2. Васильєва Н. Б., Нижниченко Я. Є., Заболотна О. С. Вплив цифровізації на трансформацію бізнес-моделей у традиційних галузях економіки // Економічний вісник університету. – 2023. – № 47. – С. 112–119.

3. Бондаренко О. М., Стрій Л. О. Вплив сучасних digital-комунікацій на поведінку споживача // Бізнес-інформ. – 2024. – № 2. – С. 67–73.

4. Андріїв Н. М. Цифрова трансформація підприємства: теоретичний базис // Ефективна економіка. – 2022. – № 5. – Режим доступу: http://www.economy.nayka.com.ua

МАШИННЕ НАВЧАННЯ У ВИЯВЛЕННІ АНОМАЛІЙ СЕРВЕРНОЇ АКТИВНОСТІ ЯК ІНСТРУМЕНТ ЗАХИСТУ ЦИФРОВОЇ ЕКОНОМІКИ

Трофименко В. О.,
ЗВО спеціальності 122 Комп'ютерні науки
Ємельянов С. І.,
старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет

Цифрова економіка стрімко розвивається, охоплюючи критичні інфраструктури, фінансові сервіси, електронну комерцію та державне управління. Зростання кількості серверів, хмарних платформ і розподілених обчислювальних систем підвищує ризик кібератак, технічних збоїв і несанкціонованого доступу. Традиційні методи кіберзахисту, засновані на фіксованих правилах або сигнатурах, дедалі частіше виявляються недостатніми. Поява нових типів загроз і динамічність цифрового середовища вимагають інструментів, здатних адаптуватися до невідомих сценаріїв поведінки систем. У цьому контексті машинне навчання стає ключовим напрямом розвитку інтелектуальних систем моніторингу та виявлення аномалій у серверній активності.

Метою роботи є узагальнення теоретичних підходів і практичного досвіду застосування машинного навчання для виявлення аномалій у серверній активності як інструменту забезпечення кіберстійкості цифрової економіки. Завданням є визначення економічної та технологічної доцільності впровадження таких систем у сучасних IT-інфраструктурах, оцінка їхньої ефективності та окреслення ризиків і обмежень.

Сучасна наукова література демонструє активне зростання інтересу до алгоритмів машинного навчання, здатних розпізнавати нетипові або потенційно небезпечні дії у великих потоках телеметричних даних [1]. Дослідники відзначають, що алгоритми кластеризації, автоенкодери, нейронні мережі зі зворотним зв'язком і методи ансамблевого навчання забезпечують високу чутливість до невідомих атак і помилок конфігурацій [2, 4]. Зокрема, підходи на основі глибокого навчання показують здатність ідентифікувати складні кореляційні патерни у поведінці системи, які недоступні для класичних методів [1, 2]. Останні публікації також підкреслюють роль гібридних рішень, що поєднують машинне навчання з експертними системами або евристичними правилами [3, 4]. Такий підхід підвищує стабільність моделей і зменшує кількість хибних спрацьовувань.

Експериментальні дослідження у сфері кіберзахисту свідчать, що застосування машинного навчання дозволяє скоротити час реагування на інциденти, підвищити точність виявлення аномалій і оптимізувати використання людських ресурсів у центрах моніторингу безпеки [1, 2]. Разом з тим, дослідники зауважують необхідність врахування проблеми «дрейфу даних», коли поведінка серверів змінюється з часом, що вимагає постійного донавчання моделей [2].

Машинне навчання у сфері виявлення аномалій виконує роль інтелектуального фільтра, що здатний аналізувати великі обсяги даних у реальному часі. Алгоритми обробляють журнали подій, мережевий трафік і системні метрики, формуючи профіль «нормальної» поведінки сервера. Відхилення від цього профілю інтерпретуються як потенційні загрози. Такий підхід дозволяє виявляти не лише відомі типи атак, а й нові, для яких ще не існує сигнатур або описів.

З економічного погляду впровадження систем машинного навчання у сферу кіберзахисту може істотно знизити прямі втрати від інцидентів безпеки, скоротити час простою систем і зменшити витрати на ручний аналіз подій. Кожен уникнений збій або компрометація даних має вимірювану вартість, а тому автоматизоване виявлення аномалій формує реальний економічний ефект. Крім того, використання таких технологій підвищує довіру клієнтів і партнерів до цифрових сервісів, що має стратегічне значення для розвитку цифрової економіки.

Водночас машинне навчання у сфері безпеки пов’язане з низкою викликів. Основним є доступ до якісних і збалансованих даних для навчання моделей, адже реальні атаки трапляються набагато рідше, ніж звичайна активність. Це створює проблему дисбалансу класів і підвищує ризик помилкових спрацьовувань. Іншою складністю є пояснюваність рішень моделей. У критичних системах адміністраторам необхідно розуміти, чому саме алгоритм визнав певну активність підозрілою. Без цього довіра до системи та ефективність реагування знижуються. Також важливо враховувати правові аспекти обробки даних, особливо коли моніторинг охоплює персональну інформацію користувачів.

Застосування машинного навчання у виявленні аномалій серверної активності є одним із ключових напрямів формування кіберстійкої цифрової економіки. Такі системи дозволяють своєчасно виявляти небезпечні події, підвищувати ефективність інформаційної безпеки та оптимізувати витрати на її забезпечення. Економічна вигода від їхнього використання виражається у зменшенні втрат від кіберінцидентів, підвищенні надійності сервісів і зростанні довіри до цифрових технологій. Проте повна реалізація цього потенціалу можлива лише за умови поєднання технічних інновацій із прозорими процедурами контролю, етичними принципами обробки даних та безперервним удосконаленням моделей. У майбутньому машинне навчання може стати не лише засобом автоматичного моніторингу, а й стратегічним інструментом управління ризиками, що визначатиме конкурентоспроможність цифрової економіки у глобальному вимірі.

Список використаних джерел

1. Vajda Dániel László, Do Tien Van, Bérczes Tamás, Farkas Károly та ін. Machine learning-based real-time anomaly detection using data pre-processing in the telemetry of server farms. Scientific Reports. 2024. Vol. 14, Article 23288. DOI: 10.1038/s41598-024-72982-z.

2. Islam Mohammad Saiful, Rakha Mohamed Sami, Pourmajidi William, Sivaloganathan Janakan, Steinbacher John, Miranskyy Andriy. Anomaly Detection in Large-Scale Cloud Systems: An Industry Case and Dataset. arXiv preprint arXiv:2411.09047. 2024. Available: https://arxiv.org/abs/2411.09047

3. Benova Lenka, Hudec Ladislav. Comprehensive Analysis and Evaluation of Anomalous User Activity in Web Server Logs. Sensors (Basel). 2024. Vol. 24, No. 3, Art. 746. DOI: 10.3390/s24030746.

4. Wang Junxiang, Zheng Xu, Chen Zhengzhang, Natsumeda Masanao, Nishioka Jun, Luo Dongsheng, Chen Haifeng. ICeTEA: Mixture of Detectors for Metric-Log Anomaly Detection. MILETS@KDD'25 (Proceedings). 2025. 6 p. Available: https://kdd-milets.github.io/milets2025/papers/MILETS_2025_paper_2.pdf

СУЧАСНІ ЗАСОБИ ЗБИРАННЯ ТА ОБРОБКИ ІНФОРМАЦІЇ

Хутко Єлизавета
ЗВО спеціальності 073 Менеджмент
Миколаївський національний аграрний університет

У сучасному інформаційному суспільстві дані є ключовим ресурсом, який визначає розвиток науки, економіки та управління. Швидкість поширення цифрових технологій змінила підходи до збирання, аналізу та обробки інформації. Якщо раніше дослідники обмежувалися традиційними інструментами (анкетами, інтерв'ю, архівними джерелами), то нині на перший план виходять автоматизовані системи, інтернет-платформи та програмні комплекси, що дозволяють працювати з великими масивами даних у режимі реального часу.