https://doi.org/10.31891/2219-9365-2025-81-6
УДК 004.05:62-1(045)

ПОНОЧОВНИЙ Петро
Державний університет інформаційно-комунікаційних технологій, м. Київ
https://orcid.org/0009-0008-6480-6990
e-mail: petja9186@gmail.com
ПЕПА Юрій
Державний університет інформаційно-комунікаційних технологій, м. Київ
https://orcid.org/0000-0003-2073-1364
e-mail: yurka14@ukr.net

РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ СЕРВЕРІВ З УРАХУВАННЯМ АНОМАЛІЙ В ПАКЕТАХ

У статті розглянуто методи аналізу мережевого трафіку в реальному часі, що базуються на статистичних методах, а також алгоритмах машинного навчання для класифікації мережевих пакетів за їх поведінковими характеристиками. Представлена система реалізує багаторівневий підхід до захисту серверів, який включає три основні етапи: первинну фільтрацію даних, статистичний аналіз та використання моделей машинного навчання. Представлені моделі дозволяють адаптуватися до нових типів атак шляхом автоматичного оновлення. Це дозволяє виявити як традиційні DDoS-атаки (сканування портів, експлуатація вразливостей мережевих протоколів та спроби ін'єкцій SQL-запитів), так і інші види загроз. Інтеграція представленої системи захисту з існуючими інструментами моніторингу та фаєрволами забезпечить точність раннього виявлення DDoS-атак, низький рівень хибно-позитивних спрацьовувань та надійний захист серверів у реальному часі і простоту впровадження.

Ключові слова: аномалії в пакетах, DDoS-атаки, машинне навчання, аналіз трафіку, захист серверів.

PONOCHOVNY Petro, PEPA Yuriy
State University of Information and Communication Technologies

IMPLEMENTATION OF A SERVER PROTECTION SYSTEM TAKING INTO ACCOUNT ANOMALIES IN PACKAGES

The article discusses methods of real-time network traffic analysis based on statistical methods and machine learning algorithms for classifying network packets by their behavioral characteristics. The presented system implements a multi-level approach to server protection, which includes three main stages: primary data filtering, statistical analysis, and the use of machine learning models. The relevance of this issue stems from the need to ensure real-time server protection, which requires high-speed traffic analysis and system adaptability to emerging threats. Modern solutions must not only detect known threats but also identify new, previously unknown attack patterns by analyzing traffic behavioral characteristics. The early anomaly detection module is a key component of the system, enabling the identification of potentially malicious actions at an early stage. To counter new, previously unknown types of attacks, the use of deep neural networks and clustering algorithms is particularly important, as it allows real-time analysis of traffic behavior patterns. The ability to respond to threats before they can cause harm to the infrastructure ensures effective early detection. The presented models allow adapting to new types of attacks by automatically updating them. This makes it possible to detect both traditional DDoS attacks (port scanning, exploitation of network protocol vulnerabilities and SQL injection attempts) and other types of threats. The integration of the presented protection system with existing monitoring tools and firewalls will ensure the accuracy of early detection of DDoS attacks, low false-positive rates, and reliable real-time protection of servers and ease of implementation. Future development prospects for the system include enhancing machine learning algorithms for precise anomaly detection, expanding the functionality of filtering modules, and integrating with cloud technologies to ensure the protection of scalable infrastructures.

Keywords: anomalies in packets, DDoS attacks, machine learning, traffic analysis, server protection.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах зростання кіберзагроз захист серверів стає критично важливим аспектом інформаційної безпеки, особливо в контексті збільшення обсягів мережевого трафіку та складності атак. Одним із ефективних підходів є використання систем захисту, що враховують аномалії у мережевих пакетах за поведінковими характеристиками [1]. Виявлення та обробка таких аномалій дозволяють оперативно ідентифікувати та нейтралізувати загрози, серед яких особливе місце займають DDoS-атаки.

Пропонується розробити таку систему, яка зможе реалізувати багаторівневий підхід до захисту серверів. В основу буде покладено три основні етапи: первинну фільтрацію даних, статистичний аналіз та використання моделей машинного навчання. На першому етапі будуть відсіюватися шкідливі пакети на основі простих критеріїв, таких як заборонені IP-адреси або некоректний формат пакетів [2]. На другому етапі пропонується застосувати статистичний аналіз для виявлення відхилень у розподілі трафіку, наприклад, раптове збільшення кількості запитів або зміну розміру пакетів [3]. Третій етап передбачає застосування класифікаторів, які навчаються на історичних даних для визначення аномалій у поведінці мережі. Така модель дозволить адаптуватися до нових типів атак шляхом автоматичного оновлення [4].

ISSN 2219-9365

Зростання кількості користувачів Інтернету змушує досліджувати динаміку взаємодій [5] у цифровому просторі. Це особливо актуально в контексті соціальних мереж, де динаміка відкриває перспективи для аналізу в різних сферах, включаючи маркетинг, соціологію, психологію та інші [6]. Сучасні інформаційні системи все частіше стають об'єктами кібератак, метою яких є виведення з ладу серверів, порушення роботи критичних інфраструктур та крадіжка конфіденційної інформації. Одним із найпоширеніших та найнебезпечніших видів атак є розподілені атаки типу «відмова в обслуговуванні» (DDoS), які створюють надмірне навантаження на сервери шляхом одночасного надсилання великої кількості запитів. Унаслідок цього ресурси системи вичерпуються, і вона перестає виконувати свої функції [7].

Ключовою проблемою у протидії таким загрозам є складність виявлення аномальних пакетів у трафіку, особливо зважаючи на постійний розвиток технік атакуючих. Традиційні методи захисту, засновані на сигнатурному аналізі або чорних списках, більше не здатні ефективно протидіяти сучасним атакам, які часто змінюють свої шаблони та обходять фільтри [8].

У відповідь на ці виклики науковці та фахівці з кібербезпеки розробляють нові підходи, що базуються на аналізі поведінкових аномалій у мережевих пакетах. Використання методів машинного навчання, нейронних мереж та статистичних алгоритмів дозволяє системам адаптуватися до нових типів загроз, виявляючи навіть найменші відхилення у поведінці трафіку. Такий підхід забезпечує швидке реагування на DDoS-атаки та інші форми загроз, зберігаючи стабільну роботу серверів [9].

У роботі розглянуто підходи до захисту серверів на основі аналізу аномалій у пакетах та акцентовано увагу на використанні багаторівневого підходу, який поєднує фільтрацію, статистичний аналіз та методи машинного навчання. Особливий акцент зроблено на практичній реалізації системи та її інтеграції з існуючими інструментами моніторингу.

Сучасний розвиток цифрових технологій супроводжується значним зростанням обсягу мережевого трафіку та збільшенням кількості кібератак, спрямованих на порушення роботи інформаційних систем. Особливу загрозу становлять розподілені атаки типу «відмова в обслуговуванні» (DDoS), які здатні блокують роботу серверів, спричиняючи значні фінансові збитки та загрожуючи конфіденційності даних. Традиційні засоби захисту, засновані на сигнатурному аналізі або фільтрації за чорними списками, стають дедалі менш ефективними через складність і змінність сучасних атак, які використовують динамічні шаблони для обходу систем захисту.

Основною проблемою низькошвидкісних DDoS атак є виявлення аномалій у мережевих пакетах, які можуть свідчити про початок кібератаки. У зв'язку з постійним зростанням обсягу даних які передаються визначення відхилень від нормальної поведінки мережі стає складнішим. Існуючі підходи не забезпечують необхідної точності виявлення, мають високу частку хибно-позитивних спрацювань, та призводять до збоїв у роботі систем та блокуванні користувачів.

Актуальність проблеми зумовлюється необхідністю забезпечення захисту серверів у реальному часі, що потребує високої швидкості аналізу трафіку та адаптивності системи до нових типів загроз. Сучасні рішення повинні не лише виявляти відомі загрози, але й бути здатними ідентифікувати нові, раніше невідомі патерни атак, базуючись на аналізі поведінкових характеристик трафіку.

Таким чином, постає потреба у розробці ефективної системи захисту серверів, яка базується на багаторівневому аналізі аномалій у мережевих пакетах. Для забезпечення максимальної точності та адаптивності система повинна поєднувати методи первинної фільтрації, статистичного аналізу та алгоритмів машинного навчання. Вирішення проблеми дозволить значно підвищити стійкість серверів до кібератак, забезпечуючи надійність і безперервність функціонування інформаційних систем.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження новітніх перспективних підходів та моделей для створення ефективної системи захисту серверів від повільних DDoS-атак, які на ранньому етапі враховують аномалії в пакетах даних. Описана система реалізує багаторівневий підхід для захисту серверів, який містить три основні етапи: первинну фільтрацію даних, статистичний аналіз та використання моделей машинного навчання.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблема захисту серверів на основі аналізу аномалій у мережевих пакетах отримала значну увагу в наукових публікаціях останніх років. У дослідженнях науковці зосереджені на ранньому виявленні аномалій, розробці ефективних алгоритмів фільтрації та інтеграції цих рішень у єдину систему.

1. Раннє виявлення аномалій.

Сучасні методи раннього виявлення загроз значною мірою базуються на використанні машинного навчання. Наприклад, дослідження демонструють ефективність застосування глибоких нейронних мереж для класифікації мережевих пакетів у режимі реального часу [10]. Особливої уваги заслуговує підхід, запропонований у [11], де використовуються рекурентні нейронні мережі (RNN) для аналізу тимчасових

залежностей у мережевому трафіку, що дозволяє ідентифікувати початкові етапи DDoS-атак. Додатково, у [12] розглянуто використання алгоритмів кластеризації для виявлення раніше невідомих аномалій у трафіку.

2. Алгоритми фільтрації.

Алгоритми фільтрації є ключовим елементом багаторівневих систем захисту. У [13] запропоновано адаптивний метод фільтрації на основі частотного аналізу мережевих запитів, що дозволяє відсівати шкідливі пакети ще до надходження до основної системи обробки. Інше рішення, описане у [14], включає інтеграцію фільтрації на основі сигнатур із поведінковим аналізом для підвищення точності виявлення. Ці підходи демонструють ефективність у виявленні як традиційних атак, так і нових видів загроз.

3. Комплексні рішення.

Інтеграція раннього виявлення та ефективних алгоритмів фільтрації дозволяє створювати комплексні системи захисту. У [15] запропоновано систему, яка об'єднує статистичний аналіз, класифікацію трафіку та оновлювані моделі машинного навчання. Це рішення дозволяє забезпечити високу точність і швидкість реагування на загрози. Інше комплексне рішення представлено в [16], де поєднано виявлення аномалій із автоматичним оновленням фільтрів, що підвищує адаптивність системи до змін у поведінці атакуючих.

Таким чином, аналіз досліджень свідчить про значний прогрес у ранньому виявленні аномалій і розробці алгоритмів фільтрації. Інтеграція цих компонентів у комплексні системи захисту є перспективним напрямом, який потребує подальшого вивчення.

ОСНОВНА ЧАСТИНА

Раннє виявлення.

Для створення системи реалізації захисту серверів запропоновано модель раннього виявлення. Модель має різні особливості. На рисунку 1, представлено процес виявлення, який поділяється на два основні етапи:

1. *Етап 1* виконує попередню обробку, а дані мережевого трафіку збираються за допомогою методу часового вікна. Звичайна атака займає часове вікно 2 с і збирає дані один раз; повільна атака займає часове вікно 5 секунд і збирає дані один раз;

2. *Етап 2* виконує навчальне моделювання CNN з виявленням аномалій у реальному часі та сповіщенням про онлайн-дані (рис. 1).

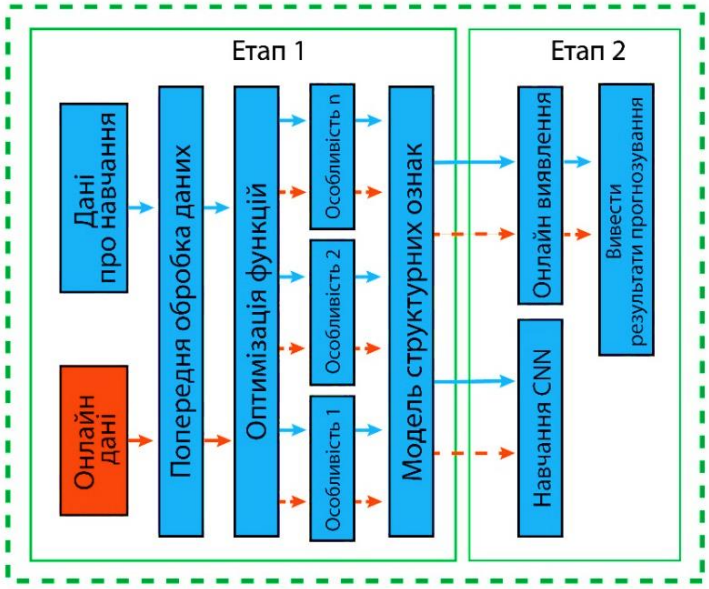

Рис. 1. Модель виявлення аномального потоку

Алгоритм фільтрації трафіку.

Коли контролер отримує невідомий пакет через протокол OpenFlow, пакет містить повну інформацію про пакет. Після того, як контролер отримає пакет, відбувається аналіз інкапсуляцію пакету, аналізуючи кожен шар пакета. Таким чином можна створити таблицю потоку для пакета на основі вилученої інформації. Надалі вихідний пакет передається на плату обміну через протокол OpenFlow. Який містить інтерфейс для пересилання. На основі цього принципу пакети, надіслані платою обміну, обробляються та необхідна інформація вилучається та передається навченій моделі для ідентифікації та прогнозування. На рис. 2 представлено алгоритм фільтрації трафіку.

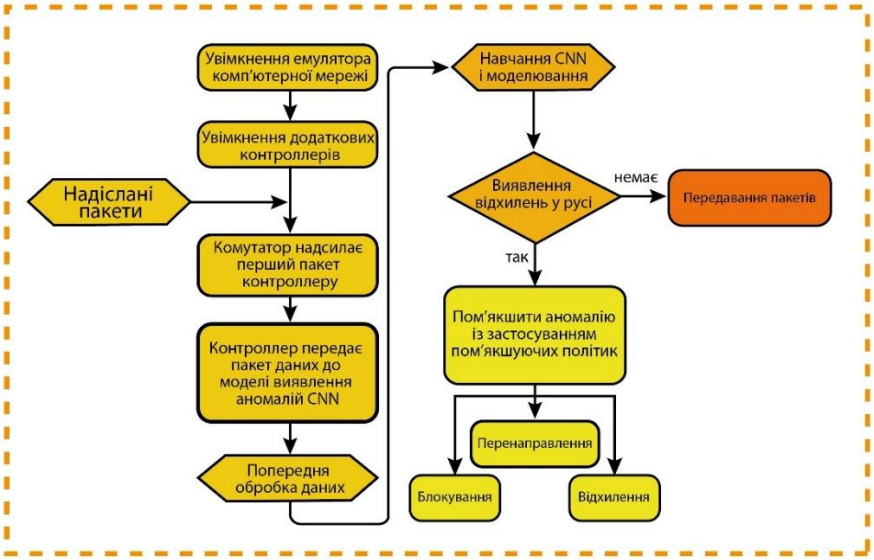

Рис. 2. Алгоритм фільтрації трафіку

Спочатку запускаємо емулятор комп'ютерної мережі і контролер, який надсилає пакети, в цей час комутатор пересилає перший пакет контролеру. Контролер передає пакет до моделі виявлення аномалії CNN. Після попередньої обробки даних навчання та моделювання CNN використовуються для виявлення аномального трафіку. Якщо це звичайний трафік, пакет передається безпосередньо. При виявленні аномального трафіку пом'якшити атаку пропонується за допомогою, блокування, перенаправлення та відхилення.

Модель DDoS-атаки на виснаження пам'яті.

У DDoS-атаці з виснаженням пам'яті жертва повинна обслуговувати запити як від законних користувачів, так і від атакуючих ботів, як у DDoS-атаці з виснаженням пропускної здатності. Тому в цій моделі можна використовувати той самий процес Пуассона [17] для представлення вхідного трафіку. Однак у цьому випадку підходить аналіз трафіку на рівні пакетів.

Зазвичай певні дані зберігаються в буфері пам'яті лише для відповідного етапу сеансу, наприклад? встановлення з'єднання в протоколі TCP. Тому аналіз трафіку на рівні сеансу більше підходить для представлення DDoS-атаки на виснаження пам'яті. Беручи до уваги це, середній розмір пакета або сесії не має значення. Середня швидкість надходження сеансу бота $\lambda_{\text{СБ}}$ і середня швидкість надходження законного сеансу користувача $\lambda_{\text{СК}}$ достатньо, щоб описати загальний вхідний трафік $\lambda_{\text{ВТ}}$.

Як і в моделі DDoS-атаки із виснаженням пропускної здатності, загальна швидкість надходження $\lambda_{\text{ВТ}}$ залежить від системної фільтрації, а саме від імовірності хибно-позитивних параметрів $P_{\text{ХП}}$ і хибно-негативних $P_{\text{ХН}}$, а також від середньої швидкості надходження сеансів ботів і законних користувачів $\lambda_{\text{ЗК}}$, і кількості ботів $\lambda_{\text{КБ}}$ в атаці:

$$\lambda_{\text{СБ}} = \sum_{i=1}^{n} \lambda_{\text{СК}_i};$$

$$\lambda'_{\text{СБ}} = \lambda_{\text{СБ}} \cdot P_{\text{ХН}};$$

$$\lambda'_{\text{КБ}} = \lambda_{\text{КБ}} \cdot \left(1 - P_{\text{ХП}}\right);$$

$$\lambda_{\text{ВТ}} = \lambda'_{\text{КБ}} + \lambda'_{\text{СБ}}.$$

Під час DDoS-атаки з виснаженням пам'яті жертва зберігає вхідні запити до тих пір, поки вони не будуть остаточно обслуговані. Однак буфер пам'яті обмежений і здатний зберігати до N сеансів одночасно. Усі збережені сеанси обслуговуються не в черзі буфер FIFO (першим прийшов, першим вийшов), а обслуговуються під час перебування в черзі. Тому пропонується використовувати чергу M/M/N/N.

У цій моделі є N послуг, які представляють, скільки даних сеансу можна зберегти в буфері пам'яті. Коли немає черги очікування, і нові дані сеансу можна зберігати, лише якщо в буфері пам'яті є хоча

б одне вільне місце. Інакше, якщо вся пам'ять зайнята, нові запити відкидаються, не обслуговуючи їх, незалежно від того, чи це запит від законного користувача чи бота (рис. 3).

Для спрощення моделі та труднощів розрізнення атаки [18] та законних сеансів у реальному часі використовуємо загальний середній час обслуговування $t_{\text{О}}$ (1), який описує середній час зберігання даних сеансу в буфері пам'яті (неважливо, чи це атака). або дані законного сеансу користувача):

$$t_{\text{О}} = \frac{\lambda'_{\text{КБ}}}{\lambda_{\text{ВТ}}} \cdot t_{\text{ЗС}} + \frac{\lambda'_{\text{СБ}}}{\lambda_{\text{ВТ}}} \cdot t_{\text{АС}} = \frac{\lambda'_{\text{КБ}} \cdot t_{\text{ЗС}} + \lambda'_{\text{СБ}} \cdot t_{\text{АС}}}{\lambda_{\text{ВТ}}} . \quad (1)$$

Загальний середній час обслуговування сеансу $t_{\text{О}}$, загальна середня швидкість надходження сеансу $\lambda_{\text{ВТ}}$ і розмір буфера пам'яті N можуть бути використані для розрахунку ймовірності падіння запиту $P_{\text{ПЗ}}$, викликаного недостатнім розміром пам'яті:

$$P_{\text{ПЗ}} = \frac{\frac{p^N}{N!}}{\sum_{j=0}^{N} \frac{p^j}{j!}}, \text{ де } p = \lambda_{\text{ВТ}} \cdot t_{\text{О}} . \quad (2)$$

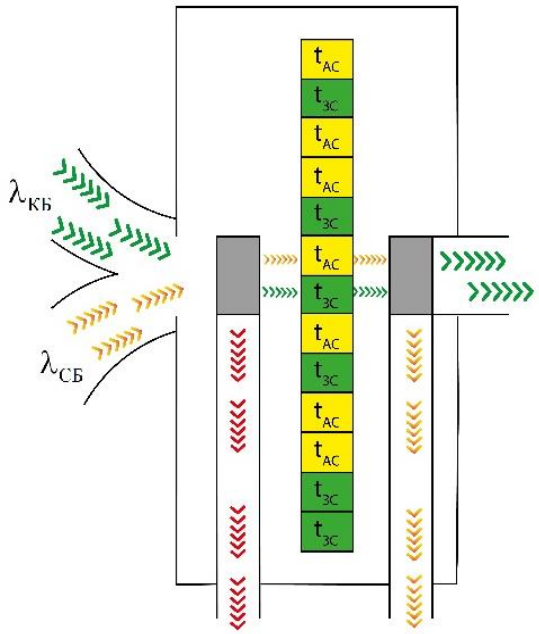

Рис. 3. Приклад моделі DDoS-атаки з виснаженням пам'яті

Імовірність успіху DDoS-атаки з вичерпанням пам'яті $P_{\text{ВП}}$ представляє частку законних сеансів користувача, які не обслуговувалися під час фільтрації або недостатньо пам'яті в буфері для їх зберігання:

$$P_{\text{ВП}} = P_{\text{ХП}} + P_{\text{ПЗ}} \cdot \left(1 - P_{\text{ХП}}\right) . \quad (3)$$

В статті не аналізуються зміни характеристик фільтрації системи в залежності від вхідного трафіку. Ці ймовірності використовуються як постійні, однак їх можна змінити на потрібні функції.

Реалізація.

Для перевірки результатів фільтрації пакетів DDoS-атак була застосована експериментальна установка у вигляді сервера, оснащеного Ubuntu 20.04, процесором Intel Core i7-1165G7 з частотою 2,80 ГГц і 16 ГБ оперативної пам'яті. Для емуляції топології мережі використовувалась платформа Mininet 2.3.0, яка полегшує створення віртуальної мережі, що включає хости, комутатори, контролери та запити. В якості комутатора обрано Cisco з відповідними налаштуваннями [19]. Щоб імітувати динаміку DDoS-атаки,

застосовано утиліту hping3, яка відома тим, що надсилає спеціалізовані пакети TCP/IP. Крім того, для створення пропускної здатності та затримки, необхідних для ініціювання атаки, задіяний Iperf, надійний інструмент маніпулювання пакетами [6].

Сценарій перед DDoS-атакою.

Вивчаючи графік, зображений на рис. 3, стає очевидним, що з плином часу існує коливання швидкості потоку в діапазоні від 9,3 до 10,5 Мбіт/с. Ця зміна зберігається до 12-ї одиниці часу, після чого швидкість потоку стабілізується на рівні 9,6 Мбіт/с. Після подальшого розгляду виявилася тенденція до зниження швидкості потоку, що стало очевидним, оскільки вимірювання падає до 9,38 Мбіт/с до 15-ї одиниці часу. Після цього моменту зміни пропускної здатності стають більш вираженими, що збігається з атакою DDoS (рис. 4).

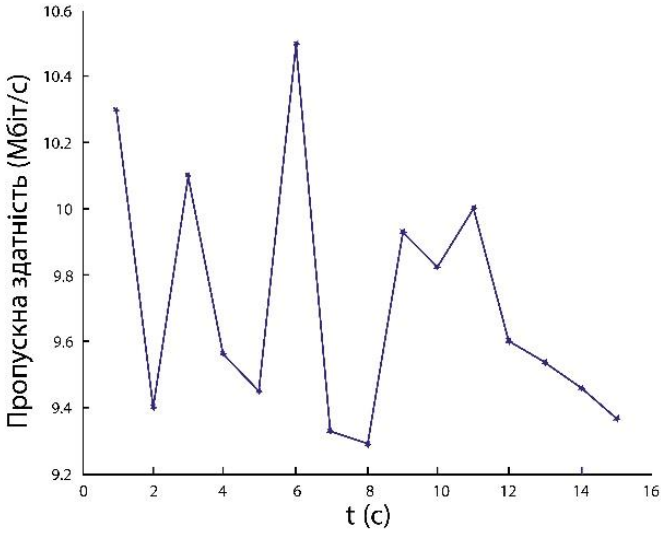

Рис. 4. Пропускна здатність перед сценарієм DDoS-атак

Сценарій після DDoS-атаки.

Звертаючись до графіка, зображеного на рис. 4, помітний початковий сплеск, при цьому потік досягає найвищого значення 630 Мбіт/с у момент часу 1. Згодом слідує помітне зменшення, що супроводжується коливаннями в діапазоні від 8 до 12 Мбіт/с. Ця закономірність приводить нас до висновку, що зниження пропускної здатності стає очевидним після DDoS-атаки (рис. 5).

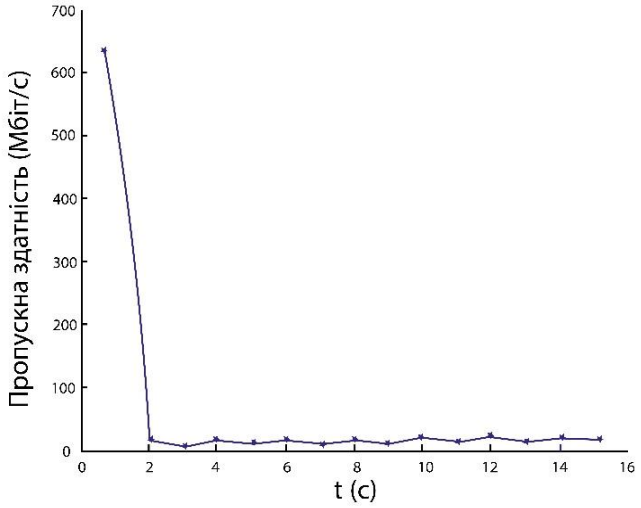

Рис. 5. Пропускна здатність після сценарію DDoS-атаки

Для побудови ефективної системи захисту серверів пропонується інтеграція раннього виявлення з алгоритмами фільтрації, яка забезпечує потужну основу. Наприклад, моделі, що використовують оновлювальні алгоритми машинного навчання, дозволяють адаптуватися до змін у шаблонах атак.

Одночасно, багаторівневий підхід, який поєднує статистичний аналіз, класифікацію та поведінкове фільтрування, мінімізує хибно-позитивні результати та знижує навантаження на систему.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У протидії загрозам при виявленні аномалій у мережевих пакетах трафіку розробка ефективних систем захисту серверів є надзвичайно актуальним завданням. Використання підходів, що базуються на ранньому виявленні аномалій і алгоритмах фільтрації трафіку, дозволяє створити комплексну систему, яка забезпечує високу надійність та адаптивність до сучасних загроз.

Модуль раннього виявлення аномалій є ключовим елементом системи, який дозволяє ідентифікувати потенційно шкідливі дії на ранніх етапах. Для протидії новим, раніше невідомим типам атак, особливо важливим є застосування глибоких нейронних мереж і алгоритмів кластеризації, що дозволяє аналізувати поведінкові патерни трафіку в реальному часі. Можливість реагувати на загрози ще до того, як вони зможуть завдати шкоди інфраструктурі, забезпечу раннє виявлення.

Алгоритми фільтрації трафіку виконують функцію блокування шкідливих пакетів, використовуючи багаторівневий підхід. Щоб забезпечити точну ідентифікацію шкідливих запитів пропонується включення частотного, сигнатурного та поведінкового аналізу. Такий підхід дозволяє уникнути високого рівня хибно-позитивних спрацьовувань, що є критично важливим для підтримки стабільної роботи серверів.

Інтеграція цих двох компонентів у єдину систему дозволила створити багаторівневий механізм захисту, який:

- здійснює моніторинг і аналіз трафіку в реальному часі;
- швидко адаптується до нових патернів атак завдяки самонавчальним моделям;
- забезпечує масштабованість і простоту інтеграції з існуючими інфраструктурами;
- забезпечує високий рівень стійкості серверів до DDoS-атак та інших форм кіберзагроз.

Наведемо переваги представленої системи захисту серверів:

1) виявляння як традиційних DDoS-атак (сканування портів, експлуатація вразливостей мережевих протоколів та спроби ін’єкцій SQL-запитів [20-22]), так і інші видів мережевих загроз;

2) інтеграція системи з існуючими програмними інструментами моніторингу та фаєрволами, що посилює рівень захисту каналу передачі пакетів даних.

Подальші перспективи розвитку системи включають вдосконалення алгоритмів машинного навчання для точного виявлення аномалій, розширення функціональності модулів фільтрації, а також інтеграцію з хмарними технологіями які забезпечують захист масштабованих інфраструктур. Використання сучасних інструментів штучного інтелекту та аналітики відкриває нові можливості у створенні надійних та адаптивних систем захисту серверів.

Література

1. Yu, S., Lu, X., & Zhu, Y. (2022). Traffic Classification Techniques in Network Security. Springer.

2. Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using novel information theory metrics. Computer Networks, 116, 96-110.

3. Akbanov M., & Koucheryavy, A. (2021). Adaptive Anomaly Detection for Cybersecurity. Wiley.

4. Jain R., & Agrawal, R. (2019). Network Intrusion Detection Systems: A Machine Learning Perspective. Computers & Security.

5. Wang P., & Gu, G. (2020). Real-Time Traffic Anomaly Detection Using Hybrid Approaches. Journal of Network Security.

6. Zhurakovsky, B., Averichev, I., & Shakhmatov, I. (2023). Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. In Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 116-126.

7. Doriguzzi-Corin, R., Millar, S., & Scott-Hayward, S. (2021). Dataset-Driven DDoS Attack Detection Using Neural Networks. IEEE Transactions on Network and Service Management.

8. Zargar, S. T., Joshi, J., & Tipper, D. A. (2020). Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials.

9. Miao, Y., Gong, Z., & Zhou, W. (2022). Machine Learning-Based DDoS Detection and Mitigation in SDN Environments. Elsevier.

10. Radovanović, M., & Filipović, N. (2021). Deep Learning Techniques for Anomaly Detection in Network Traffic. IEEE Access, 2021.

11. Abawajy, J. & Hassan, M. (2022). RNN-Based Approaches for Early DDoS Detection. Elsevier.

12. Kaur, J., & Kumar, V. (2021). Unsupervised Anomaly Detection Using Clustering Techniques. Journal of Network Security.

13. Sharma, S., & Gupta, P. (2020). Frequency-Based Filtering Methods for DDoS Attack Prevention. International Journal of Computer Applications.

14. Liu, H., & Zhang, Y. (2022). Hybrid Filtering Techniques for Anomaly Detection in High-Volume Traffic. Computers & Security.

15. Park, K., & Kim, S. (2021). Integrated Multi-Layer Network Defense Against DDoS. Springer.

16. Zhu, Y., & Chen, L. (2023). Adaptive Filtering and Anomaly Detection in Real-Time Systems. IEEE Transactions on Information Forensics and Security.

17. Стефурак, О.Р., Тихонов, Ю.О., Лаптєв, О.А., & Зозуля, С.А. (2020). Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. Сучасний захист інформації, 2(42), 19-26.

18. Пепа, Ю.В., Хорошко, В.О., Хохлачова, Ю.Є. & Аль-Далваш, А. (2024). Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз. Сучасний захист інформації, 1(57), 69-76.

19. Опанасенко, М.І., & Поночовний, П.М. (2023). Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock. Сучасний захист інформації, 1(53), 72-78.

20. Пархомей, І., Бойко, Ю., & Лемешко, В. (2024). Алгоритм налаштування кількості потоків для виконання фонових задач. Measuring and computing devices in technological processes, (4), 162–173. https://doi.org/10.31891/2219-9365-2024-80-20.

21. Пархомей, І., Бойко, Ю., & Лемешко, В. (2025). Математична модель та адаптивне управління алгоритмом обслуговування даних журналу в умовах змінного серверного навантаження. Herald of Khmelnytskyi National University. Technical Sciences, 347(1), 168-174. https://doi.org/10.31891/2307-5732-2025-347-23.

22. Семенко, А. І., Бойко, Ю. М., Шпур, О. М., Стрелковська, І. В., Корчинський, В. В., & Яровий, Р. О. (2024). Сучасні технології інфокомунікаційних та комп'ютерних мереж. Європейський університет, ФО-П Білецький Р.Г.

References

1. Yu, S., Lu, X., & Zhu, Y. (2022). Traffic Classification Techniques in Network Security. Springer.

2. Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using novel information theory metrics. Computer Networks, 116, 96-110.

3. Akbanov M., & Koucheryavy, A. (2021). Adaptive Anomaly Detection for Cybersecurity. Wiley.

4. Jain R., & Agrawal, R. (2019). Network Intrusion Detection Systems: A Machine Learning Perspective. Computers & Security.

5. Wang P., & Gu, G. (2020). Real-Time Traffic Anomaly Detection Using Hybrid Approaches. Journal of Network Security.

6. Zhurakovsky, B., Averichev, I., & Shakhmatov, I. (2023). Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. In Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 116-126.

7. Doriguzzi-Corin, R., Millar, S., & Scott-Hayward, S. (2021). Dataset-Driven DDoS Attack Detection Using Neural Networks. IEEE Transactions on Network and Service Management.

8. Zargar, S. T., Joshi, J., & Tipper, D. A. (2020). Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials.

9. Miao, Y., Gong, Z., & Zhou, W. (2022). Machine Learning-Based DDoS Detection and Mitigation in SDN Environments. Elsevier.

10. Radovanović, M., & Filipović, N. (2021). Deep Learning Techniques for Anomaly Detection in Network Traffic. IEEE Access, 2021.

11. Abawajy, J. & Hassan, M. (2022). RNN-Based Approaches for Early DDoS Detection. Elsevier.

12. Kaur, J., & Kumar, V. (2021). Unsupervised Anomaly Detection Using Clustering Techniques. Journal of Network Security.

13. Sharma, S., & Gupta, P. (2020). Frequency-Based Filtering Methods for DDoS Attack Prevention. International Journal of Computer Applications.

14. Liu, H., & Zhang, Y. (2022). Hybrid Filtering Techniques for Anomaly Detection in High-Volume Traffic. Computers & Security.

15. Park, K., & Kim, S. (2021). Integrated Multi-Layer Network Defense Against DDoS. Springer.

16. Zhu, Y., & Chen, L. (2023). Adaptive Filtering and Anomaly Detection in Real-Time Systems. IEEE Transactions on Information Forensics and Security.

17. Stefurak, O.R., Tikhonov, Y.O., Laptev, O.A., & Zozulya, S.A. (2020). Improvement of the Stochastic Model for Determining the Threats of Damage or Unauthorized Information Leakage. Modern Information Protection, 2(42), 19-26.

18. Pepa, Y.V., Khoroshko, V.O., Khokhlachova, Y.E., & Al-Dalvash, A. (2024). Methods of Analysis and Assessment of Security of Information Security Systems Taking into Account the Degree of Overlap of Threats. Modern Information Protection, 1(57), 69-76.

19. Opanasenko, M.I., & Ponochovnyi, P.M. (2023). Technology for Ensuring Cybersecurity of the Cloud Environment Based on the Cisco Cloudlock Solution // Modern Information Protection, 1(53), 72-78.

20. Parkhomey I., Boiko J., & Lemeshko V. (2024). Algorithm for configuring the number of threads for background task execution. Measuring and computing devices in technological processes, (4), 162–173. https://doi.org/10.31891/2219-9365-2024-80-20.

21. Parkhomey, I., Boiko, J., & Lemeshko, V. (2025). Mathematical model and adaptive control of a data log management algorithm under variable server load conditions. Herald of Khmelnytskyi National University. Technical Sciences, 347(1), 168-174. https://doi.org/10.31891/2307-5732-2025-347-23.

22. Semenko, A. I., Boiko, J. M., Shpur, O. M., Strelkovska, I. V., Korchynskyi, V. V., & Yarovyi, R. O. (2024). Suchasni tekhnolohii infokomunikatsiinykh ta kompiuternykh merezh. European University, LLC Biletskyi R.H.