безпечного житлового простору стає можливим на базі доступного комп'ютерного обладнання. Це відкриває нові перспективи для створення надійних та персоналізованих систем автоматизації.

Список використаних джерел:

1. Бакурова А. В., Терещенко О. В. Інтернет речей: технології та застосування : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 245 с.
2. Олійник В. В. Периферійні обчислення (Edge Computing) в системах розумного дому: переваги та виклики // Сучасні інформаційні технології та комп'ютерна інженерія. 2024. Вип. 15. С. 112–118.
3. Коваленко О. М. Архітектура розподілених систем управління на базі мікроконтролерів ESP32 та протоколу MQTT // Вісник комп'ютерних систем та мереж. 2023. № 4. С. 45–52.
4. LoRA: Low-Rank Adaptation of Large Language Models / E. J. Hu, Y. Shen, P. Wallis [та ін.] // arXiv preprint. 2021. URL: https://arxiv.org/abs/2106.09685 (дата звернення: 16.03.2026).
5. Офіційна документація платформи Home Assistant. URL: https://www.home-assistant.io/docs/ (дата звернення: 16.03.2026).

УДК 004.056.53:004.8

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

Олійник М.С.
maksres01@gmail.com
Черкаський державний фаховий бізнес-коледж
Медолиз М.М.
м. Черкаси, Україна

У сучасному середовищі інформаційних технологій динаміка розвитку кіберзагроз вимагає впровадження інтелектуальних засобів захисту. Традиційні системи виявлення вторгнень (IDS), що базуються на сигнатурному аналізі, демонструють обмежену ефективність проти атак нового типу, оскільки вони не

здатні розпізнавати аномалії, що відсутні у заздалегідь визначених базах даних. Саме тому застосування методів машинного навчання є пріоритетним напрямком, що дозволяє автоматизувати процес ідентифікації підозрілої активності на основі аналізу статистичних характеристик мережевих потоків [2].

Для побудови ефективної моделі розглядається архітектура системи, що базується на обробці великих масивів даних у режимі реального часу. Важливим етапом проектування є вибір репрезентативного набору даних для навчання. У ході дослідження проаналізовано характеристики сучасного датасету NSL-KDD, який є вдосконаленою версією KDD Cup 99 та містить записи нормальної активності та основних категорій атак, таких як відмова в обслуговуванні та несанкціоноване сканування [4]. Використання даного набору дозволяє уникнути надмірності даних, що позитивно впливає на якість навчання класифікаторів та швидкість обробки інформації модулями виявлення.

Особлива увага при реалізації системи приділяється етапу попередньої обробки та виділення найбільш інформативних ознак. Для точної ідентифікації вторгнень критично важливими визначено параметри тривалості сесії, типу протоколу та кількості помилкових пакетів [1]. Застосування методів нормалізації значень дозволяє збалансувати вплив різних ознак на кінцевий результат, що підвищує стабільність роботи алгоритмів у гетерогенних мережевих середовищах. Процес підготовки даних реалізується засобами мови програмування Python із використанням спеціалізованих бібліотек для обробки статистичної інформації.

У процесі аналізу алгоритмів машинного навчання встановлено, що використання ансамблевих методів, зокрема випадкового лісу, дозволяє досягти високої точності класифікації за рахунок побудови сукупності дерев рішень. Такий підхід суттєво знижує ризик перенавчання моделі та забезпечує надійне розпізнавання аномалій навіть у складних структурах трафіку [1]. Крім того, досліджено можливості методу опорних векторів, який демонструє високу ефективність у задачах розділення трафіку на легітимний та шкідливий за умови коректного вибору ядерної функції та параметрів регуляризації [3].

Експериментальна перевірка системи підтверджує, що обрані математичні підходи дозволяють виявляти вторгнення з точністю понад 97%. Програмна реалізація системи передбачає модульну структуру, що дозволяє інтегрувати її в існуючі комплекси моніторингу мережевої активності. Оцінка продуктивності моделі проводилася на основі метрик повноти та точності, що підтвердило здатність системи мінімізувати кількість хибнопозитивних спрацювань. Це створює умови для ефективного розгортання інтелектуальних модулів у корпоративних мережах з метою забезпечення проактивного захисту інформаційних ресурсів.

Таким чином, інтеграція методів машинного навчання в архітектуру систем захисту інформації дозволяє створити адаптивний та гнучкий механізм виявлення загроз. Запропонований підхід забезпечує стабільність функціонування мережі та автоматизує процес розпізнавання нових типів атак, що є критично важливим для сучасних систем кібербезпеки. Подальші дослідження у даному напрямку можуть бути спрямовані на вдосконалення моделей для аналізу зашифрованого трафіку та використання методів глибокого навчання для підвищення швидкодії системи в умовах високої інтенсивності передачі даних.

Список використаних джерел:

1. Бурячок В. Л., Толубко В. Б. Інформаційна та кібербезпека: соціотехнічний аспект. Київ: ДУТ, 2019. 432 с.
2. Гнатуш А. В. Методи та засоби машинного навчання в кібербезпеці: навч. посіб. Львів : Видавництво Львівської політехніки, 2022. 180 с.
3. Сучасні інтелектуальні системи захисту інформації в комп'ютерних мережах. URL: https://infosec.org.ua/intellectual-ids (дата звернення: 01.03.2026).
4. Bishop C. M. Pattern Recognition and Machine Learning. Springer, 2006. 738 p.

NSL-KDD Dataset for Network Intrusion Detection. University of New Brunswick. URL: https://www.unb.ca/cic/datasets/nsl.html (дата звернення: 08.03.2026).

УДК 004.8:004.93

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ У ВІДЕОПОТОЦІ БПЛА

Монько С.Ю.
stasmonko6@gmail.com
Черкаський державний фаховий бізнес-коледж
Швиденко А.В
м. Черкаси, Україна

У сучасних інформаційних системах важливим напрямом розвитку є автоматизований аналіз відеоданих, отриманих із безпілотних літальних апаратів (БПЛА). Такі системи застосовуються передусім у військовій сфері, а також для моніторингу територій, аналізу дорожнього руху, контролю інфраструктури, екологічного спостереження та інших прикладних задач [1].

Особливістю відеопотоку з БПЛА є висока динамічність сцени, зміна ракурсу, вплив погодних умов, коливання освітлення та наявність шумів. Це ускладнює процес розпізнавання об'єктів і вимагає використання ефективних алгоритмів комп'ютерного зору, здатних працювати в реальному часі [1, 2].

Одним із найбільш результативних підходів є використання згорткових нейронних мереж, які забезпечують автоматичне вилучення ознак із зображення та їх класифікацію. Сучасні моделі дозволяють ефективно ідентифікувати об'єкти навіть за умов складного фону та часткового перекриття [2].

Серед алгоритмів детекції об'єктів особливе місце займає сімейство моделей YOLO (You Only Look Once), що орієнтоване на обробку відеопотоку в реальному часі. Модель YOLOv8 вирізняється оптимізованою архітектурою та високою швидкодією при збереженні достатнього рівня точності [3].

Сучасна версія моделі YOLOv8 характеризується покращеною архітектурою та оптимізованими алгоритмами обробки. Архітектура моделі включає три основні компоненти (рис. 1): backbone, neck та head. Backbone