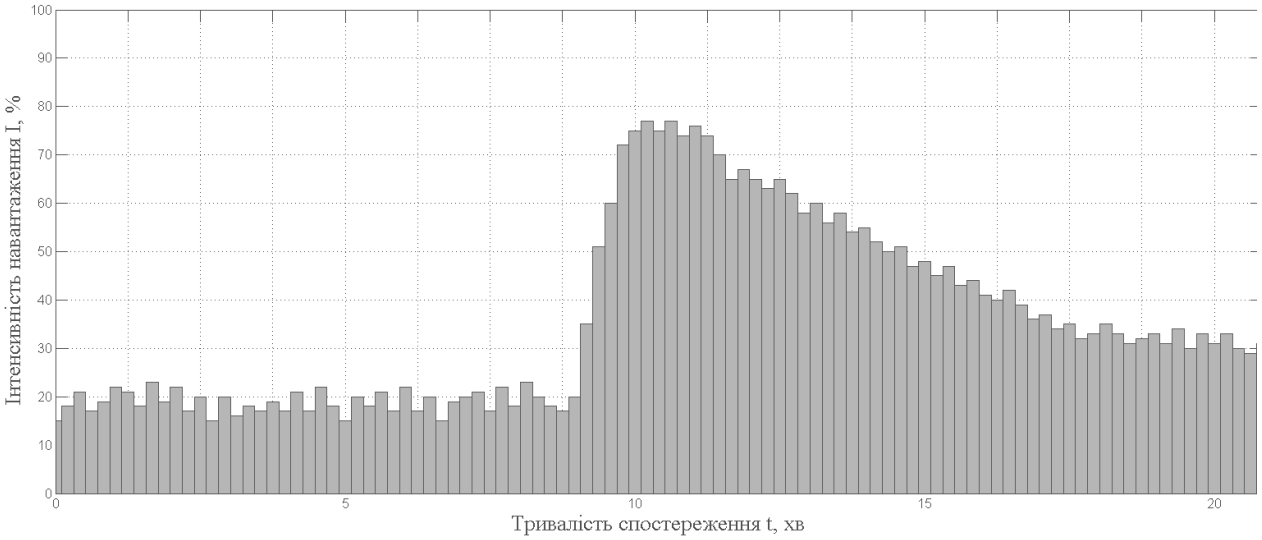

Рис. 6. Навантаження мережі під час DDoS атаки з використанням алгоритму аналізу вхідного трафіку

Із наведених вище графіків бачимо, як алгоритм аналізу вхідного трафіку впливає на інтенсивність навантаження мережі під час атаки типу «розподілена відмова в обслуговуванні». За нормальної роботи інформаційної системи навантаження на серверну частину становить близько 20 %, а після початку DDoS атаки – різко збільшується до максимальних значень в 100 %. Це

означає, що після початку мережевої атаки користувачі не зможуть отримати послуги, які повинна надавати їм інформаційна система.

При атаці такої самої потужності, але з використанням розробленого алгоритму для захисту від мережевих DDoS атак, інтенсивність навантаження зростає, оскільки вхідні запити від хостів ботнету обробляє інформаційна система, проте не досягає пікових значень (рис. 7). Допустимі значення пікового навантаження 70–80 % під час атаки дають змогу надавати послуги клієнтам з достатнім показником якості обслуговування. Після початку атаки спостерігається найбільша інтенсивність навантаження, рівень якої згодом зменшується до значень, близьких до початкових. Розбіжність викликана тим, що для блокування запитів від аномального трафіку, тобто від заражених ботів, список яких збережений у вигляді елементів масиву MasIPblock, мережеве обладнання все ж використовує частину своїх ресурсів.

Висновки. Проаналізовано мережеві атаки типу «розподілена відмова від обслуговування» та запропоновано приховану марківську модель DDoS атаки. Перевагою цієї моделі є можливість визначення характеру поведінки “ботів” у інформаційній мережі. Це дає змогу ефективно визначати вразливі місця за рахунок декомпозиції мережі на окремі частини, що є необхідним для визначення найменш захищених її ланок. На основі цієї моделі розроблено алгоритм відбиття DDoS атак, який базується на методах аналізу вхідного трафіку при появі аномальних властивостей в мережі. Алгоритм дозволяє значно знизити інтенсивність навантаження на інформаційну систему під час мережевих атак для забезпечує її неперервного функціонування.

Виконані дослідження дають змогу ефективно боротися із розподіленими мережевими атаками. Запропоновані алгоритми та методи можна використати у інформаційних системах та мережах, що мають вихід у глобальну мережу Internet, для забезпечення безперебійної роботи усіх послуг та сервісів, адже сучасні інформаційні мережі повинні бути захищеними, надійними та доступними у будь-який час.

1. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. 2. Тимошенко А.А. Защита информации в специализированных информационно-телекоммуникационных системах. — 2010. 3. Northcutt S., Cooper M., Fearnow M., Frederik K. Intrusion Signatures and Analysis. — New Riders Publishing (англ.), 2001. 4. Домарев Д.В. Математическое описание процессов атак на компьютерные сети // Проблеми інформатизації та управління. – 1(29). – 2010. – С. 50–54. 5. Jadhav V., Devale P. Anomaly detection on user browsing behaviors for prevention APP_DDOS // International Journal of Advances in Engineering & Technology. – Vol. 1. – Issue 5. – Nov 2011. – P. 492–499. 6. Beliaiev I., Dovbush Y. Analysis and research of the most common security threats for informational corporate network // Modern Problems of Radio Engineering Telecommunications and Computer Science (TCSET): Proc. Int. Conf TCSET'2012. – Lviv: Publishing house of Lviv Polytechnic, 2012. – P. 351–352.