Є.В. та ін. Нетрадиційні релігійні та містичні культи України: Навчальний посібник/ За заг. редакцією В.В. Остроухова. – К. , 2003. – 336 с.

ORGANIZING STUDENT OLYMPIADS AND OTHER COMPETITIONS IN INFORMATION SECURITY: IMPLEMENTING THEIR OUTCOMES INTO THE EDUCATIONAL PROCESS

The purpose, methodology, and evaluation system of the International Student Olympiad "Ways and Mechanisms of Protecting Ukraine's Information Space from Malicious Information and Psychological Influence" and the All-Ukrainian Student Olympiad "Developing Critical Thinking Through Identifying Reliable, Unreliable, Partially Reliable, and Possibly Reliable Information" (also titled "Social Engineering: Ways and Mechanisms of Protection") are described. The VII International Conference "Protection of Democratic Values and Respect for Human Rights in the Activities of Special Services" is also presented, focusing on the specialization "Russian Aggression Against Ukraine as a Fundamental Threat to Freedom, Democratic Values, and Human Rights: Ukrainian, European, and Global Contexts." The practical significance of these competitions is demonstrated through the implementation of their outcomes into the educational process of higher education institutions. Proposals are being developed for organizing new student olympiads, particularly in non-technical aspects of information security and in the field of religious studies.

Keywords: student olympiads, malicious information and psychological influence, protection of the information space, information security, information and psychological confrontation.

Петрик Валентин Михайлович, кандидат наук з державного управління, доцент, доцент кафедри кібербезпеки, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Valentyn Petryk, PhD in Public Administration, Associate Professor of the Department of Cybersecurity of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: iszzi_open@ukr.net.

ORCID ID: 0000-0003-2301-0722.

УДК 004.05(045)

СИСТЕМА РЕАЛІЗАЦІЇ ЗАХИСТУ СЕРВЕРІВ З УРАХУВАННЯМ АНОМАЛІЙ В ПАКЕТАХ

Поночовний Петро Михайлович, Пепа Юрій Володимирович

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. Виявлення та обробка таких аномалій дозволяють оперативно ідентифікувати та нейтралізувати загрози, серед яких особливе місце займають DDoS-атаки. 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 [1]. Представлена система реалізує багаторівневий підхід до захисту серверів, який включає три основні етапи: первинну фільтрацію даних, статистичний аналіз та використання моделей машинного навчання. На першому етапі відсіюються шкідливі пакети на основі простих критеріїв, таких як заборонені IP-адреси або некоректний формат пакетів [2]. На другому етапі застосовується 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. Перелік представлених моделей дозволяє адаптуватися до нових типів атак шляхом автоматичного оновлення [4]. Наведемо переваги представленої системи: виявляє як традиційні DDoS-атаки (сканування портів, експлуатація вразливостей мережевих протоколів та спроби ін'єкцій SQL-запитів), так і інші види загроз. По-друге, її інтеграція з існуючими інструментами моніторингу та фаєрволами. Також забезпечує простоту впровадження без значного збільшення витрат завдяки інтеграції з існуючими інструментами моніторингу та фаєрволами [5]. Система відзначається високою точністю виявлення атак, низьким рівнем хибно-позитивних спрацьовувань. Та забезпечує ефективний захист серверів у реальному часі для забезпечення безперервності бізнес-процесів та запобігання фінансовим і репутаційним втратам.

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

ВСТУП

Зростання кількості користувачів Інтернету змушує досліджувати динаміку взаємодій 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.

Постановка проблеми

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.

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

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:

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

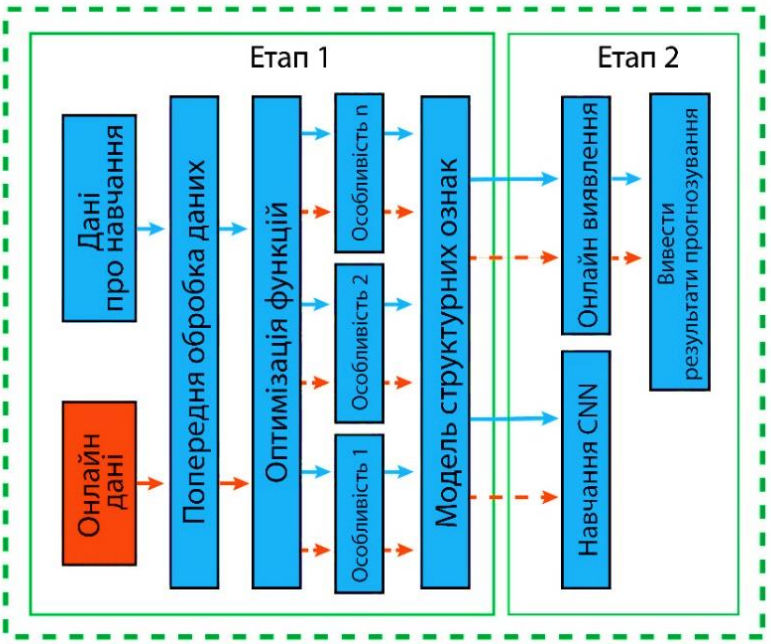

Рисунок 1. Модель виявлення аномального потоку

Алгоритм фільтрації трафіку можливо застосувати 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 рисунку 2 представлено алгоритм фільтрації трафіку.

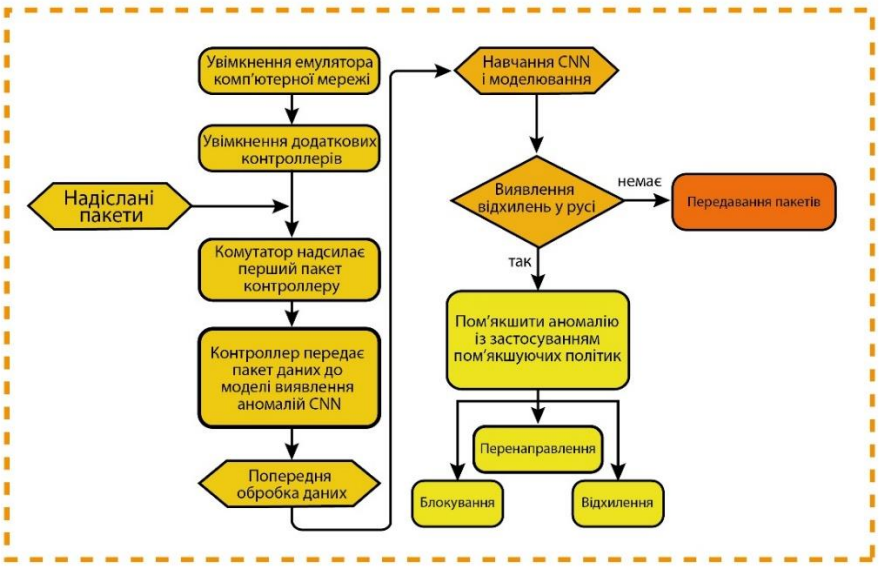

Рисунок 2. Алгоритм фільтрації трафіку

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.

У Моделі DDoS-атаки на виснаження 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 $\lambda_{СБ}$ і середня швидкість надходження законного сеансу користувача $\lambda_{СК}$ достатньо, щоб описати загальний вхідний трафік $\lambda_{ВТ}$.

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

$$\lambda_{СБ} = \sum_{i=1}^{n} \lambda_{СК_i};$$

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

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

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

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).

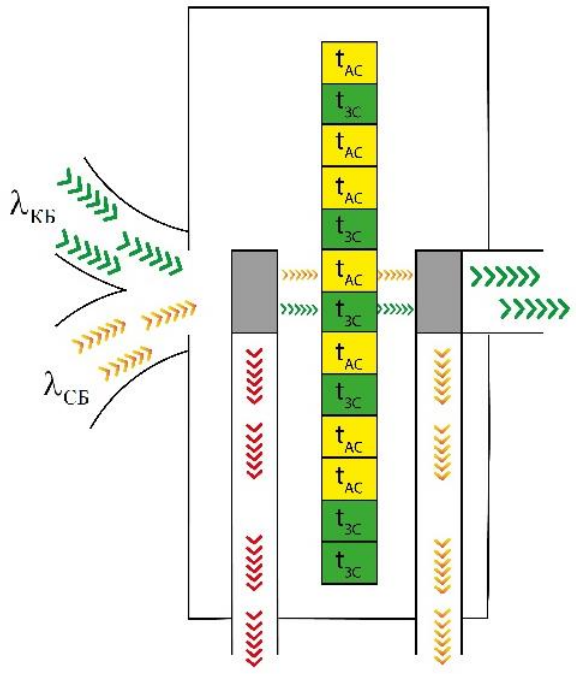

Рисунок 3 Приклад моделі DDoS-атаки з виснаженням пам'яті

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

$$t_О = \frac{\lambda'_{КБ}}{\lambda_{ВТ}} \cdot t_{ЗС} + \frac{\lambda'_{СБ}}{\lambda_{ВТ}} \cdot t_{АС} = \frac{\lambda'_{КБ} \cdot t_{ЗС} + \lambda'_{СБ} \cdot t_{АС}}{\lambda_{ВТ}}$$

. (1)

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

$$P_{ПЗ} = \frac{\frac{p^N}{N!}}{\sum_{j=0}^{N} \frac{p^j}{j!}}, \text{ де } p = \lambda_{ВТ} \cdot t_О.$$

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

$$P_{ВП} = P_{ХП} + P_{ПЗ} \cdot (1 - P_{ХП}).$$

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.

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].

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).

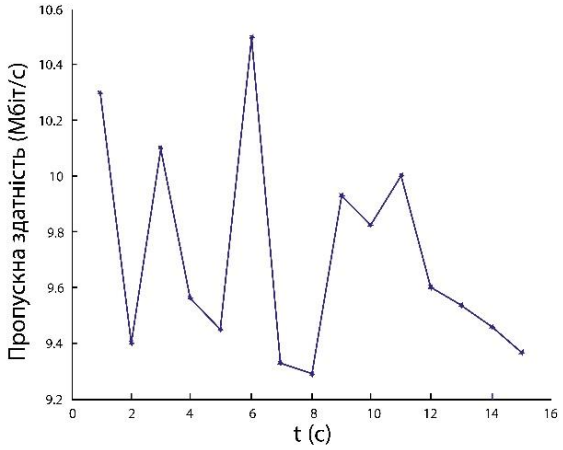

Рисунок 4 Пропускна здатність перед сценарієм DDoS-атак.

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).

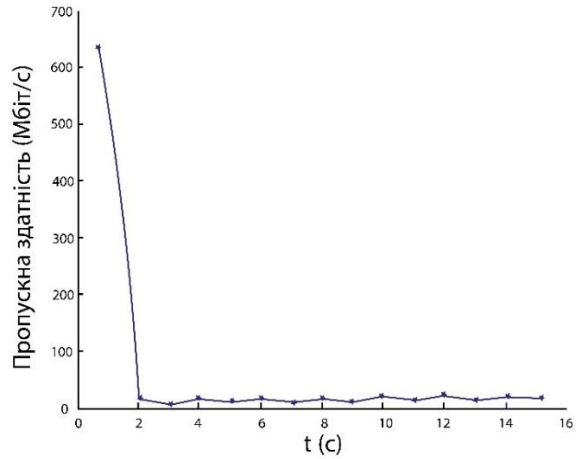

Рисунок 5 Пропускна здатність після сценарію DDoS-атаки

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

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.

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. Traffic Classification Techniques in Network Security. – Springer, 2022.

[2].Behal S., Kumar K. Detection of DDoS Attacks Using Machine Learning Algorithms. // International Journal of Computer Applications, 2020.

[3].Akbanov M., Koucheryavy A. Adaptive Anomaly Detection for Cybersecurity. – Wiley, 2021.

[4]. Jain R., Agrawal R. Network Intrusion Detection Systems: A Machine Learning Perspective. // Computers & Security, 2019.

[5]. Wang P., Gu G. Real-Time Traffic Anomaly Detection Using Hybrid Approaches. // Journal of Network Security, 2020.

[6]. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. / Bohdan Zhurakovskyi, Ihor Averichev and Ivan Shakhmatov // Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 2023. – С.116-126.

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

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

[9]. Miao Y., Gong Z., Zhou W. Machine Learning-Based DDoS Detection and Mitigation in SDN Environments. – Elsevier, 2022.

[10]. Radovanović M., Filipović N. Deep Learning Techniques for Anomaly Detection in Network Traffic. // IEEE Access, 2021.

[11]. Abawajy J., Hassan M. RNN-Based Approaches for Early DDoS Detection. – Elsevier, 2022.

[12]. Kaur J., Kumar V. Unsupervised Anomaly Detection Using Clustering Techniques // Journal of Network Security, 2021.

[13]. Sharma S., Gupta P. Frequency-Based Filtering Methods for DDoS Attack Prevention. // International Journal of Computer Applications, 2020.

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

[15].Park K., Kim S. Integrated Multi-Layer Network Defense Against DDoS. – Springer, 2021.

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

[17].Стефурак О.Р., Тихонов Ю.О., Лаптєв О.А., Зозуля С.А. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації // Сучасний захист інформації, 2020. – № 2(42). – С.19-26.

[18].Пепа Ю.В., Хорошко В.О., Хохлачова Ю.Є., Аль-Далваш А. Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз // Сучасний захист інформації, 2024. – № 1(57). – С.69-76.

[19].Опанасенко М.І., Поночовний П.М. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // Сучасний захист інформації, 2023. – № 1(53). – С.72-78.

[20] Хорошко В.О., Лаптєв О.А., Хохлачева Ю.Є., Аль-далваш Аблуллах Фоуад, Пепа Ю.В. Особливості проектування захищених інформаційних мереж. Наукоємні технології. 2024.Том 62. № 2 . С.154-163 https://doi.org/10.18372/2310-5461.62.18709

[21] Дробик О. В., Лаптєв О. А., Пархоменко І. І., Богуславська О. В., Пепа Ю. В., Пономаренко В. В. Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. Сучасний захист інформації. 2024. №2. С.13-23. https://doi.org/ 10.31673/2409-7292.2024.020002

IMPLEMENTATION OF PROTECTION OF SERVERS WITH ABNORMAL ACCOUNTS IN THE PACKAGE SYSTEM

Server protection is a very important aspect of information security as cyber threats grow, especially as network traffic increases and attack complexity. One effective approach is to use a

protection system that takes into account network packet anomalies. The detection and processing of such anomalies allows you to quickly identify and neutralize threats where DDos attacks occupy a special place. This article describes how to analyze network traffic in real time based on statistical methods and machine learning algorithms and classify network packets according to their behavioral characteristics [1]. The system implements a multi-layered approach to server protection, which includes three main stages: initial data filtering, statistical analysis, and the use of machine learning models. At the first stage, malicious packets are excluded based on simple criteria, such as forbidden IP addresses and incorrect packet formats.[2] In Phase 2, statistical analysis is used to detect deviations in the traffic distribution, for example, a sharp increase in the number of requests or a change in packet size [3]. The third stage involves the use of classifiers trained with historical data to identify anomalies in network operation. The list of presented models allows you to adapt to new types of attacks by automatically updating [4]. The advantages of the presented system are: It detects both traditional DDoS attacks (port scans, exploits of network protocol vulnerabilities, and SQL injection attempts) and other types of threats. Second, integration with existing monitoring tools and firewalls. Integration with existing monitoring tools and firewalls [5] also

Communication Technologies, Kyiv, Ukraine

makes it easy to implement without significant cost increases. The system is characterized by high attack detection accuracy, low false positive rate. It provides efficient real-time server protection to ensure business continuity and prevent financial and reputation loss.

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

Поночовний Петро Михайлович, аспірант кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій, Київ, Україна.

Ponochovny Petro Mykhailovych, PhD student of department Technical system cyber security of the State University of Information and Communication Technologies, Kyiv, Ukraine.

E-mail: petja9186@gmail.com

ORCID ID 0009-0008-6480-6990

Пепа Юрій Володимирович, к.т.н., доцент, професор кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій, Київ, Україн.а

Pepa Yuriy Volodymyrovych, Ph.D., docent, professor of department Technical system cyber security of the State University of Information and

E-mail: yurka14@ukr.net.

ORCID ID 0000-0003-2073-1364

УДК 004.056.5

СИСТЕМНИЙ ПІДХІД ДО БЕЗПЕКИ ВЕБДОДАТКІВ: АНАЛІЗ ЗАГРОЗ ТА МЕТОДИ КІБЕРЗАХИСТУ

Анна Ільєнко, Денис Спис, Лілія Галата, Олена Дубчак

Дослідження присвячене аналізу поширених вразливостей вебдодатків, їх впливу на безпеку інформаційних систем, економічні, репутаційні та правові наслідки, а також методи їх виявлення та усунення. Проведено всебічний огляд сучасного стану безпеки вебдодатків, включаючи статистичні дані щодо актуальних загроз, аналіз тенденцій розвитку атак та розгляд найвідоміших інцидентів останніх років. Особливу увагу приділено порівнянню різних підходів до класифікації вразливостей, зокрема OWASP Top 10, CWE Top 25, MITRE ATT&CK, NIST SP 800-53 та інших стандартів, з метою оцінки їх ефективності та практичного застосування. У роботі розглянуто методи тестування безпеки вебдодатків, зокрема статичний (SAST), динамічний (DAST) та інтерактивний аналіз (IAST), а також можливості застосування штучного інтелекту та машинного навчання (AI/ML) для автоматизованого виявлення загроз. Досліджено переваги та недоліки різних методів кіберзахисту, а також практичні аспекти їх використання у реальних умовах. Крім того, проведено детальний аналіз впливу вразливостей на організації, зокрема їх економічні наслідки, репутаційні ризики, а також правові наслідки. Результати дослідження дозволяють сформувати комплексний підхід до мінімізації ризиків, що включає впровадження передових методів аналізу безпеки, використання рекомендацій міжнародних стандартів та застосування сучасних інструментів кіберзахисту. Це забезпечує ефективніше виявлення та усунення загроз на ранніх етапах розробки та експлуатації вебдодатків.

***Ключові слова**: кібербезпека, вразливості вебдодатків, OWASP Top 10, статичний аналіз коду, динамічний аналіз, машинне навчання, автоматизоване виявлення вразливостей, кіберзагрози.*