Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U003049

Особливі позначки: відкрита

Дата реєстрації: 21-07-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Поночовний Петро Михайлович

2. Petro Ponochovnyi

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0008-6480-6990

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту:

Спеціальність за освітою: Технологічна освіта

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 9899

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.23.37, 49.33.35, 28.31.04

Тема дисертації:

1. СИСТЕМА ПРОТИДІЇ УПЕРЕДЖЕННЯ НИЗЬКОШВИДКІСНИХ HTTP DDOS-АТАК НА ВЕБ-РЕСУРСИ
2. COUNTERMEASURES SYSTEM FOR PREVENTING LOW-SPEED HTTP DDOS ATTACKS ON WEB RESOURCES

Реферат:

1. Поночовний П.М. Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека» (12 – Інформаційні технології). - Державний університет інформаційно-комунікаційних технологій, м. Київ, 2025. Дисертаційна робота присвячена підвищенню надійності серверів з використанням системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси. Об’єктом дослідження дисертаційної роботи є процес захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак. Предметом дослідження дисертаційної роботи є системи захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак. В дисертаційній роботі проведено аналіз існуючих та сучасних методів, моделей та систем протидії низькошвидкісним HTTP DDoS-атакам. Встановлено, що традиційні підходи, такі як обмеження трафіку або сигнатурний аналіз, недостатньо ефективні через

динамічний характер атак, що використовують легальні HTTP-запити. На основі цього сформульовано вимоги до системи, зокрема необхідність аналізу груп пакетів та аномалій на рівні мережевої взаємодії. Метою дослідження є зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси. В процесі досягнення зазначеної мети та вирішення наукового завдання у роботі одержано основні наукові результати: • вперше розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача, яка за рахунок виявлення аномального потоку, алгоритму фільтрації трафіку, модуля пам'яті, дозволить передувати та протидіяти низькошвидкісним HTTP DDoS-атакам на рівні кінцевого користувача; • вперше розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, який за рахунок умов фільтрації трафіку, а саме обмеження кількості запитів з одного IP/підмережі, блокування трафіку з регіонів, де немає клієнтів, тривалості запиту, дає можливість зменшити навантаження на сервер від 40 до 60 % і підтримати цілісність системи. • вперше розроблено систему протидії низькошвидкісним HTTP DDOS-атакам на веб-ресурси з урахуванням аномалій в пакетах, яка за рахунок розроблених моделі та методу, дає можливість упередженню та покращенню захисту від низькошвидкісних HTTP DDoS-атак на 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей. Дані особливості порівнюються з вхідним трафіком (відбувається онлайн виявлення), під час якого виявлені аномалії, та низькошвидкісні HTTP DDoS-атаки передаються для «Навчання ШІ» після опрацювання передаються до блоку «Даних про навчання». Історія навчань використовується при наступних виявленнях загроз. Експериментальна оцінка ефективності розробленої системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси показала, що розроблена система знижує навантаження на сервер на 40–60% порівняно з базовими рішеннями. Точність виявлення атак становить 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей. У вступі обґрунтовано актуальність теми дисертації, сформульовано мету і завдання дослідження, визначено наукову та практичну цінність отриманих результатів і особистий внесок автора у спільних публікаціях. У першому розділі проаналізовано методи, моделі та системи упередження низькошвидкісних HTTP DDoS-атак. Проаналізовано системи протидії DDoS атакам які застосовуються на території України, враховано всі особливості, та сформульовано обґрунтований напрям наукового вирішення проблеми. Системи які було проаналізовані наведені в табл. 1.1 з урахуванням їх особливостей за 10 основними характеристиками безпеки. У другому розділі запропоновано модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача. Досліджено та вдосконалено модель за допомогою фільтрування особливостей пакетів з використанням Штучного інтелекту. Розроблено комплексну модель виявлення аномального потоку, яка враховує наступні особливості: - наявність пустих пакетів; - час тривалості запиту; - кодування регіону. Для оцінки захищеності користувачів використовуються попередньо згадані особливості, при виявлені аномалій дані опрацьовуються ШІ та передаються для блоку «Дані про навчання». Аномалії, які виявлені таким шляхом будуть враховані при наступному колі фільтрації вхідного трафіку. Також у даному розділі удосконалено алгорим роботи методу раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак на основі аналізу обробки пакетних груп. Що забезпечує ретельніший захист кінцевого користувача від аномалій, поведінка яких схожа на низькошвидкісні HTTP DDoS-атаки. Наступним кроком даного розділу було вперше розроблено та представлено Систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси. Яка складається з моделі упередження низькошвидкісних HTTP DDoS-атак з використанням штучного інтелекту, алгоритму фітрації та модуля виснаження пам'яті при DDoS-атаці.

2. Ponomochovnyi P.M. System for Counteracting the Anticipation of Low-Rate HTTP DDoS Attacks on Web Resources. - Qualification scientific work on the rights of manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 125 - "Cybersecurity" (12 - Information Technology). - State University of Information and Communication Technologies, Kyiv, 2025. The dissertation is devoted to improving the reliability of servers through the implementation of a system to counter the impact of low-rate HTTP DDoS attacks on web resources. The object of the dissertation research is the process of protecting web resources from low-rate HTTP DDoS attacks. The subject of the study is systems for protecting web resources against low-rate HTTP DDoS attacks. The dissertation analyzes existing and modern methods, models, and systems for countering low-rate HTTP DDoS

attacks. It is established that traditional approaches—such as traffic limiting or signature-based analysis—are insufficiently effective due to the dynamic nature of attacks that exploit legitimate HTTP requests. Based on this, system requirements were formulated, particularly the need for packet group analysis and anomaly detection at the network interaction level. The aim of the research is to reduce the effectiveness of low-rate HTTP DDoS attacks on web resources. To achieve this goal and solve the scientific problem, the dissertation presents the following main scientific results: For the first time, a model was developed to preempt low-rate HTTP DDoS attacks at the end-user level, enabling early detection and mitigation of such attacks through traffic anomaly detection, filtering algorithms, and memory modules. For the first time, a method for early detection and protection against low-rate HTTP DDoS attacks was developed. By applying specific filtering conditions—such as limiting the number of requests from a single IP/subnet, blocking traffic from regions without clients, and measuring request duration—the server load can be reduced by 40–60% while preserving system integrity. For the first time, a system was designed to counter low-rate HTTP DDoS attacks on web resources, taking into account packet anomalies. This system, based on the developed model and method, improves detection and mitigation by 73% through a combination of packet group analysis and dynamic traffic characteristics. These characteristics are compared to incoming traffic (real-time detection), and the identified anomalies and low-rate HTTP DDoS attacks are transmitted to the "AI Training" module. After processing, data is stored in the "Training Data" block. The training history is used for subsequent threat detections. Experimental evaluation of the developed system showed a 40–60% reduction in server load compared to baseline solutions. Attack detection accuracy reached 73% due to the combination of packet group analysis and traffic dynamics. The introduction justifies the relevance of the dissertation topic, outlines the aim and objectives of the study, defines the scientific and practical value of the obtained results, and specifies the author's personal contribution to joint publications. Chapter One analyzes methods, models, and systems for preempting low-rate HTTP DDoS attacks. It examines DDoS countermeasures used in Ukraine, considers their specific features, and formulates a scientifically justified approach to solving the problem. The analyzed systems are summarized in Table 1.1 based on 10 key cybersecurity characteristics. Chapter Two proposes a model for preempting low-rate HTTP DDoS attacks at the end-user level. The model is enhanced through packet feature filtering using artificial intelligence. A comprehensive model for detecting anomalous traffic was developed, taking into account: - the presence of empty packets; - request duration; - region-based encoding. These features are used to assess user protection. Upon detecting anomalies, the data is processed by AI and transferred to the “Training Data” module. These anomalies will be considered in the next round of input traffic filtering. The chapter also improves the early detection method based on packet group analysis to better protect end-users from behavior resembling low-rate HTTP DDoS attacks. Furthermore, a System for Countering Low-Rate HTTP DDoS Attacks was designed for the first time. It includes a model based on AI, a traffic filtering algorithm, and a memory exhaustion protection module. These components form an effective solution for securing end users. Chapter Three presents the validation of the developed system. It evaluates incoming traffic using anomaly detection methods and monitors server load. The results show that the system performs its tasks effectively and adapts rapidly by filtering out malicious/anomalous traffic.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 1. Лук’яненко Т.Ю. (Lukyanenko T. Yu.), Поночовний П.М. (Ponochovnyy P. M.), Легомінова С.В. (Lehominova S. V.), Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу // Сучасний захист інформації, 2022. – № 2. – 15-21. Режим доступу:

https://doi.org/10.31673/2409-7292.2022.021521
- 2. Опанасенко М.І., Поночовний П.М., Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // Сучасний захист інформації, 2023. – № 1. – С.72-78. Режим доступу: https://doi.org/10.31673/2409-7292.2023.010010
- 3. Прокопенко А.Г., Лаврінець К.Г., Поночовний П.М., Оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення // Зв'язок, 2024. – № 4. – С.19-23. Режим доступу: https://doi.org/10.31673/2412-9070.2024.041923
- 4. Савченко В.А., Поночовний П.М., Аверічев І.М. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. // Прикладні проблеми комп`ютерних наук, безпеки та математики. Луцьк: Волинський національний університет імені Лесі Українки, 2024. №3. – С.71-76. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127
- 5. Поночовний П.М. Модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача // Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка. Київ: Київський столичний університет імені Бориса Грінченка, 2024. Том 2 № 26. – С.291-304. Режим доступу: https://doi.org/10.28925/2663-4023.2024.26.695
- 6. Поночовний П.М., Іванченко І.С. Метод раннього виявлення та захисту від мінливих DDoS атак на основі аналізу обробки пакетних груп // Наукові записки ДУІКТ – 2024. No2. – С.153-164. Режим доступу: https://doi.org/10.31673/2786-8362.2024.027035
- 7. Поночовний П.М., Пепа Ю.В. Реалізація системи захисту серверівз урахуванням аномалій в пакетах // Вимірювальна та обчислювальна техніка в технологічних процесах, 2025, №2. м. Хмельницький – С.44-51. Режим доступу: https://doi.org/10.31891/2219-9365-2025-81-6
- 8. Рижаков М.М., Поночовний П.М. Модель трансформації на основі штучного інтелекту з елементами захисту від DDoS-атак // Прикладні проблеми комп'ютерних наук, безпеки та математики. 2025, №4 м. Луцьк – С. 14-32. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128
- 9. Поночовний П.М., Пепа Ю.В. Система реалізації захисту серверів з урахуванням аномалій в пакетах // Український журнал досліджень інформаційної безпеки. 2025, Том 26, №2. м. Київ С. 270-277. Режим доступу: https://doi.org/10.18372/2410-7840.26.20018
- 10. Ponochovnyy P. M., Pepa Yu. V. Method for determining vulnerabilities to ddos attacks on content management systems // The IV International Conference on emerging technology trends on the smart industry and the internet of things "TTSIIT - 2025", Kyiv National University of Construction and Architecture -january 30-31, 2025, Ukraine-Iraq-Poland pp. – 95-100. Access mode: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view
- 11. Поночовний П.М. Автоматизоване реагування на кіберінциденти за допомогою ШІ: міф чи реальність сучасних SOC? // XIIV Міжнародна науково-технічна ITSec-2025 Безпека інформаційних технологій, 2025, м. Тернопіль – с.156-159. Режим доступу: https://drive.google.com/drive/u/0/folders/1f_WDoOIyqDmVMa5eJZDJ-ABFERbSdEWG

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U100245

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Іванченко Ігор Сергійович

2. Ihor Ivanchenko

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Пепа Юрій Володимирович

2. Yurii V. Pepa

Кваліфікація: к.т.н., доц., 05.22.13

Ідентифікатор ORCID ID: 0000-0003-2073-1364

Додаткова інформація: https://orcid.org/0000-0003-2073-1364;https://www.scopus.com/authid/detail.uri?authorId=57479016800

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Хлапонін Юрій Іванович

2. Yurii Khlaponin

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-9287-0817

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет будівництва і архітектури

Код за ЄДРПОУ: 02070909

Місцезнаходження: проспект Повітряних сил, буд. 31, Київ, 03037, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович

2. Pavlo M. Skladannyi

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7775-6039

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Казмірчук Світлана Володимирівна

2. Svitlana Kazmirchuk

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0001-6083-251X

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Щавінський Юрій Віталійович

2. Yurii V. Shchavinskyi

Кваліфікація: к. т. н., доц., 20.02.14

Ідентифікатор ORCID ID: 0000-0002-2319-8983

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Іванченко Євгенія Вікторівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Іванченко Євгенія Вікторівна
Відповідальний за підготовку облікових документів	Лазоренко Людмила Михайлівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна