https://doi.org/10.31891/2307-5732-2026-365-64
УДК 004.056

МУЛЯР ІГОР
Хмельницький національний університет
http://orcid.org/0000-0002-6659-605X
e-mail: muliariv@khmnu.edu.ua
АНІКІН ВОЛОДИМИР
Хмельницький національний університет
https://orcid.org/0000-0003-3395-2764
e-mail: anikin_volodymyr@khmnu.edu.ua
ДИКА ВІКТОРІЯ
Хмельницький національний університет
https://orcid.org/0009-0002-6142-9196
e-mail: dikaviktoria48@gmail.com

МЕТОД ПРОТИДІЇ ЯВНИМ ТА ПРИХОВАНИМ АТАКАМ НА ВЕБЗАСТОСУНКИ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ АНАЛІЗУ ТРАФІКУ

У статті запропоновано метод протидії атакам на вебзастосунки, який базується на використанні інтелектуальної системи аналізу трафіку. Сучасні вебзастосунки стикаються з численними загрозами, серед яких найбільш поширеними є атаки типу SQL-ін'єкцій, кроссайт-скриптинг (XSS), а також розподілені атаки типу відмови в обслуговуванні (DDoS), які можуть застосовуватись як у явному вигляді, так і з застосуванням методів обфускації, стеганографічної, або криптографічної модифікації. У зв'язку з цим, важливість своєчасного виявлення таких атак та ефективного їхнього блокування є критичною для функціонування комплексних систем захисту інформації (КСЗІ).

Метод, запропонований у цій статті, ґрунтується на використанні інтелектуальних алгоритмів аналізу трафіку, зокрема машинного навчання та алгоритмів штучного інтелекту, для детекції аномалій та визначення можливих загроз у реальному часі. Особливістю даного підходу є здатність системи автоматично навчатися та адаптуватися до нових типів атак, що з'являються внаслідок постійних змін у технологічних підходах до здійснення злочинних дій.

Ключові слова: *вебзастосунки, безпека, машинне навчання, аналіз трафіку, комплексні системи захисту інформації, адаптація алгоритмів, кластеризація, криптографія, стеганографія.*

MULIAR IHOR, ANIKIN VOLODYMYR, DYKA VIKTORIIA
Khmelnitsky national university

A METHOD FOR COUNTERING OBVIOUS AND HIDDEN ATTACKS ON WEB APPLICATIONS USING AN INTELLIGENT TRAFFIC ANALYSIS SYSTEM

The article proposes a method for countering attacks on web applications, which is based on the use of an intelligent traffic analysis system. Modern web applications face numerous threats, among the most common of which are SQL injection attacks, cross-site scripting (XSS), and distributed denial-of-service attacks (DDoS), which can be used both explicitly and using obfuscation, steganographic, or cryptographic modification methods. In this regard, the importance of timely detection of such attacks and their effective blocking is critical for the functioning of comprehensive information protection systems.

Attention is paid to developing methods for adapting intelligent systems to new, previously unknown attacks that arise as a result of the evolution of hacking techniques. Given the limitations of standard comprehensive information security systems, this research aims to create an effective, adaptive, and scalable mechanism for protecting web applications, capable of ensuring a high level of security in a dynamically changing information environment. The method proposed in this article relies on the use of intelligent algorithms for traffic analysis, particularly machine learning and artificial intelligence algorithms, to detect anomalies and identify potential threats in real time. A key feature of this approach is the system's ability to automatically learn and adapt to new types of attacks that emerge as a result of constant changes in technological approaches to carrying out malicious activities.

The results confirm that the use of intelligent network traffic analysis systems is an effective approach to strengthening web application security. Such systems demonstrate the ability not only to identify known malicious patterns, but also to adapt to detecting new, previously unknown attack vectors. At the same time, there are still some big problems that need to be solved. You need a lot of computing power to handle massive data flows, minimize false positives, and regularly retrain models to keep threat detection rates high. Integrating machine learning models with SIEM systems will enable automated threat detection and response, improving incident response times.

Keywords: *web applications, security, machine learning, traffic analysis, comprehensive information protection systems, algorithm adaptation, clustering, cryptography, steganography.*

Стаття надійшла до редакції / Received 16.03.2026
Прийнята до друку / Accepted 16.04.2026
Опубліковано / Published 28.05.2026

Постановка проблеми

З розвитком цифрових технологій та масовим впровадженням вебзастосунків в усіх сферах діяльності, від електронної комерції до фінансових сервісів і державних послуг, безпека цих систем стала одним з найважливіших аспектів захисту інформації та інфраструктури [1, 2]. Вебзастосунки обробляють величезні обсяги чутливої інформації, і навіть незначні вразливості можуть стати об'єктом атак, що загрожують не тільки бізнесу, але й загальному довірі до цифрових технологій.

Загрози для вебзастосунків стають все більш складними та різноманітними. Найпоширенішими типами атак є SQL-ін'єкції, кроссайт-скриптинг (XSS), міжсайтові атаки (CSRF), а також атаки типу відмови в

обслуговуванні (DDoS) [3, 4]. Крім того, з'являються нові методи злому, які використовують недоліки в архітектурі вебзастосунків або у взаємодії між клієнтом і сервером. Ці атаки можуть призводити до серйозних наслідків, таких як витік персональних даних, блокування доступу до послуг, порушення конфіденційності, фінансові втрати, а також ураження репутації компанії або організації.

Традиційні методи захисту, що базуються на сигнатурах атак або простих правилах виявлення вторгнень (IDS/IPS), часто не здатні виявляти нові або невідомі загрози. Стандартні фаєрволи, антивірусні програми та механізми фільтрації можуть бути ефективними для боротьби з відомими типами атак, однак не здатні справлятися з новими, складними або адаптивними методами злому [5]. Наприклад, атаки, які використовують невідомі вразливості в програмному забезпеченні або специфічні стратегії соціальної інженерії, можуть бути пропущені стандартними засобами захисту.

Особливої уваги заслуговують приклади атак, де корисне навантаження передається не в явному, а в певному замаскованому вигляді. Найбільш поширеним прикладом цього є використання різноманітних засобів обфускації, зокрема, з елементами криптографії, стеганографії, кодових перетворень тощо. Складність протидії таким атакам полягає в тому що аналіз корисного навантаження в них або унеможливлюється або суттєво ускладнюється, із суттєвим зростанням обчислювальних потужностей систем захисту. Найпростішим прикладом таких перетворень є кодування корисного навантаження SQL або JS у відповідних ін'єкційних атаках. Такі перетворення «розмиють» патерни корисного навантаження, проте все ще будуть коректно розпізнаватись та інтерпретуватись сервером. У більш складних сценаріях атаки можуть застосовуватись і безпосередньо криптографічні перетворення, як правило на рівні окремих використаних модулів ресурсу або прикладних протоколів.

У цьому контексті виникає необхідність у впровадженні в КСЗІ інтелектуальних систем, здатних адаптуватися до нових типів загроз і на основі аналізу трафіку у реальному часі виявляти аномалії, що свідчать про потенційні атаки [6]. Одним із таких підходів є застосування технологій машинного навчання та штучного інтелекту для аналізу трафіку вебзастосунків. Алгоритми штучного інтелекту можуть вивчати звичні патерни поведінки користувачів та автоматично виявляти аномалії, які можуть вказувати на спроби атаки, навіть якщо вони мають нові або модифіковані форми. Системи самонавчання дозволяють адаптуватися до змін у характері трафіку і постійно покращувати ефективність виявлення загроз без необхідності оновлювати сигнатури.

Аналіз трафіку на основі штучного інтелекту також дозволяє не лише виявляти та блокувати атаки, але й здійснювати попереджувальні заходи, надаючи організаціям можливість своєчасно реагувати на загрози [7]. Такий підхід забезпечує більш високий рівень захисту, порівняно з традиційними методами, що зазвичай працюють за принципом детекції на основі сигнатур.

Основною проблемою залишається здатність інтелектуальних систем виявляти нові, раніше невідомі атаки, при цьому мінімізуючи ймовірність помилкових спрацьовувань (false positives) [8]. Крім того, такі системи потребують значних обчислювальних ресурсів, що може бути обмеженням для організацій з обмеженим бюджетом. Ще однією проблемою є потреба у великій кількості високоякісних даних для тренування моделей машинного навчання, що вимагає значних затрат часу та ресурсів на збір, очищення та аналіз даних.

Отже, постає проблема розробки ефективних методів виявлення та протидії атакам КСЗІ, та їх вебзастосунки, які будуть здатні вчасно реагувати на нові загрози і адаптуватися до змін у тактиках зловмисників, при цьому зберігаючи високу ефективність і низьку ймовірність помилкових спрацьовувань [5, 6]. Вирішення цієї проблеми потребує використання передових технологій аналізу трафіку, а також інтеграції у КСЗІ інтелектуальних систем для забезпечення проактивного захисту.

Аналіз останніх джерел

Актуальність проблеми забезпечення безпеки вебзастосунків у світі, що швидко розвивається, визначається постійним збільшенням кількості та складності атак, спрямованих на ці системи. Протягом останніх кількох років значно зросла роль інтелектуальних систем, зокрема, машинного навчання та штучного інтелекту, у забезпеченні безпеки вебзастосунків, оскільки традиційні методи, засновані на сигнатурах атак або простих правилах, вже не можуть ефективно протистояти новим, невідомим або модифікованим загрозам. У зв'язку з цим наукові дослідження останніх років значно розширили наші знання щодо застосування цих технологій для аналізу трафіку вебзастосунків та виявлення аномалій, що вказують на атаки [1, 8].

Дослідження в галузі інтелектуальних систем виявлення аномалій для забезпечення безпеки вебзастосунків зосереджуються на використанні технологій машинного навчання для виявлення атак в реальному часі. Однією з основних задач є розробка методів, які здатні аналізувати великі обсяги трафіку та виділяти аномальні патерни, що свідчать про спроби атаки. Такі методи базуються на здатності систем до самонавчання, що дозволяє адаптувати алгоритми до нових типів атак. Останні роботи, такі як дослідження Tantithamthavorn et al. (2020) та Pham et al. (2021), підкреслюють успішне застосування глибинних нейронних мереж для аналізу вебтрафіку та виявлення різноманітних загроз, прихованої стеганографічної інформації, SQL-ін'єкцій, XSS, DDoS-атаки та багато інших. Алгоритми машинного навчання дозволяють системам не лише ефективно виявляти відомі загрози, але й адаптуватися до нових методів атак, що з'являються через еволюцію технік злому [4].

Водночас великої уваги в наукових дослідженнях набуває проблема моделювання «нормального» трафіку, що є основою для подальшого виявлення аномалій. Моделювання трафіку є важливою складовою систем виявлення аномалій, оскільки дозволяє побудувати так звану «нормальну» модель поведінки користувачів та їх взаємодії з вебзастосунками. У своїх роботах Zhang et al. (2021) і Zhou et al. (2022) автори пропонують нові

підходи до побудови таких моделей з використанням глибоких нейронних мереж та ансамблевих методів. Це дає змогу значно підвищити точність виявлення аномалій і зменшити кількість помилкових спрацьовувань, що є важливою проблемою для систем, що працюють у реальному часі [5, 6].

Іншим важливим аспектом є застосування алгоритмів класифікації для детекції конкретних типів атак. У своїх дослідженнях Sharma et al. (2023) і Zhou et al. (2022) підкреслюють важливість комбінування різних методів класифікації, таких як методи підтримки векторів (SVM), дерева рішень і глибоке навчання, для ефективного виявлення атак. Ці алгоритми дозволяють визначати характер атак, що постійно змінюються, а також адаптуватися до нових технік злому, що, у свою чергу, підвищує рівень захисту вебзастосунків [7].

Значною проблемою, яка виникає при застосуванні у КСЗІ інтелектуальних систем для захисту вебзастосунків, є питання адаптації до нових атак, що постійно з'являються. Інтелектуальні системи повинні бути здатні самостійно навчатися і покращувати свою ефективність на основі нових даних. Це дає змогу системам постійно адаптуватися до нових загроз, що з’являються в результаті еволюції атакуючих стратегій. Проблема адаптації стала темою численних досліджень, таких як роботи Bakar et al. (2021) та Kumar et al. (2022), які висвітлюють способи інтеграції адаптивних алгоритмів, що забезпечують швидку реакцію на нові або модифіковані атаки, а також знижують кількість помилкових спрацьовувань [9, 10].

Таким чином, аналіз останніх джерел свідчить про те, що впровадження інтелектуальних систем для аналізу трафіку є ефективним методом підвищення безпеки вебзастосунків. Ці системи здатні не лише виявляти відомі загрози, а й адаптуватися до нових типів атак, що з’являються. Однак існують значні виклики, такі як проблема обчислювальних ресурсів для великих обсягів даних, зменшення кількості помилкових спрацьовувань та необхідність постійного оновлення моделей для підтримки високої ефективності. Це потребує подальших досліджень і вдосконалення існуючих підходів [11, 12].

Формулювання цілей

Метою даного дослідження є розробка методів і підходів для забезпечення ефективної протидії атакам на вебзастосунки за допомогою інтелектуальних систем аналізу трафіку. Основною задачею є створення адаптивної системи, здатної виявляти нові типи атак, зокрема, в умовах криптографічної та стеганографічної протидії виявленню, а також швидко реагувати на них, використовуючи алгоритми машинного навчання та штучного інтелекту для аналізу аномалій у мережевому трафіку. Зокрема, дослідження спрямоване на розробку моделей, які дозволяють ідентифікувати атаки на основі поведінкових патернів користувачів КСЗІ, а також визначати відхилення від звичайного трафіку, що може свідчити про потенційні загрози [1].

Крім того, одним з основних завдань є вдосконалення існуючих підходів до класифікації атак і зниження рівня помилкових спрацьовувань у системах виявлення вторгнень. Важливим аспектом є розробка методів адаптації інтелектуальної системи до нових, раніше невідомих атак, що виникають в результаті еволюції технік злому. Враховуючи обмеження стандартних КСЗІ, це дослідження має на меті створити ефективний, адаптивний та масштабований механізм для захисту вебзастосунків, здатний забезпечити високий рівень безпеки в умовах динамічно змінюваного інформаційного середовища [6, 7].

Виклад основного матеріалу

Алгоритм Support Vector Machines (SVM)

Один з найбільш потужних інструментів для класифікації і виявлення аномалій у мережевому трафіку є алгоритм Support Vector Machines (SVM) [13]. Алгоритм SVM здобув популярність завдяки своїй здатності ефективно працювати з великими та високорозмірними наборами даних, що робить його особливо корисним для виявлення атак на вебзастосунки, де трафік може містити складні, багатофункціональні патерни [14].

SVM є методом нагляданого навчання, тобто він вимагає попередньо позначених даних для навчання моделі. Основним завданням алгоритму є побудова гіперплощини, яка максимально розділяє різні класи даних, наприклад, нормальний трафік та атакуючий [15]. Застосовуючи цей підхід до аналізу вебтрафіку, можна створити систему, яка ефективно виявляє аномалії та потенційні загрози. На рис. 1 зображено принцип роботи методу підтримувальних векторів:

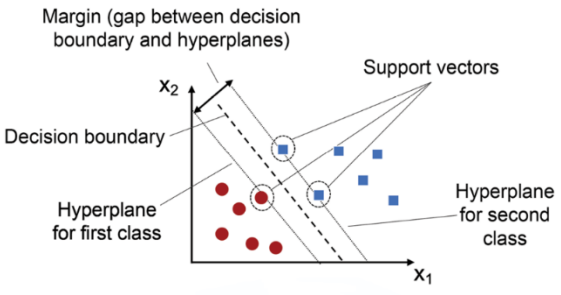

Рис. 1. Принцип роботи методу SVM

Алгоритм Support Vector Machines базується на концепції гіперплощини, що розділяє два класи даних, при цьому намагається знайти таку гіперплощину, яка має максимальний марж — відстань між найближчими точками різних класів (вони називаються опорними векторами) [16]. Математично це можна описати таким чином:

$$f(x) = wTx + b = 0, \#(1)$$

Згідно з формулою (1), алгоритм намагається знайти такі параметри w і b, які забезпечують максимальний розподіл (марж) між двома класами. Іншими словами, SVM мінімізує кількість помилкових класифікацій, знаходячи рівновагу між точністю моделі та її узагальнюючою здатністю [17].

У контексті аналізу мережевого трафіку ця гіперплощина виконує роль кордону між нормальними та підозрілими запитами. Кожен новий запит, який надходить до вебзастосунку, представлений як вектор ознак x, і далі перевіряється знаком функції f(x): якщо f(x) > 0, запит класифікується як нормальний, а якщо f(x) < 0, то система розпізнає його як потенційно атакуючий.

Таким чином, алгоритм формує адаптивну межу між звичайною поведінкою користувачів і підозрілою активністю. Якщо модель налаштована коректно, вона може успішно виявляти навіть нові, раніше невідомі типи атак, оскільки базується не на сигнатурах, а на поведінкових закономірностях у даних.

Для використання алгоритму SVM у задачах виявлення атак на вебзастосунки необхідно підготувати відповідну вибірку даних. Кожен HTTP-запит або сесія, що надходить на вебзастосунок, розглядається як вектор ознак, що містить важливу інформацію про запит. До таких ознак можуть входити тип HTTP-запиту (GET, POST, PUT, DELETE), часовий параметр (час між запитами), розмір запиту, наявність підозрілих символів (наприклад, для SQL ін'єкцій або XSS атак), а також частота запитів, що дозволяє виявляти брутфорс-атаки.

Ці ознаки формують вектор, який є основою для тренування моделі SVM. Використання різноманітних характеристик запиту дозволяє алгоритму навчатися розрізняти нормальний трафік і атакуючий, забезпечуючи тим самим високу точність класифікації.

Ключовим етапом є навчання моделі SVM. Під час цього етапу алгоритм використовує позначені дані для оптимізації параметрів w та b. Процес навчання спрямований на мінімізацію помилок класифікації, при цьому важливим є правильний вибір ядра та налаштування гіперпараметрів.

Для навчання моделі необхідно вибрати ядро, яке буде визначати, як перетворюються дані у просторі більшої розмірності. Найпоширенішими є лінійне ядро, яке підходить для лінійно роздільних даних, і радіально-базисне ядро (RBF), яке дозволяє працювати з даними з нелінійними залежностями. Після вибору ядра важливо оптимізувати гіперпараметри, такі як коефіцієнт регуляризації C та параметр ядра γ, що значно впливає на точність моделі.

Навчена модель тестується на незалежних даних, що дозволяє оцінити її здатність правильно класифікувати нові, невідомі запити, а також її ефективність у виявленні атак.

Перевагами даного методу є також те, що навіть застосування різноманітних методів обфускації корисного навантаження, з великою долею ймовірності буде виявлено як підозріле, оскільки саме по собі буде аномальним, по відношенню до звичного трафіку, подібного тому, на якому проводилось навчання моделі.

Однією з головних переваг алгоритму SVM є його висока точність. Алгоритм здатний ефективно розрізняти нормальний та атакуючий трафік, мінімізуючи помилки класифікації. Це дозволяє точно виявляти навіть нові та раніше невідомі типи атак. Іншою важливою перевагою є адаптивність моделі, оскільки SVM працює з патернами поведінки трафіку, що дозволяє йому адаптуватися до нових типів атак без необхідності створення нових сигнатур.

Метод адаптивного управління ресурсами

Алгоритм K-Nearest Neighbors (KNN) є одним із найбільш популярних методів класифікації та виявлення аномалій у мережевому трафіку. Завдяки своїй простоті та здатності адаптуватися до нових даних, цей алгоритм широко застосовується для виявлення атак на вебзастосунки та в інших сферах кібербезпеки. KNN є методом навчання без вчителя, що дає йому значну гнучкість у виявленні нових типів атак без необхідності попереднього навчання на сигнатурах.

Принцип роботи алгоритму KNN полягає в тому, що кожен новий об'єкт класифікується на основі його схожості з уже існуючими об'єктами навчальної вибірки. Для цього алгоритм обчислює відстань між новим запитом та всіма іншими об'єктами в наборі даних, після чого вибирає K найближчих сусідів. Класифікація нового запиту здійснюється на основі більшості класу серед найближчих сусідів [18]. Вибір метрики відстані (найпоширеніша — евклідова відстань) є важливим етапом, оскільки від цього залежить точність класифікації. Евклідова відстань між двома об'єктамиxx iyy, що представлені векторами ознак, обчислюється за формулою:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}, \#(2)$$

Згідно з формулою (2), чим менше значення d(x,y) d(x,y), тим ближчими є об’єкти за своїми характеристиками, а отже, більша ймовірність того, що вони належать до одного класу. Таким чином, модель KNN оцінює подібність нових запитів до вже відомих зразків поведінки, визначаючи, чи є запит нормальним або потенційно шкідливим.

Алгоритм KNN можна застосувати до задач виявлення атак на вебзастосунки, де важливими є аномальні патерни поведінки користувачів. Кожен запит або сесія на вебсайті може бути представлений вектором ознак, що включає різні характеристики, такі як тип HTTP-запиту, розмір запиту, наявність підозрілих символів (для SQL-ін’єкцій або XSS-атак), частоту запитів, час між запитами тощо [19]. Завдяки цьому KNN може

класифікувати нові запити, порівнюючи їх із уже відомими патернами трафіку. Наприклад, брутфорс-атаки можуть бути виявлені через велику кількість запитів від одного джерела за короткий період, тоді як SQL-ін'єкції або XSS можуть бути розпізнані за наявністю специфічних символів у запитах. На рис. 2 зображено процес навчання моделі для класифікації даних в двовимірному просторі з використанням машинного навчання.

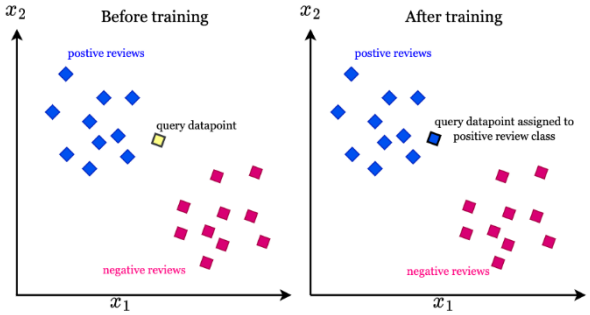

Рис. 2. Класифікація за допомогою алгоритму KNN

Однією з головних переваг KNN є його адаптивність. Алгоритм може ефективно працювати з новими типами атак, оскільки він не покладається на заздалегідь визначені сигнатури, а працює з поведінковими патернами. Це дозволяє йому виявляти навіть ті загрози, які раніше не були відомі, що робить його корисним для боротьби з новими або невідомими атаками.

Проте алгоритм має й певні недоліки. Одним із них є висока обчислювальна складність, оскільки для кожного нового запиту необхідно обчислювати відстань до кожного елемента в навчальній вибірці. Це може бути проблемою для великих наборів даних. Крім того, правильний вибір параметра K (кількості сусідів) має вирішальне значення для ефективності класифікації. Занадто маленьке значення K може призвести до чутливості до шуму, а надто велике — до погіршення точності класифікації. Алгоритм також може бути чутливим до помилок у даних, оскільки будь-який неправильний або зашумлений об'єкт може вплинути на результат.

Важливою умовою коректної роботи даного методу є його коректна інтеграція в вебінфраструктуру. Найбільш якісні результати даний метод досягає тоді, коли трафік аналізується не на проміжних ланках, по типу маршрутизаторів, чи проксі, де трафік, як правило, повністю шифрований, оскільки передається за допомогою захищених протоколів, таких як HTTPS, WSS тощо, а безпосередньо на стороні вебсервера, або у внутрішній приватній мережі вебінфраструктури, де подібного шифрування вже немає і аналізу піддаються справжні параметри трафіку, а не шифровані високоентропійні пакети.

Попри ці недоліки, KNN є потужним інструментом для виявлення атак у мережевому трафіку, особливо коли потрібно ідентифікувати нові чи невідомі загрози. Його застосування є ефективним у системах, де важливо виявляти аномальні поведінкові патерни, і коли не існує чітких сигнатур для атак. Таким чином, алгоритм KNN забезпечує адаптивний підхід до класифікації, що підвищує точність виявлення атак у сучасних вебсистемах.

Обґрунтування наукових результатів

Результати проведеного дослідження демонструють значні переваги застосування алгоритмів Support Vector Machines (SVM) та K-Nearest Neighbors (KNN) в порівнянні з традиційними статистичними методами для виявлення атак на вебзастосунки. Основною проблемою традиційних статистичних підходів є їх обмежена здатність до адаптації, що робить ці методи менш ефективними при виявленні нових та складних типів атак. На противагу цьому, алгоритми SVM та KNN здатні обробляти великі та високорозмірні набори даних, що дозволяє їм забезпечити більш точну і ефективну класифікацію трафіку в умовах змінної загрози.

Традиційні статистичні методи виявлення атак зазвичай ґрунтуються на визначених порогах для ключових параметрів мережевого трафіку, таких як кількість запитів за певний період часу, розмір запиту або частота повторних запитів. Вони працюють шляхом виявлення аномалій, якщо значення певного параметра перевищує або не досягає встановленого порогу. Однак ці методи мають кілька суттєвих недоліків. По-перше, вони зазвичай здатні ефективно працювати лише в простих випадках, таких як виявлення брутфорс-атак або SQL-ін'єкцій, де можна чітко визначити аномальні значення. Однак для більш складних і невідомих атакз використанням методів стеганографії, обфускації, криптогафії традиційні методи виявлення, як правило, виявляються неефективними, оскільки вони не здатні адаптуватися до нових патернів атак, що виникають. Таким чином, ці методи залишають системи уразливими до нових загроз, що постійно з'являються.

Алгоритми SVM і KNN відрізняються від традиційних статистичних методів здатністю враховувати багатовимірні патерни в поведінці мережевого трафіку. SVM використовує гіперплощину для максимального розмежування класів, що дозволяє ефективно розрізняти нормальний і атакуючий трафік, навіть з нелінійними закономірностями. KNN класифікує нові запити за схожістю з найближчими елементами в навчальній вибірці, що допомагає виявляти аномалії.На відміну від традиційних методів, які зазвичай реактивні та потребують оновлення після виявлення атаки, SVM і KNN можуть адаптуватися в реальному часі, що дозволяє їм своєчасно виявляти нові аномалії та змінювати стратегію класифікації. Це робить ці алгоритми більш ефективними для виявлення нових типів атак.

Сама концепція пошуку аномалій дистанціюється від конкретики в аналізі трафіку, спрямованої на виявлення конкретної атаки, натомість вона оперує абстрактними поняттями подібності чи неподібності конкретного трафіку до «звичного». Це, в свою чергу, робить подібні методи виявлення більш дієвими до виявлення замаскованих атак, оскільки, як приклад, той чи інший шифрований чи замаскований блок даних в заголовках чи тілі запиту, сам по собі буде аномальним, за умови що раніше на його місці були якісь прості осмислені параметри, без необхідності проводити криптографічний чи стеганографічний аналіз самого блоку.

Для перевірки ефективності зазначених підходів було проведено серію експериментів, де порівняно алгоритми SVM і KNN з традиційними статистичними методами на реальних наборах даних мережевого трафіку. Результати показали, що обидва алгоритми продемонстрували значно вищу точність класифікації, зокрема зменшили кількість помилкових спрацьовувань і покращили здатність виявляти нові типи атак. Це підтверджує, що методи машинного навчання є більш надійними інструментами в порівнянні з традиційними статистичними підходами, оскільки вони не залежать від чітко визначених порогів або фіксованих правил класифікації, а здатні адаптуватися до змінних умов атак. На рис. 3 зображено результати моделювання порівняння лінійної регресії та KNN-регресії на вибірці даних.

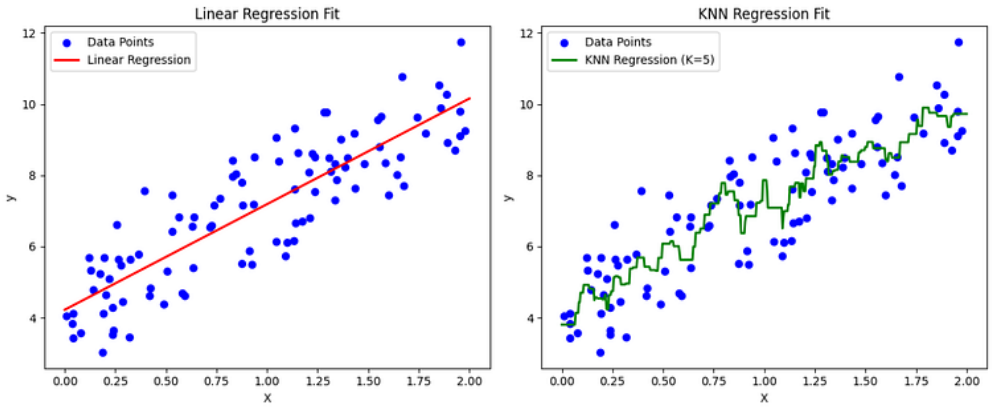

Рис. 3. Порівняння Linear Regression та K-Nearest Neighbors

Порівнюючи час реакції на нові атаки, було виявлено, що алгоритми SVM та KNN швидше пристосовуються до нових типів загроз, ніж статистичні методи. Традиційні методи зазвичай не можуть реагувати на нові атаки, поки вони не потрапляють до зібраних баз даних або не оновлюються вручну, що створює потенційні вікна для зловмисників. В той же час, SVM та KNN адаптуються до нових загроз, використовуючи принципи самонавчання, що дозволяє знижувати ймовірність пропуску атак.

Важливим аспектом є також здатність обох методів до обробки великих обсягів даних. Статистичні методи часто стикаються з проблемами при роботі з великими наборами даних, особливо коли трафік вебзастосунків надто великий і складний для обробки за допомогою фіксованих порогів або статистичних показників. Алгоритми SVM та KNN, на відміну від традиційних методів, добре справляються з високорозмірними даними, що дає їм значну перевагу при обробці великих наборів мережевого трафіку.

Загалом, результати дослідження підтверджують, що алгоритми SVM і KNN значно перевищують традиційні статистичні методи за точністю класифікації, здатністю адаптуватися до нових загроз і обробкою великих наборів даних. Ці методи не тільки забезпечують високу ефективність виявлення атак, але й відкривають можливості для подальшого розвитку систем безпеки, що здатні реагувати на нові типи загроз в режимі реального часу.

Висновки з даного дослідження і перспективи подальшого розвитку у даному напрямку

У цьому дослідженні було досягнуто поставленої мети – розробки та теоретичного обґрунтування методів машинного навчання для виявлення атак на вебзастосунки, зокрема на основі алгоритмів SVM та KNN. Було доведено, що ці методи значно перевершують традиційні статистичні підходи за точністю та здатністю адаптуватися до нових типів загроз. Основною перевагою наших алгоритмів є їх здатність до самостійного навчання та адаптації на основі аналізу мережевого трафіку, що дозволяє виявляти навіть нові, раніше невідомі атаки, зокрема замасковані різноманітними криптографічними, стеганографічними та іншими методами, без необхідності в постійному оновленні сигнатур.

Практична значущість роботи полягає в тому, що запропоновані методи можуть бути використані для створення високоефективних систем виявлення аномалій у вебзастосунках, здатних забезпечити високий рівень захисту в КСЗІ. Розроблені алгоритми можна інтегрувати в існуючі системи безпеки, що дозволить автоматизувати процес виявлення атак та покращити здатність систем реагувати на нові типи загроз у реальному часі.

Виділено три основні напрямки для перспектив подальшого розвитку:

1. Вдосконалення інтерпретованості моделей. Розвиток технологій Explainable AI (XAI) дозволить забезпечити кращу прозорість рішень, що приймаються алгоритмами машинного навчання, що підвищить їх прийняття в реальних системах кібербезпеки;

2. Мультиджерельний аналіз даних. Об'єднання даних з різних джерел, таких як мережеві логи та

системи моніторингу загроз, дозволить підвищити точність виявлення атак та зменшити кількість хибних спрацювань;

3. Інтеграція з системами управління інцидентами безпеки (SIEM), які є складовими КСЗІ. Інтеграція моделей машинного навчання з SIEM системами дозволить автоматизувати виявлення і реагування на загрози, покращуючи швидкість реагування на інциденти.

Література

1. Лєнков С., Джулій В., Муляр І., Димбовський М. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі. *Underwater Technologies: Industrial and Civil Engineering*. 2023. Вип. 13. С. 45–59. DOI: 10.32347/uwt.2023.13.1205 (дата звернення: 07.03.2025).
2. Шулімова Д. Д., Бойко А. О., Мурзін І. В., Довженко Т. П. Алгоритмічні підходи до виявлення аномалій на основі машинного навчання. *Телекомунікаційні та інформаційні технології.* 2025. Вип. 2. С. 126-133. DOI: 10.31673/2412-4338.2025.026117 (дата звернення: 07.03.2025).
3. Srinivasan P. AI-Based Detection of Abnormal Traffic Patterns in Web Applications. *International Journal of Emerging Research in Engineering and Technology*. 2025. Vol. 28, no 2. P. 94-101. DOI: 10.63282/3050-922X.ICRCEDA25-112 (дата звернення: 07.03.2025).
4. Іванченко Є. В., Берестяна Т.В. Аналіз ефективності моделей машинного навчання для прогнозування кібератак у корпоративній мережі. Науково-практична конференція «Актуальні проблеми інформаційно-комунікаційних систем»: збірник тез всеукраїнської науково-практичної конференції. Київ. 5 лист. 2025 р. С. 59-65.
5. Bakhshi T., Ghita B. Anomaly Detection in Encrypted Internet Traffic Using Hybrid Deep Learning. *Security and Communication Networks*. 2021. Vol. 1. DOI: 10.1155/2021/5363750 (дата звернення: 07.03.2025).
6. Поліщук В. А. Розробка системи виявлення вторгнень на основі аналізу аномалій у мережевому трафіку з використанням машинного навчання : робота на здобуття кваліфікаційного ступеня магістра: спец. 125 - Кібербезпека та захист інформації / наук. кер. М. А. Стадник. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 82 с.
7. Talpur A., Gurusamy M. Machine Learning for Security in Vehicular Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2022. Vol. 24, no. 1. P. 346–379. URL: https://doi.org/10.1109/comst.2021.3129079 (date of access: 12.03.2026).
8. Skip A., Baryshev Y. SOFTWARE SUPPLY CHAIN SECURITY ANALYSIS. Cybersecurity: Education, Science, Technique. 2025. Vol. 1, no. 29. P. 263–273. URL: https://doi.org/10.28925/2663-4023.2025.29.820 (date of access: 12.03.2026).
9. Ahmed A. A., Agunsoye G. A Real-Time Network Traffic Classifier for Online Applications Using Machine Learning. Algorithms. 2021. Vol. 14, no. 8. P. 250. URL: https://doi.org/10.3390/a14080250 (date of access: 12.03.2026).
10. Федюшин І. О. та ін. Виявлення аномалій у мережевому трафіку веб-додатків з використанням алгоритму random forest. *Вісник Херсонського національного технічного університету*. 2025. Т. 3, № 4. С. 269–275. DOI: 10.35546/kntu2078-4481.2025.4.3.31 (дата звернення: 12.03.2026).
11. Okoli U. I. et al. Machine learning in cybersecurity: a review of threat detection and defense mechanisms. *World journal of advanced research and reviews*. 2024. Vol. 21, no. 1. P. 2286–2295. DOI: 10.30574/wjarr.2024.21.1.0315 (date of access: 12.03.2026).
12. Zhuravchak A., Piskozub A. Analysis of machine learning methods for automating penetration testing. Cybersecurity: Education, Science, Technique. 2025. Vol. 3, no. 27. P. 54–62. URL: https://doi.org/10.28925/2663-4023.2025.27.711 (date of access: 12.03.2026).
13. Shaochen Ren, Shiyang Chen, Qun Zhang. Reinforcement Learning Paradigms for Proactive Cybersecurity and Dynamic Risk Management. Frontiers in Artificial Intelligence Research. 2025. Vol. 2, no. 3. P. 436–456. URL: https://doi.org/10.71465/fair417 (date of access: 12.03.2026).
14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors. 2024. Vol. 24, no. 15. P. 4888. URL: https://doi.org/10.3390/s24154888 (date of access: 12.03.2026).
15. Olateju O. O. et al. Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud Asian Journal of Research in Computer Science. 2024. Vol. 17, no. 6. P. 264–292. DOI: 10.9734/ajrcos/2024/v17i6472 (date of access: 12.03.2026).
16. Mulyar I. et al. A method for finding web application vulnerabilities using the ChatGPT API. Smart technologies: Industrial and Civil Engineering. 2024. Vol. 2, no. 15. P. 46–55. URL: https://doi.org/10.32347/st.2024.2.1203 (date of access: 12.03.2026).
17. Петляк Н. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. Measuring and computing devices in technological processes. 2025. № 1. С. 180–186. DOI: 10.31891/2219-9365-2025-81-21 (дата звернення: 12.03.2026).
18. Sobolenko I., Platonenko A. Automated detection of anomalies in corporate wireless network traffic using python: methods, implementation, and effectiveness evaluation. *Cybersecurity: Education, Science, Technique*.

2025. Vol. 1, no. 29. DOI: 10.28925/2663-4023.2025.29.939 (date of access: 12.03.2026).

19. Stetsiuk M., Anikin V., Pyrch O., Kozelskiy O., Salem A.-B.M. Method of detecting anomalies in IOT device traffic based on statistical analysis using the modified z score. *Ceur Workshop Proceedings: Conference paper*. 2025.

References

1. Lienkov S., Dzhulii V., Muliar I., Dymbovskyi M. Model vyznachennia aktualnykh zahroz bezpeky konfidentsiinykh danykh v rozpodilenii informatsiinii systemi. Underwater Technologies: Industrial and Civil Engineering. 2023. Vyp. 13. S. 45–59. DOI: 10.32347/uwt.2023.13.1205 (data zvernennia: 07.03.2025).

2. Shulimova D. D., Boiko A. O., Murzin I. V., Dovzhenko T. P. Alhorytmichni pidkhody do vyiavlennia anomalii na osnovi mashynnoho navchannia. Telekomunikatsiini ta informatsiini tekhnolohii. 2025. Vyp. 2. S. 126-133. DOI: 10.31673/2412-4338.2025.026117 (data zvernennia: 07.03.2025).

3. Srinivasan P. AI-Based Detection of Abnormal Traffic Patterns in Web Applications. International Journal of Emerging Research in Engineering and Technology. 2025. Vol. 28, no 2. P. 94-101. DOI: 10.63282/3050-922X.ICRCEDA25-112 (data zvernennia: 07.03.2025).

4. Ivanchenko Ye. V., Berestiana T.V. Analiz efektyvnosti modelei mashynnoho navchannia dlia prohnozuvannia kiberatak u korporatyvnii merezhi. Naukovo-praktychna konferentsiia «Aktualni problemy informatsiino-komunikatsiinykh system»: zbirnyk tez vseukrainskoi naukovo-praktychnoi konferentsii. Kyiv. 5 lyst. 2025 r. S. 59-65.

5. Bakhshi T., Ghita B. Anomaly Detection in Encrypted Internet Traffic Using Hybrid Deep Learning. Security and Communication Networks. 2021. Vol. 1. DOI: 10.1155/2021/5363750 (data zvernennia: 07.03.2025).

6. Polishchuk V. A. Rozrobka systemy vyiavlennia vtorhnen na osnovi analizu anomalii u merezhevomu trafiku z vykorystanniam mashynnoho navchannia : robota na zdobuttia kvalifikatsiinoho stupenia mahistra: spets. 125 - Kiberbezpeka ta zakhyst informatsii / nauk. ker. M. A. Stadnyk. Ternopil : Ternopilskyi natsionalnyi tekhnichnyi universytet imeni Ivana Puliuia, 2024. 82 s.

7. Talpur A., Gurusamy M. Machine Learning for Security in Vehicular Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2022. Vol. 24, no. 1. P. 346–379. URL: https://doi.org/10.1109/comst.2021.3129079 (date of access: 12.03.2026).

8. Skip A., Baryshev Y. SOFTWARE SUPPLY CHAIN SECURITY ANALYSIS. Cybersecurity: Education, Science, Technique. 2025. Vol. 1, no. 29. P. 263–273. URL: https://doi.org/10.28925/2663-4023.2025.29.820 (date of access: 12.03.2026).

9. Ahmed A. A., Agunsoye G. A Real-Time Network Traffic Classifier for Online Applications Using Machine Learning. Algorithms. 2021. Vol. 14, no. 8. P. 250. URL: https://doi.org/10.3390/a14080250 (date of access: 12.03.2026).

10. Fediushyn I. O. ta in. Vyiavlennia anomalii u merezhevomu trafiku veb-dodatkiv z vykorystanniam alhorytmu random forest. Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu. 2025. T. 3, № 4. S. 269–275. DOI: 10.35546/kntu2078-4481.2025.4.3.31 (data zvernennia: 12.03.2026).

11. Okoli U. I. et al. Machine learning in cybersecurity: a review of threat detection and defense mechanisms. World journal of advanced research and reviews. 2024. Vol. 21, no. 1. P. 2286–2295. DOI: 10.30574/wjarr.2024.21.1.0315 (date of access: 12.03.2026).

12. Zhuravchak A., Piskozub A. Analysis of machine learning methods for automating penetration testing. Cybersecurity: Education, Science, Technique. 2025. Vol. 3, no. 27. P. 54–62. URL: https://doi.org/10.28925/2663-4023.2025.27.711 (date of access: 12.03.2026).

13. Shaochen Ren, Shiyang Chen, Qun Zhang. Reinforcement Learning Paradigms for Proactive Cybersecurity and Dynamic Risk Management. Frontiers in Artificial Intelligence Research. 2025. Vol. 2, no. 3. P. 436–456. URL: https://doi.org/10.71465/fair417 (date of access: 12.03.2026).

14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors. 2024. Vol. 24, no. 15. P. 4888. URL: https://doi.org/10.3390/s24154888 (date of access: 12.03.2026).

15. Olateju O. O. et al. Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud Asian Journal of Research in Computer Science. 2024. Vol. 17, no. 6. P. 264–292. DOI: 10.9734/ajrcos/2024/v17i6472 (date of access: 12.03.2026).

16. Mulyar I. et al. A method for finding web application vulnerabilities using the ChatGPT API. Smart technologies: Industrial and Civil Engineering. 2024. Vol. 2, no. 15. P. 46–55. URL: https://doi.org/10.32347/st.2024.2.1203 (date of access: 12.03.2026).

17. Petliak N. Analiz modelei vyiavlennia anomalii trafiku v suchasnykh informatsiino-komunikatsiinykh systemakh ta merezhakh. Measuring and computing devices in technological processes. 2025. № 1. S. 180–186. DOI: 10.31891/2219-9365-2025-81-21 (data zvernennia: 12.03.2026).

18. Sobolenko I., Platonenko A. Automated detection of anomalies in corporate wireless network traffic using python: methods, implementation, and effectiveness evaluation. Cybersecurity: Education, Science, Technique. 2025. Vol. 1, no. 29. DOI: 10.28925/2663-4023.2025.29.939 (date of access: 12.03.2026).

19. Stetsiuk M., Anikin V., Pyrch O., Kozelskiy O., Salem A.-B.M. Method of detecting anomalies in IOT device traffic based on statistical analysis using the modified z score. Ceur Workshop Proceedings: Conference paper. 2025.