КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.695
УДК 004.05.(045)

Поночовний Петро Михайлович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0008-6480-6990
petja9186@gmail.com

МОДЕЛЬ УПЕРЕДЖЕННЯ НИЗЬКОШВИДКІСНИХ HTTP DDOS АТАК НА КІНЦЕВОГО КОРИСТУВАЧА

Анотація. Низькошвидкісні HTTP DDoS-атаки становлять серйозну загрозу для інформаційних систем та веб-сервісів, оскільки вони використовують тонкі методи виснаження ресурсів серверів. Ці атаки, зокрема, спрямовані на виснаження обчислювальних ресурсів, здатності обробляти запити чи управління з'єднаннями на рівні додатків [1]. Модель упередження таких атак потребує особливого підходу до аналізу поведінки трафіку та характеристик запитів, що дозволяє виявляти аномалії навіть за мінімальних показників мережевої активності [2], [15]. Значним викликом для таких атак є складність їхнього розпізнавання через подібність до легітимного трафіку. Це вимагає розробки інтелектуальних систем, здатних аналізувати складні шаблони взаємодії між клієнтом і сервером. Запропонована модель ґрунтується на комплексному аналізі мережевої активності з використанням багаторівневої системи виявлення загроз. У даній моделі застосовано алгоритми машинного навчання, що забезпечують адаптивність до змінних характеристик атак та підвищують точність виявлення малопомітних аномалій у трафіку [3], [13]. Це дозволяє мінімізувати кількість хибних спрацьовувань та оперативно реагувати на зміну векторів атак. Результати симуляцій демонструють високу ефективність запропонованого підходу, оскільки система здатна реагувати на атаку ще до моменту виснаження ресурсів. Особливістю моделі є її здатність виявляти загрози з низькою інтенсивністю трафіку на ранньому етапі, які не генерують значного навантаження на мережеве обладнання [4]. Проте мають руйнівний вплив на сервіси через постійне використання обчислювальних потужностей. Унікальною перевагою підходу є можливість інтеграції з існуючими SIEM-системами, що дозволяє забезпечити більш комплексний моніторинг мережевої активності в реальному часі. Це також відкриває перспективи для впровадження розподілених систем кіберзахисту, що працюють у багатозональних мережах із високою інтенсивністю трафіку. Запропонована модель забезпечує можливість обробки даних у великих масштабах завдяки оптимізації алгоритмів класифікації та їхньої паралельної реалізації. Запропонована модель може бути інтегрована у різні системи кібербезпеки без значного впливу на продуктивність мережі [5], [6], [14]. Модель є перспективною в напрямі автоматизації виявлення нових типів атак, інтеграції з існуючими SIEM-системами та підвищення швидкості обробки великих обсягів трафіку. Даний підхід також передбачає можливість розширення для роботи з іншими типами DDoS-атак, що базуються на використанні низькоінтенсивного трафіку, завдяки універсальності механізмів аналізу пакетних груп. Це робить систему актуальною для захисту не лише веб-додатків, але й інших мережевих сервісів, зокрема IoT-платформ та хмарних інфраструктур. Запропонований підхід може стати основою для розробки інтелектуальних систем захисту від DDoS-атак. Його ефективність та адаптивність створюють потенціал для розширення функціональності систем кіберзахисту, підвищення рівня стійкості інформаційних систем до сучасних загроз і мінімізації негативного впливу на критичні сервіси.

Ключові слова: DDoS-атаки; трафік; поведінкова аналітика; машинне навчання; адаптивний захист; виявлення аномалій.

ВСТУП

Інформаційне суспільство прогресує з кожним днем і все більше покладається на інформаційні системи. Однак ця залежність може викликати величезні проблеми, якщо певна система ІТС раптово перестане надавати необхідні послуги. Якщо якийсь компонент цієї служби буде частиною іншої розподіленої системи, відмова в обслуговуванні вплине на інші системи та користувачів. Деякий час DoS не розглядався як окрема проблема безпеки і розглядався як наслідок неможливості керування конфіденційністю або проблемою цілісності. Однак швидкість і масштаби шкоди від DoS-атак показують, що DoS-атаки є важливими і повинні розглядатися як проблема безпеки. Розуміння атак DoS як окремої проблеми безпеки зросло разом із популярністю розподілених систем [7].

Постановка проблеми. В сучасних умовах стрімкого розвитку інформаційних технологій питання кібербезпеки набуває особливої актуальності. Одним із найбільш поширених і небезпечних видів кібератак є DDoS (Distributed Denial of Service) атаки, які спрямовані на виснаження ресурсів цільових систем. Особливу загрозу становлять низькошвидкісні HTTP DDoS-атаки, які є складними для виявлення через їхню приховану природу.

На відміну від традиційних атак, що створюють значне мережеве навантаження, низькошвидкісні HTTP DDoS-атаки використовують мінімальну кількість запитів, імітуючи звичайну поведінку користувачів. Їх метою є поступове виснаження обчислювальних потужностей серверів або блокування доступу до критично важливих сервісів. Такі атаки здатні залишатися непоміченими традиційними системами захисту, які орієнтовані на виявлення аномалій із високою інтенсивністю трафіку.

Існуючі методи боротьби з HTTP DDoS-атаками, як правило, не враховують низькоінтенсивний характер цих атак і потребують значних ресурсів для обробки великого обсягу мережевого трафіку. Недостатньо адаптивні або обчислювально затратні системи виявлення стають причиною зниження ефективності захисту, особливо для платформ із великою кількістю користувачів, таких як електронна комерція, банківські сервіси чи хмарні платформи [12].

Дані обставини обгрунтовують актуальність вирішення нового наукового завдання спрямованого по виявленню та оцінці низькошвидкісних DDoS-атак при цьому необхідно врахувати аналіз поведінкових характеристик трафіку. Для раннього виявлення низькошвидкісних DDoS-атак можна застосувати машинне навчання, а саме адаптивного виявлення аномалій. Також є очевидним використання механізмів пріоритизації запитів для захисту критично важливих сервісів.

Аналіз останніх досліджень і публікацій. Проблема полягає у створенні ефективної, економічно доцільної та адаптивної моделі, здатної виявляти низькошвидкісні HTTP DDoS-атаки без значного впливу на продуктивність системи.

Проаналізувавши, відомі DoS-атаки, можна виділити багато причин успіху DoS-атаки. Один з відомих випадків, коли законні користувачі спричиняли відмову в обслуговуванні систем, під час першого дня продажу квитків через Інтернет [7]. Усі користувачі намагалися якомога швидше придбати квитки та отримати найкращі місця. Однак система не змогла обслужити таку величезну кількість запитів. Це вплинуло на скорочення часу обслуговування, а іноді деякі користувачі навіть не обслуговувалися взагалі. Це лише один приклад, коли відмова в обслуговуванні може виникнути не через зловмисні дії.

Аналізуючи структуру виникнення викликів DoS, не існує єдиного стандарту для класифікації атак DoS і DDoS, тому наведемо декілька різних способів. D. Karig і R. Lee у своїй роботі [7]. Поділяє DoS-атаки з огляду на місце, де відбувається атака, на п’ять категорій:

- рівень мережевого пристрою;
- рівень операційної системи;
- рівень програми;
- потік даних;
- атака на особливості протоколу.

Така класифікація проста і однозначно визначає місце в класифікації, тобто захист об’єкта установки. Однак вона не описує всі властивості атаки, які важливі для аналізу та вибору контрзаходів, і це тому, що є перенасичення даних і атака спрямована на особливості протоколу та поділена на менші частини. Цього недостатньо, щоб описати всю ситуацію DoS-атаки.

A. Fadlallah і A. Serhrouchni [8] використовують таксономію атак DoS, враховуючи кількість комп’ютерів, які використовуються для виконання однієї атаки. На рис. 1 наведено таксономія DoS-атак.

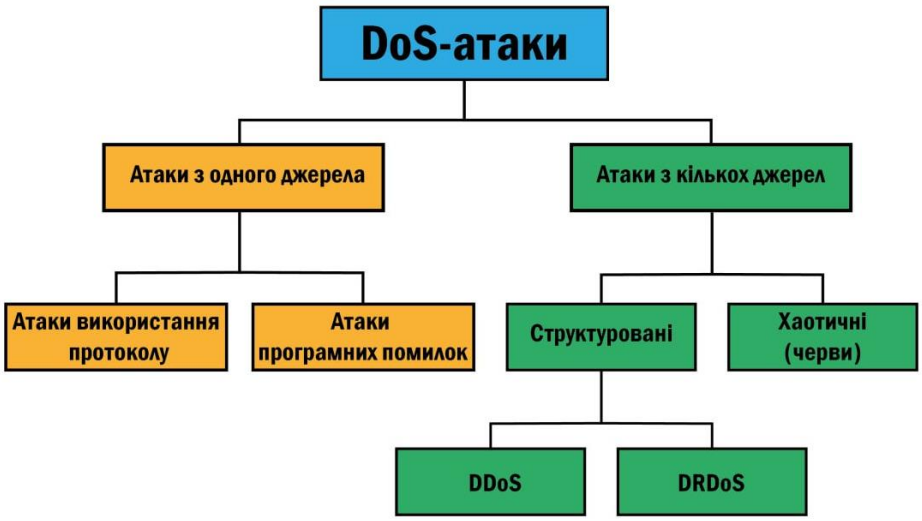

Рис. 1. Таксономія DoS-атак

Вони поділяють DoS-атаки на дві основні категорії (рис. 1):

- атаки з одного джерела;
- атаки з кількох джерел.

Атаки з одного джерела класифікуються на атаки використання протоколу та атаки програмних помилок. Водночас атаки з кількох джерел класифікуються на хаотичні і структуровані (розподілена відмова від джерела та розподілена відображена відмова в обслуговуванні).

Така систематика атак DoS є простою та чітко визначає межі атак DoS та DDoS. Однак вони не звертають уваги на додаткові функції атаки, наприклад, які саме вразливості використовуються.

Роботи [7], [11], де описано лише таксономію атак DDoS, є більш повними та класифікують більше властивостей атак.

C. Douligeris і A. Mitrokotsa [9] не розрізняють цілі DDoS-атаки, але зосереджуються на описі атаки відповідно до різних підходів (рис. 2):

- ступінь автоматизації;
- використання вразливості;
- динаміка швидкості атаки;
- вплив.

Згідно з такою класифікацією кожна атака описана з урахуванням підходів усіх чотирьох груп. Це дозволяє визначити відповідний засіб протидії в усіх цих категоріях і прийняти єдине рішення для цього типу атак.

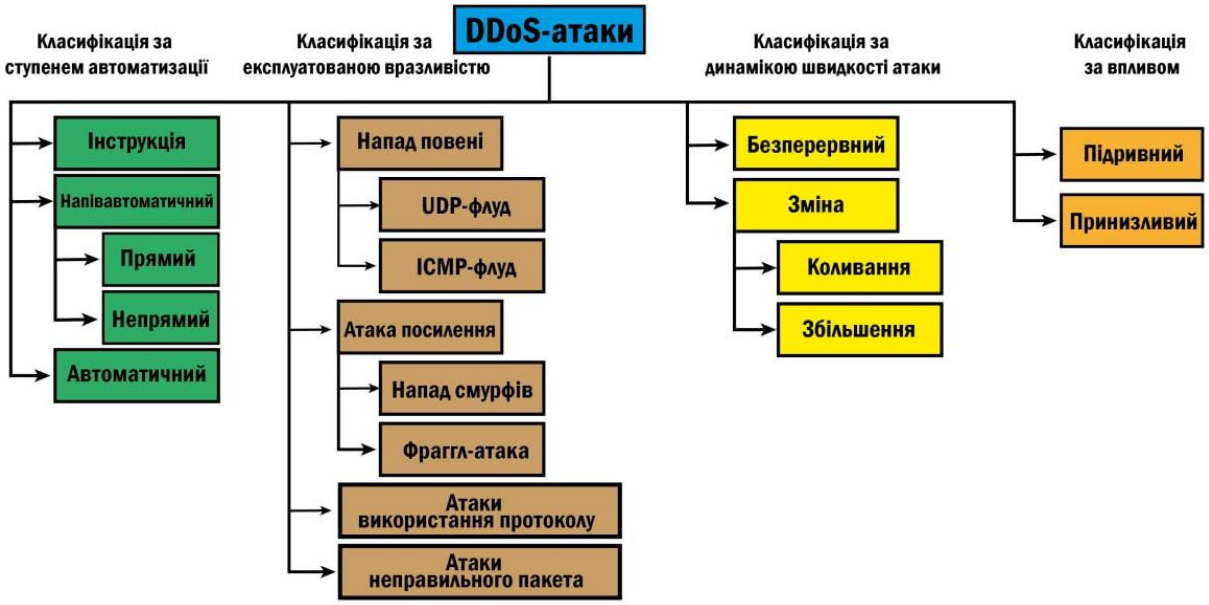

Рис. 2. Таксономія DoS-атак запропонована C. Douligeris

J. Mirkovic і P. Reiher у своїй статті [8] використовують подібну структуру таксономії атак DDoS. Але вони класифікують механізми DDoS-атак на вісім категорій (рис. 3):

- автоматизація;
- експлуатована слабкість;
- достовірність адреси джерела;
- динаміка швидкості атаки;
- можливість характеристики;
- постійність набору агентів;
- тип жертви;
- вплив на потерпілого.

Така таксономія орієнтована на опис DDoS-атаки з точки зору зловмисника. Вона досить повна і за своїми властивостями придатна для представлення DDoS-атаки; однак повний (за всіма категоріями) опис атаки є складним. Це пов’язано з тим, що нові модифікації DDoS-атаки вимагають глибокого аналізу, щоб визначити деякі властивості, необхідні для цієї класифікації.

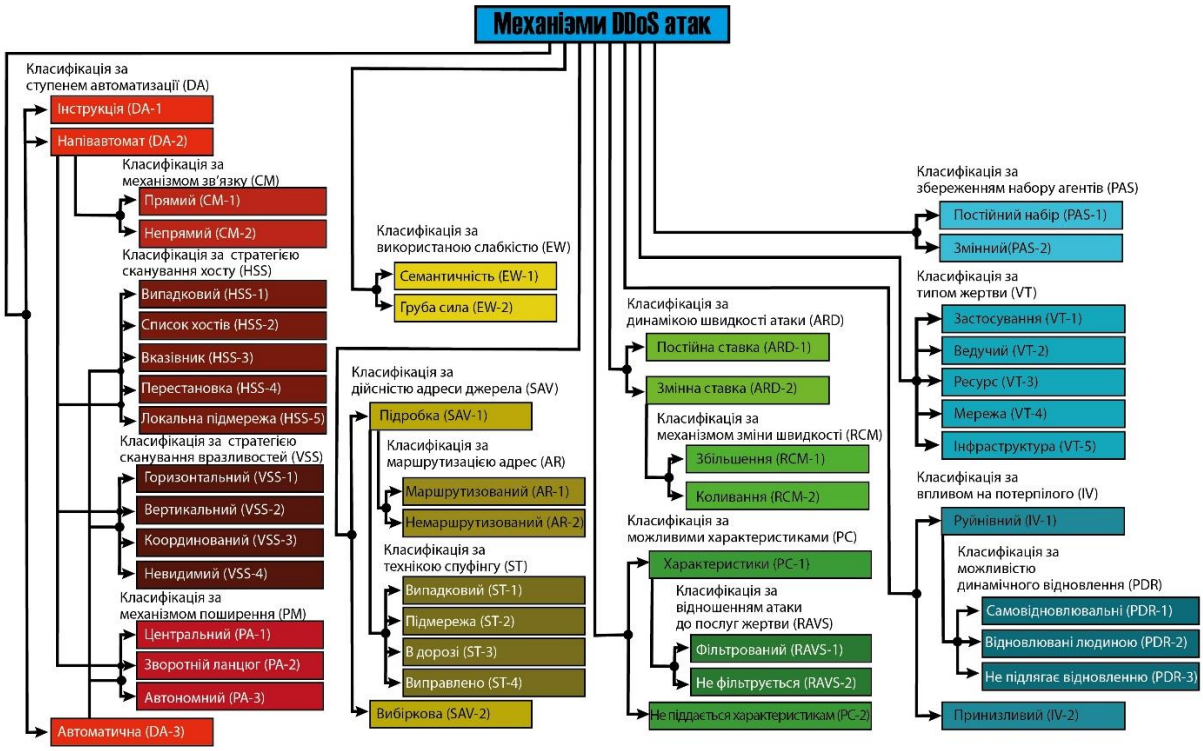

Рис. 3. Таксономія атак DoS, запропонована J. Mirkovich

Більш орієнтованою на комплексне та миттєве визначення характеристик атаки є таксономія атак S. Specht і R. Lee DDoS, описана в статті [10] (рис. 4). Вони зосереджуються на тому, як відбувається атака та які слабкі сторони жертви використовуються (пропускна здатність або виснаження ресурсу). Але вони не врахували додаткові властивості атаки, за винятком типу вразливості, яка використовується для виклику DoS-ефекту.

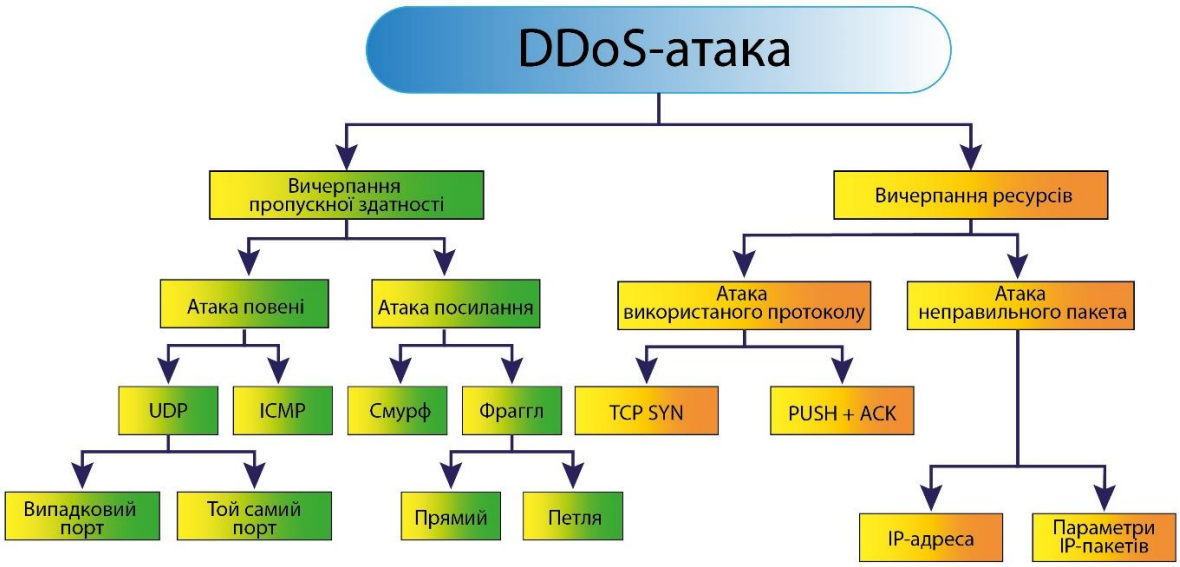

Рис. 4. Таксономія DoS-атак, запропонована S. Specht

З огляду на це, усі проаналізовані таксономії мають специфічні властивості. Однак J. Mirkovich [8] запропонував найбільш детальну таксономію.

Таксономія засобів протидії атак DoS

Через те, що тип DoS є більш нерівним, для обробки певного типу DoS можна використовувати багато різних типів контрзаходів. Класифікація існуючих засобів протидії DoS-атакам важлива через можливість отримати чітке уявлення про механізми захисту, можливість вибрати один єдиний механізм захисту з усіх можливих методів. D. Kagir [7] виокремлює п’ять груп протидії DoS-атакам, які орієнтовані на тип жертви (рис. 5):

- рівень мережевого пристрою;
- рівень ОС;
- рівень програми;
- стандартний рівень протоколу;
- реплікація та балансування навантаження (пропускна здатність).

Більш детальний опис можливий для підкатегорій цих п’яти груп; однак він може бути мінімальним, оскільки в цих групах є дві основні підкатегорії, тобто ітераційне обслуговування та використання додаткових систем.

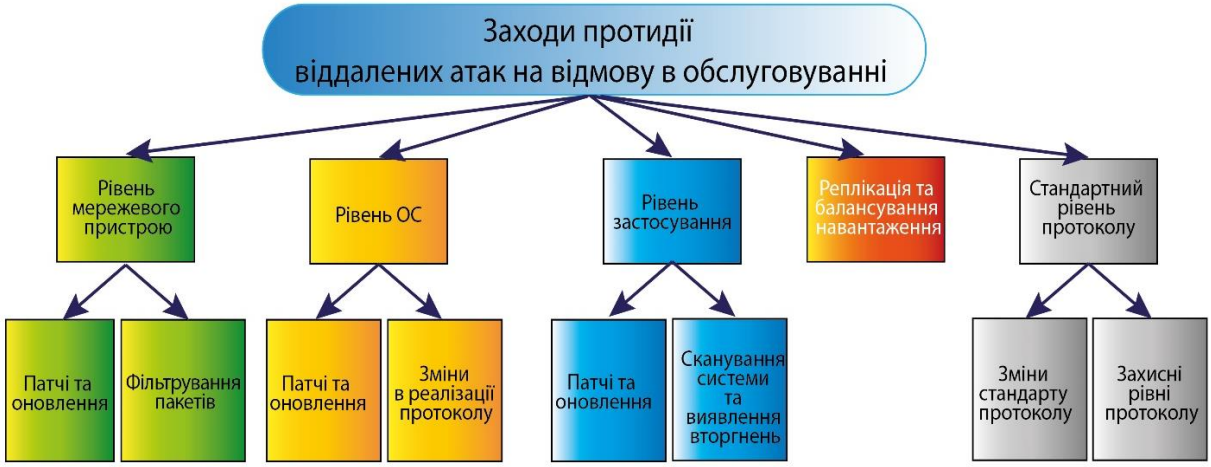

Рис. 5. Таксономія протидії атак DoS, запропонована Д. Кагіром

A. Asosheh [11] запропонував таксономію DDoS-атаки, яка також орієнтована на тип жертви, але є більш детальною. Перш за все, існує дві основні категорії, що представляють можливі фази контрзаходів (рис. 6):

- профілактика;
- виявлення.

Ці категорії охоплюють тип жертви (цільова мережа та проміжна мережа для обох фаз і додаткова вихідна мережа для фази виявлення). Крім того, кожна підкатегорія має свою і досить детальну класифікацію.

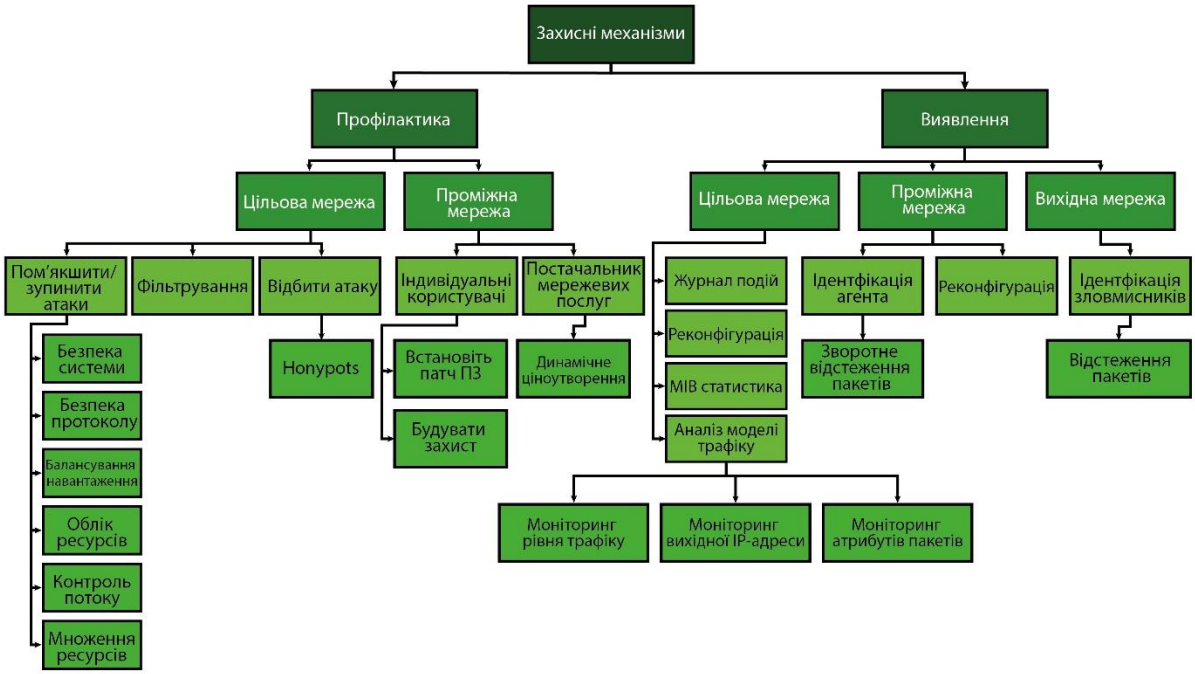

Рис. 6. Таксономія протидії атак DoS, запропонована А. Асоше

Головним недоліком цієї класифікації є недостатнє представлення можливих фаз контрзаходів. M. Specht [10] бере це до уваги та класифікує шість фаз (рис. 7):

- виявляти та знешкоджувати обробників;
- виявляти та запобігати вторинним жертвам;
- виявляти та запобігати потенційним атакам;
- послаблення та припинення атак;
- відбивати атаки;
- криміналістика після нападу.

Більшість із цих етапів мають підкатегорії, призначені для більш детального опису протидії DDoS. Але ця та всі інші згадані класифікації протидії DoS зосереджені лише на одній характеристиці, тобто протидія DoS може належати лише до однієї категорії в цій класифікації.

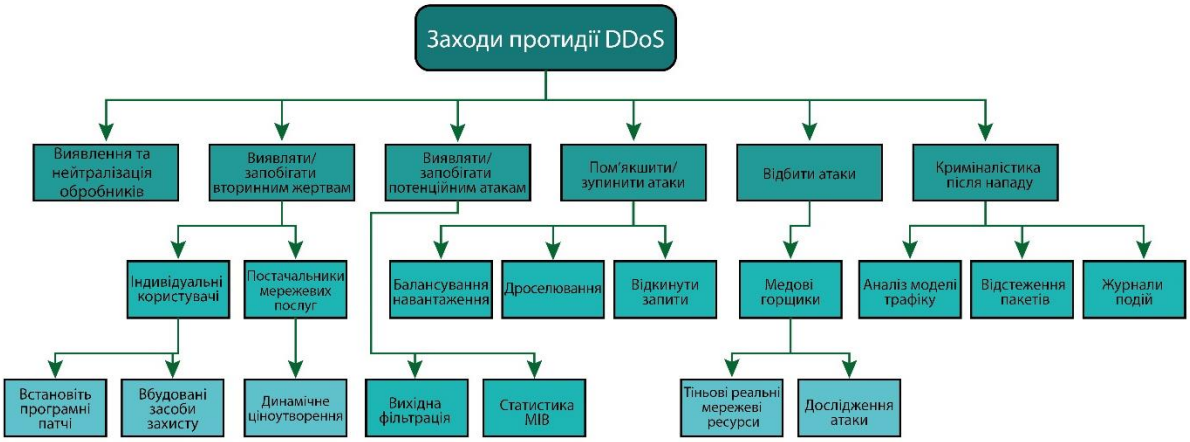

Рис. 7. Таксономія протидії атак DoS, запропонована М. Шпехтом

Критерії класифікації протидії DDoS (рис. 8):

- класифікація щодо діяльності;
- класифікація щодо розташування.

Класифікація щодо розташування раніше не згадувалась і представляє можливе розташування захисту від DoS, тобто в жертвах, вихідній або проміжній мережі.

A. Fadlallah і J. Mirkovich [7] також виділяють третій критерій для класифікації протидії DoS, і це класифікація щодо ступеня співпраці:

- автономний;
- кооператив;
- взаємозалежні.

Основна відмінність між цими двома таксономіями полягає в повноті. A. Fadlallah виокремлює кілька підкатегорій для всіх критеріїв. Між тим у Дж. Мірковича таксономія більш детальна. Він навіть поділяє фазу запобігання на атаку та запобігання DoS.

Таксономії протидії DoS, DDoS більш чутливі до старіння, ніж таксономії DoS, DDoS. Вони мають більш специфічні властивості протидії, тому, якщо з'являться нові ідеї щодо протидії DoS, вони можуть не бути представлений у поточній таксономії.

ОСНОВНА ЧАСТИНА

Можна розрізнити всі можливі комбінації DDoS-атак і властивостей їх протидії, якщо існує детальна систематика. Однак для отримання кількісного виразу аналізованих властивостей DDoS-атаку або її протидію необхідно оцінити на практиці або змоделювати відповідними інструментами.

Найпоширенішою ситуацією атаки DDoS є ситуація, коли трафік атаки вичерпує як пропускну здатність, так і ресурси пам'яті. У цій статті під час аналізу DDoS-атаки береться до уваги DDoS-модель пропускної здатності та виснаження пам'яті, а також властивості фільтрації системи. Концепція цієї комбінованої моделі пояснюється на рис. 8.

Вхідний трафік може бути заблокований через недостатню пропускну здатність. Іншу частину трафіку можна блокувати системою фільтрації. Нарешті, те, що залишилося після фільтрації, може бути заблоковано недостатнім місцем у буфері, призначеному для зберігання відкритих з'єднань.

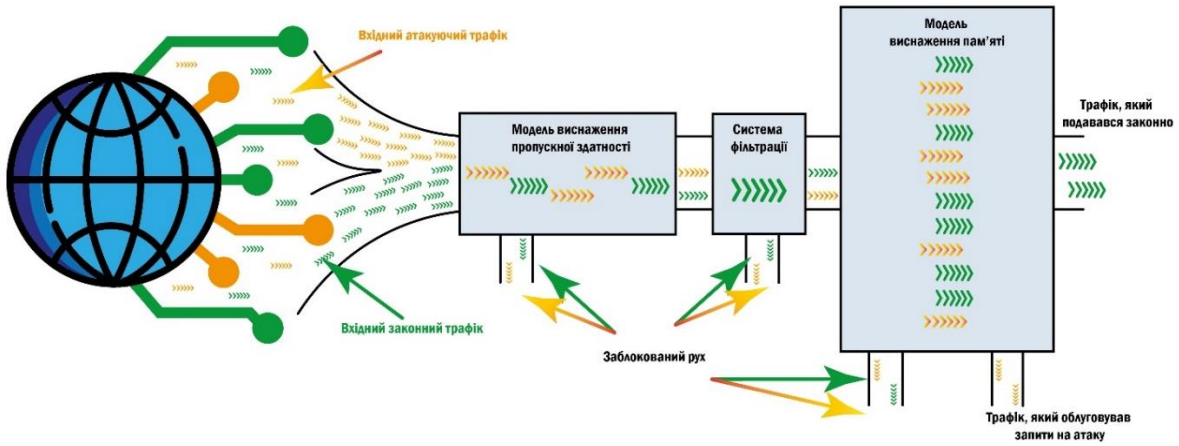

Рис. 8. Концептуальна модель комбінованої DDoS-атаки з пропускною здатністю та вичерпанням пам'яті

ISSN 2663 - 4023

Щоб представити повну ймовірність атаки, ми модифікуємо формулу

$$P = 1 - \overline{P}_B * \overline{P}_M * \overline{P}_C \quad (1)$$

де P — ймовірність DDoS-атаки з виснаженням ресурсу, P_B — зниження пропускної здатності P_C — виснаження процесів, P_M — вичерпання пам'яті щоб додати ймовірність фільтрації законного трафіку P_{Fn}:

$$P = 1 - (1 - P_B) * (1 - P_{Fn}) * (1 - P_M) \quad (2)$$

де P_{Fn} — ймовірність фільтрації законного трафіку.

Використовуючи запропоновану композитну модель DDoS-атаки, досліджувалися різні ситуації. Мета цих експериментів полягала в тому, щоб розрізнити вплив різних властивостей атаки на успіх атаки DDoS.

ЕКСПЕРЕМЕНТАЛЬНА ЧАСТИНА

Для аналізу цих експериментів були обрані стандартні параметри ситуації:

- Звичайний трафік 20 Мбіт/с (100 запитів на секунду по 200 біт у кожному).
- Трафік атаки 10 Мбіт/с (50000 запитів на секунду по 200 біт у кожному).
- 1 канал із пропускною здатністю 100 Мбіт/с.
- Жертва використовує фільтри, які фільтрують 20% атак і 2% законних запитів користувачів.
- Для виконання законного запиту потрібно 200 мс.
- Виконання запиту атаки займає 2000 мс.
- Буфер може зберігати інформацію про 50 з'єднань.

Ці параметри атаки та жертви призводять до 8,7% виснаження пропускної здатності, 2% законних запитів відфільтровано та ймовірності виснаження пам'яті 39,3%. Композитна ймовірність успіху DDoS-атаки склала 45,7%.

Змінюючи властивості фільтрації, стає зрозуміло, що ймовірність блокування легітимних запитів є дуже важливим та лінійно збільшує ймовірність успіху композитної DDoS-атаки. Водночас фільтрація трафіку атаки викликає нелінійну зміну пам'яті та ймовірності проведення складної DDoS-атаки (рис. 9).

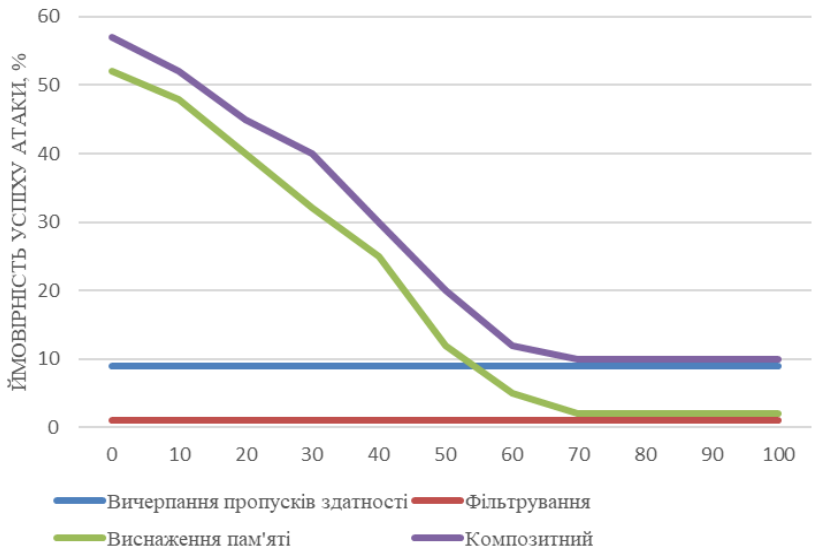

Рис. 9. Залежність успіху атаки від відсотка фільтрації запитів атаки

ISSN 2663 - 4023

Подібні тенденції також стосуються впливу часу успішного проведення атаки. Як видно з рис. 9 збільшенням середнього часу обслуговування (як легітимних запитів, так і запитів атаки) збільшується ймовірність виснаження пам’яті, але її вплив на успіх композитної атаки не є пропорційним, що відмічено на рис. 10.

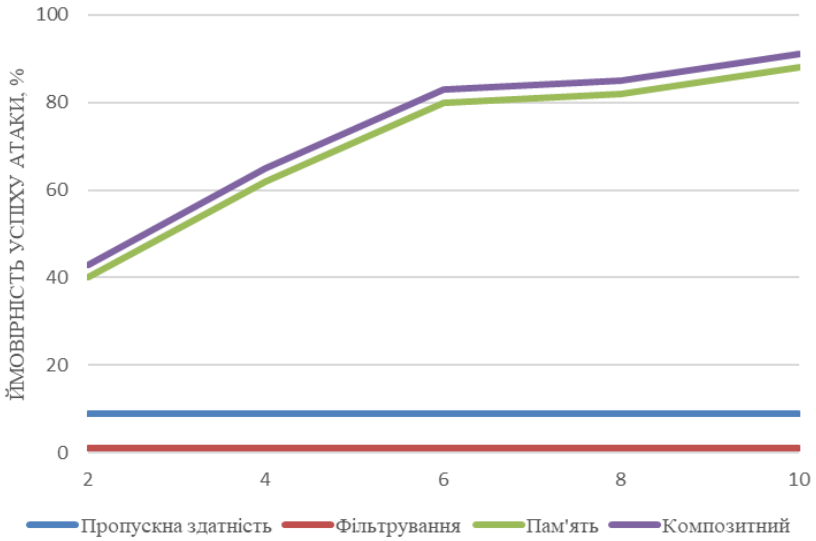

Рис. 10. Імовірність успіху атаки залежить від часу обслуговування запиту атаки

Попередні експерименти вплинули лише на виснаження пам’яті та ймовірність складної атаки. Тим часом зміна властивостей вхідного трафіку також впливає на ймовірність вичерпання пропускної здатності.

Збільшення законного трафіку та трафіку атаки призводить до збільшення успіху атаки, але в нашому експериментальному середовищі збільшення виснаження пам’яті вище, ніж ймовірність вичерпання пропускної здатності. Навіть якщо зменшити час обслуговування в 10 разів, вплив виснаження пропускної здатності на ймовірність успіху комбінованої атаки буде більшим лише до тих пір, поки швидкість атаки буде досить низькою (рис. 11).

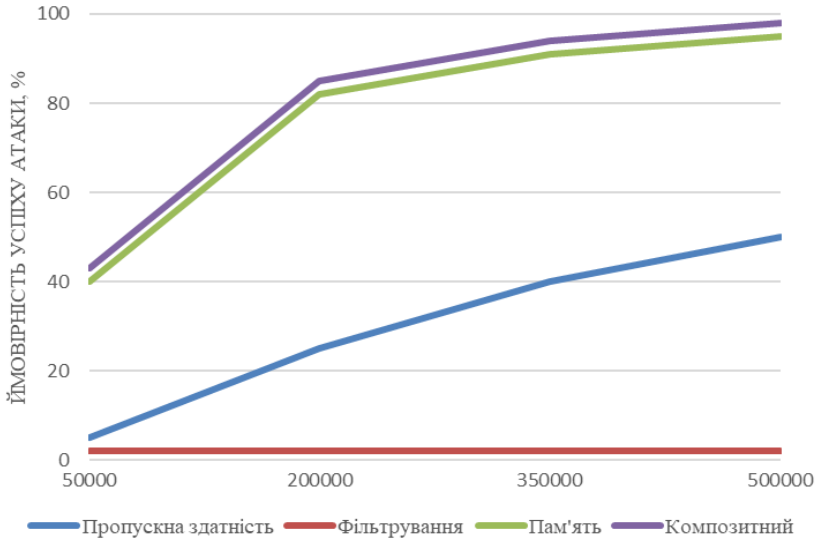

Рис. 11. Залежність ймовірності успіху атаки від частоти надходження запитів із середнім часом обслуговування

При використанні більшого трафіку атаки ймовірність виснаження пам’яті має більший вплив і більш чутлива до розміру атаки рис. 12.

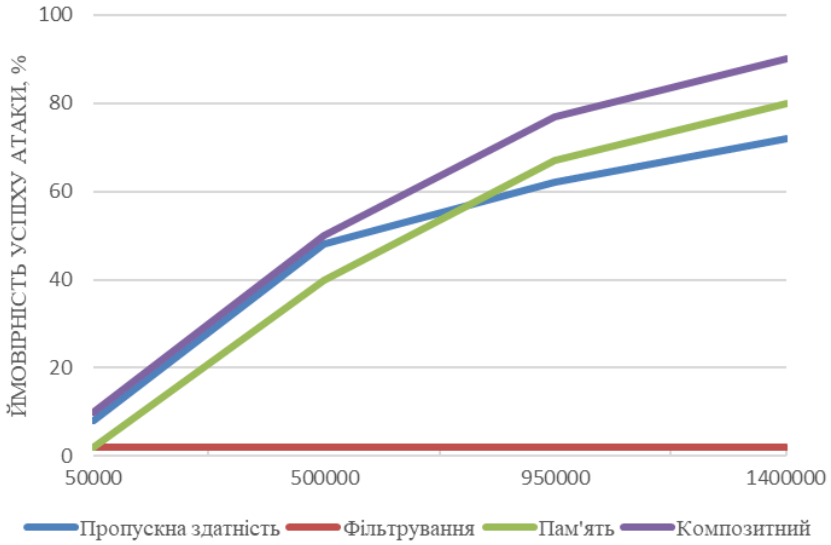

Рис. 12. Залежність ймовірності успіху атаки від швидкості надходження запиту з дуже коротким часом обслуговування

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонована система раннього упередження є ефективним алгоритмом протидії просочування DDoS-атаки на кінцевого користувача. Така система гарно інтегрується з інтелектуальними системами від DDoS-атак.

Проведені експериментальні дослідження показують, як різні часткові та комплексні DDoS-атаки можуть залежати від різних параметрів атаки та жертви.

За допомогою запропонованої моделі було виявлено деякі факти щодо ймовірності успіху DDoS-атаки:

- Погана конфігурація системи фільтрації може завдати більше шкоди, ніж сама атака DDoS.
- Атаки виснаження пам’яті більш чутливі до вхідного трафіку змін і може бути основною причиною високого успіху композитної атаки ймовірність.
- Зміни в DDoS-атаці та значеннях властивостей жертви мають нелінійний вплив на ймовірність успіху атаки, не кажучи вже про повну ймовірність успіху DDoS-атаки.

Запропонований підхід може стати основою для подальшої розробки інтелектуальних систем захисту від DDoS-атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34(2),* 39–53.
2. Beitollahi, H., & Deconinck, G. (2012). Analyzing low-rate DoS attacks against application servers. *Computers & Security, 31(8),* 847–860.
3. Yu, S., Zhou, W., & Doss, R. (2013). Information theory based detection against network behavior mimicking DDoS attacks. *IEEE Communications Letters, 17(5),* 1052–1055.

4. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 44(5),* 643–666.
5. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15(4),* 2046–2069.
6. Kolodchak, O. M. (2012). Modern methods of anomaly detection in intrusion detection systems. *Bulletin of Lviv Polytechnic National University. Computer systems and networks, 745,* 98–104.
7. Karig, D., Lee, R. (2001). Remote Denial of Service At-tacks and Countermeasures. *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002DoS attack taxonomy proposed by A. Fadlallah (Fadlallah and Serhrouchmi 2005).*
8. Mirkovich, J., Dietrich, S., Dittrich, D., Reiher, P. (2005). *Internet Denial of Service: Attack and Defense Mechanisms.* New Jersey: Prentice Hall.
9. Douligeris, C., Mitrokots, A. (2004). DDoS atacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 4(2004),* 643–666.
10. Specht, S. M., Lee, R. B. (2004). Distributed Denial of Service: Taxonomy of Attacks, Tools and Countermeasures. *17th International Conference on Parallel and Distributed Computing Systems,* 543–550.
11. Asosheh, A., Ranezani, N. (2008). A comprehensive faxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Communications 7(4),* 281–290.
12. Yevseiev, S., Melenti, Y. Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Prokopenko, O., Sievierinov, O., Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies, 3(9(111)),* 63–83. http://dx.doi.org/10.15587/1729-4061.2021.233533
13. Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN flooding attacks. *IEEE INFOCOM, 3,* 1530–1539.
14. Chen, Y., Hwang, K., & Ku, W. (2007). Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transactions on Parallel and Distributed Systems, 18(12),* 1649–1662.
15. Gu, Y., & Lu, J. (2011). An efficient algorithm for DDoS attack detection based on entropy analysis. *Journal of Networks, 6(6),* 1033–1040.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Petro Ponochovny
Postgraduate student
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0008-6480-6990
petja9186@gmail.com

LOW-SPEED HTTP DDOS ATTACK PREVENTION MODEL FOR END USERS

Abstract. Slow HTTP DDoS attacks pose a serious threat to information systems and web services because they use sophisticated techniques to exhaust server resources. These attacks specifically target compute resource exhaustion, request throughput, or connection management at the application layer [1]. Biased modeling of such attacks requires a special approach to analyze traffic behavior and request characteristics, allowing anomalies to be detected even with minimal network activity [2], [15]. The main problem with such attacks is that they are difficult to recognize because of their similarity to legitimate traffic. Therefore, it is necessary to develop intelligent systems that can analyze the complex interaction patterns between clients and servers. The proposed model is based on a complex analysis of network activity using a layered threat detection system. The model utilizes machine learning algorithms that adapt to changing attack characteristics and improve the accuracy of detecting subtle anomalies in traffic [3], [13]. This minimizes the number of false positives and allows the system to respond quickly to changes in the attack vector. Simulation results demonstrate the effectiveness of the proposed approach, as it can respond to attacks even before the system has exhausted its resources. A feature of this model is its ability to detect early threats with low traffic intensity that do not impose a significant load on network equipment [4]. However, such threats always consume computing power and thus have a devastating impact on services. A unique advantage of this approach is that it can be integrated with existing SIEM systems, allowing for more comprehensive real-time monitoring of network activity. It also opens prospects for the realization of distributed cyber defense systems operating in multi-area networks with high traffic intensity. The proposed model provides high data processing performance through optimization of the classification algorithm and its parallel implementation. The proposed model can be integrated into various cybersecurity systems without significant impact on network performance [5], [6], [14]. The model is promising in the direction of automatic detection of new types of attacks, integration with existing SIEM systems, and faster processing of large amounts of traffic. Furthermore, the versatility of the packet group analysis mechanism allows its extension to other types of DDoS attacks based on the use of low-intensity traffic. This makes it suitable for protecting not only web applications but also other network services such as IoT platforms and cloud infrastructures. The proposed approach provides a basis for the development of intelligent defense systems against DDoS attacks. Its efficiency and adaptability will expand the capabilities of cyber defense systems, increase the resilience of information systems against modern threats, and minimize the negative impact on critical services.

Keywords: DDoS attacks; traffic; behavioral analysis; machine learning; adaptive defense; anomaly detection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34(2),* 39–53.
2. Beitollahi, H., & Deconinck, G. (2012). Analyzing low-rate DoS attacks against application servers. *Computers & Security, 31(8),* 847–860.
3. Yu, S., Zhou, W., & Doss, R. (2013). Information theory based detection against network behavior mimicking DDoS attacks. *IEEE Communications Letters, 17(5),* 1052–1055.
4. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 44(5),* 643–666.
5. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15(4),* 2046–2069.

6. Kolodchak, O. M. (2012). Modern methods of anomaly detection in intrusion detection systems. *Bulletin of Lviv Polytechnic National University. Computer systems and networks, 745,* 98–104.
7. Karig, D., Lee, R. (2001). Remote Denial of Service At-tacks and Countermeasures. *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002DoS attack taxonomy proposed by A. Fadlallah (Fadlallah and Serhrouchmi 2005)*.
8. Mirkovich, J., Dietrich, S., Dittrich, D., Reiher, P. (2005). *Internet Denial of Service: Attack and Defense Mechanisms.* New Jersey: Prentice Hall.
9. Douligeris, C., Mitrokots, A. (2004). DDoS atacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 4(2004),* 643–666.
10. Specht, S. M., Lee, R. B. (2004). Distributed Denial of Service: Taxonomy of Attacks, Tools and Countermeasures. *17th International Conference on Parallel and Distributed Computing Systems,* 543–550.
11. Asosheh, A., Ranezani, N. (2008). A comprehensive faxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Communications 7(4),* 281–290.
12. Yevseiev, S., Melenti, Y. Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Prokopenko, O., Sievierinov, O., Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies, 3(9(111)),* 63–83. http://dx.doi.org/10.15587/1729-4061.2021.233533
13. Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN flooding attacks. *IEEE INFOCOM, 3,* 1530–1539.
14. Chen, Y., Hwang, K., & Ku, W. (2007). Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transactions on Parallel and Distributed Systems, 18(12),* 1649–1662.
15. Gu, Y., & Lu, J. (2011). An efficient algorithm for DDoS attack detection based on entropy analysis. *Journal of Networks, 6(6),* 1033–1040.