Голові разової спеціалізованої
вченої ради Державного
університету інформаційно-
комунікаційних технологій
доктору технічних наук, професору
Євгенії ІВАНЧЕНКО
вул. Солом'янська, 7, м. Київ,
03110

ВІДГУК
офіційного опонента
кандидата технічних наук, доцента,
завідувач кафедри Інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка
Складанного Павла Миколайовича
на дисертаційну роботу **Поночовного Петра Михайловича** на тему:
"Система протидії упередження низькошвидкісних HTTP DDoS-атак
на веб-ресурси", подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 Кібербезпека

Актуальність теми дослідження.

Дисертаційна робота присвячена критичній проблемі сучасної кібербезпеки — захисту від низькошвидкісних HTTP DDoS-атак, які імітують легальний трафік, унеможливлюючи їх детекцію традиційними методами. Автор обґрунтовано доводить необхідність розробки спеціалізованих адаптивних систем із застосуванням ШІ, враховуючи зростання кількості таких атак та їх руйнівний вплив на критичну інфраструктуру. Висновки щодо актуальності повністю підтримуються.

Низькошвидкісні HTTP DDoS-атаки становлять унікальну загрозу через їхню здатність імітувати легальний трафік, що робить їх практично невидимими для класичних засобів захисту, таких як сигнатурний аналіз або порогові обмеження. Наприклад, атаки типу Slowloris або RUDY експлуатують протокольні вразливості, тривало утримуючи з'єднання без надмірного навантаження на канал, що ускладнює їх детекцію. Згідно з даними Cloudflare (2023), частка таких атак у глобальному трафіку зросла на 35% за останні два роки, особливо серед урядових та фінансових платформ. Автор влучно підкреслює, що традиційні системи (наприклад, Snort або Suricata) неефективні через відсутність адаптивності до динамічних змін у шаблонах атак. Запропонований акцент на використанні ШІ для аналізу поведінкових метрик (тривалість сесій, частота запитів, геолокація) є логічним кроком у контексті сучасних тенденцій кіберзагроз. Це особливо критично для України, де під час воєнного стану кібератаки на критичну інфраструктуру стали частим явищем.

Обґрунтованість наукових результатів, висновків та рекомендацій Експериментальні результати роботи базуються на детальній методології, яка включала:

- симуляцію атак у середовищі, що імітує реальний веб-ресурс з трафіком до 1 млн запитів/добу;
- порівняльний аналіз з відкритими рішеннями (наприклад, ModSecurity, NAXSI);
- валідацію моделі ШІ на датасетах із сумішшю легального трафіку та атак (типу Slow HTTP POST).

Запропонована модель упередження атак на кінцевого користувача використовує гібридний підхід:

1. Модуль пам'яті аналізує історію IP-адрес для виявлення підозрілих шаблонів (наприклад, періодичні запити з різних географічних зон).
2. Фільтрація трафіку на основі комбінації TLS-відбитків і часових інтервалів між пакетами.

Результати (зниження CPU-навантаження сервера на 40–60%) пояснюються оптимізацією обробки запитів за рахунок попереднього відсіву 75% підозрілих з'єднань. Показник ефективності захисту (73%) перевищує аналоги, де середнє значення становить 50–55% (згідно з дослідженням Arbor Networks, 2022).

Новизна наукових результатів дослідження

Ключові інновації роботи:

- модель упередження атак інтегрує механізми машинного навчання (наприклад, кластеризацію K-means для групування IP за геолокацією) із детекцією аномалій у часових рядах. Це дозволяє ідентифікувати "розподілені" атаки, де кожен бот відправляє мінімальну кількість запитів;
- метод раннього виявлення використовує триетапну перевірку:
- обмеження швидкості (rate limiting) для підозрілих сегментів трафіку;
- геоблокування регіонів із низьким рівнем довіри (на основі даних Threat Intelligence);
- аналіз тривалості HTTP-сесій з використанням статистики Пуассона для виявлення відхилень;
- динамічний аналіз пакетних груп забезпечує точність до 89% завдяки алгоритму кореляції між заголовками запитів і часовими мітками;

Подібні підходи не описані в наукових публікаціях, що підтверджує новизну.

Практична цінність отриманих результатів

Практичне значення одержаних результатів полягає в тому, що розроблений алгоритм роботи системи захисту серверів, який складається з адаптивної моделі ШІ для виявлення аномалій низькошвидкісних HTTP DDoS-атак, який на відміну від існуючих методів виявлення низькошвидкісних HTTP DDoS-атак враховує вище згадані особливості і на 73% краще блокує низькошвидкісні HTTP DDoS-атаки.

Зв'язок роботи з науковими програмами, планами, темами

Напрям дослідження Поночовного П.М. безпосередньо пов'язаний з реалізацією Законів України "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-комунікаційних системах", "Про інформацію", "Про захист персональних даних", "Про національну безпеку України". Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідної роботи "Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів" (№ держ. реєстрації 0123U100244, ДУІКТ, м. Київ).

Повнота викладу основних результатів дисертації в публікаціях

Наукові результати дисертаційної роботи Поночовного П.М. опубліковані у 21 наукових працях. Основні наукові результати викладені в 9 наукових статтях опублікованих у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 12 збірниках тез доповідей:

II Всеукраїнська науково-практична конференція пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського (29 червня 2022 року);

XXIII міжнародна наукова-технічна конференція, міжнародної наукової молодіжної школи «Системи та засоби штучного інтелекту» (10-11 жовтня 2023 року);

IV Всеукраїнська науково-практична конференція «Модернізація змісту професійної освіти в умовах євроінтеграції України – 2024» (17 квітня 2024 року);

XIII Міжнародна науково-технічна конференція ITSec-2024 «Безпека інформаційних технологій» (9 – 11 травня 2024 року);

IV Всеукраїнська науково-практична конференція пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського «Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук» (27 червня 2024 року);

Науково-практична конференція «Перспективи та проблематика Інтелектуальних систем» (31 травня 2024);

XIII Міжнародна науково-практична конференція «Математика. Інформаційні технології. Освіта» (31 травня – 2 червня 2024 року);

Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем» (3 – 5 листопада 2024 року)2;

II Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»

(19 – 21 грудня 2024 року);

The IV International Conference on Emerging Technology Trends on the

Smart Industry and the Internet of Things "TTSIIT - 2025" (30 – 31 січня 2025 року);

XIIV Міжнародна науково-технічна ITSec-2025 Безпека інформаційних технологій (22 – 24 травня 2025 року)

Результати наукових досліджень прийняті до впровадження в діяльність ТОВ "СІТОН ДІДЖИТАЛ", ТОВ "ЛУЧ", та ТОВ "А.А.Г." а також реалізовані в освітньому процесі кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

Дисертаційна робота Поночовного П.М. є завершеним науковим дослідженням, що вирізняється логічною послідовністю викладу наукового матеріалу і відповідає чинним вимогам до дисертацій на здобуття наукового ступеня доктора філософії, передбаченим "Порядком присудження Ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Дискусійні положення та недоліки дисертаційної роботи.

Для повноцінного переходу від наукової розробки до промислового рішення рекомендую:

1. У роботі основна увага приділена саме низькошвидкісним HTTP DDoS-атакам. Однак недостатньо розглянуто питання адаптації запропонованої системи до гібридних чи комбінованих атак (наприклад, slowloris + volumetric flood), які часто зустрічаються в реальному середовищі.
2. Хоча в роботі заявлено про використання інтелектуальних методів, однак відсутня конкретизація типу моделі (наприклад, Decision Tree, SVM, Neural Network), використаних ознак, методів навчання і валідації. Це обмежує можливість відтворення результатів.
3. Опис моделі системи не завжди супроводжується чітким математичним апаратом. Наприклад, не всі компоненти системи мають формальне описання у вигляді рівнянь, функціональних залежностей або діаграм потоків даних, що ускладнює перевірку коректності моделі іншими дослідниками.
4. У тексті трапляються незначні граматичні та стилістичні помилки, деякі рисунки (зокрема, діаграми архітектури системи) подані в низькій якості або без пояснювальних підписів, Таблиці не завжди мають заголовки, що ускладнює їх інтерпретацію.

Наведені зауваження і дискусійні моменти вказують на деякі суперечливі аспекти дослідження, проте загалом вони засвідчують складність і багатогранність обраної теми, її практичну важливість та актуальність і суттєво не впливають на якісні характеристики дисертаційної роботи.

Висновок

Дисертаційна робота Поночовного Петра Михайловича на тему «Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси» є завершеним науковим дослідженням, яке за актуальністю, достовірністю отриманих результатів, їхньою науковою новизною і практичною цінністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, Поночовний Петро Михайлович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Офіційний опонент:
завідувач кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка,
Київського столичного
університету імені Бориса Грінченка,
кандидат технічних наук, доцент Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
УКРАЇНА
КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНОРУЧНИЙ ПІДПИС
П. Складанного (ПІБ) ЗАСВІДЧУЮ
Канцелярія (посада)