УДК 004:005.3]:640.4

ДОСЛІДЖЕННЯ ПІДХОДІВ ЗАЛУЧЕННЯ КЛІЄНТІВ ДО МЕРЕЖІ КАВ'ЯРЕНЬ

Проценко М.М., Панфьорова І.Ю.
e-mail: mariia.protsenko@nure.ua, iryna.panforova@nure.ua
Харківський національний університет радіоелектроніки, каф. ІУС
м. Харків, Україна

Nowadays, the world has undergone irreversible changes in understanding what modern, effective business advertising should look like. To a large extent, the changes depend on the rapid development of new technologies, which people have understood how to master with benefit for themselves. This work explores methods for attracting a new audience designed for the gastronomic sector. The approaches are described and compared, and their advantages and limitations are characterized, considering further planning. The most effective of the listed ones is determined.

Маркетингові заходи є важливою складовою розвитку як великого, так і малого бізнесу. План маркетингових заходів, що представляє собою структуроване покрокове керівництво щодо реалізації певного комплексу заходів, спрямований на ефективне досягання визначених бізнес-цілей у обмежений проміжок часу. Для розробки плану маркетингових заходів важливо визначити найбільш ефективні заходи для залучення клієнтів в гастрономічному секторі.

Проведений аналіз історичних даних, таких як показники рентабельності інвестицій, вартості залучення клієнта до мережі кав'ярень та сума середнього чеку за проміжок часу реалізації запланованих заходів, показав, що найбільший інтерес до кав'ярень був спричинений завдяки таким заходам, як програма лояльності, пакет ваучерів, таргетована реклама у соціальних мережах, персоналізовані e-mail-пропозиції та колаборація з вже відомими бізнесами. Програма лояльності передбачає видачу карток клієнтам із спеціально виділеними місцями для наліпок, які можна отримати за кожну покупку певної позиції. Самі картки знаходяться у легкому доступі для клієнта під час дії заходу. Після того, як вся картка буде заповнена, клієнту надається можливість обміняти її на визначену бізнесом одиницю асортименту. Таким чином цей підхід стимулює повторні візити та формує у клієнтів звичку відвідувати кав'ярню.

Пакет ваучерів, в свою чергу, базується на розповсюдженні листівок з кодами на знижки, які можна використовувати онлайн або офлайн. Цей метод розрахований на різні групи населення та за рахунок цього розширює цільову авдиторію бізнеса, хоча має зазвичай короткостроковий ефект.

На сьогоднішній день за рахунок стрімкого розвитку соціальних мереж таргетована реклама стала найпопулярнішим рекламним форматом.

Таргетована реклама – це специфічний формат реклами в соціальних медіа, яку бачать тільки користувачі, які підпадають під вказані параметри: гендерна приналежність, вік, геолокація, список інтересів та інші [1].

Даний підхід є фінансово затратним, адже потребує спеціально навчених людей для налаштування усіх ключових характеристик і орієнтований на конкретно визначену цільову авдиторію, що обмежує кількість охопленого населення.

Цей підхід має й суттєві переваги. Таргетована реклама може містити заголовки, зображення та текст. Це дає великі можливості для креативу та привернення уваги клієнтів до мережі кав'ярень.

Персоналізовані e-mail-пропозиції є не менш ефективними при залученні клієнтів до кав'ярень. Персоналізація в емейл-маркетингу – це практика адаптації контенту до користувачів, тематики листів та інших елементів емейл розсилки на основі індивідуальних даних одержувача [2]. Персоналізація може полягати, як на додаванні особистих даних, так і на врахуванню історії покупок клієнта, його поведінку в інтернеті та способи взаємодії клієнта з мережею.

Колаборація – це процес спільної роботи двох або більше сторін з метою досягнення спільних цілей або створення нового продукту. До ознак вигідності співпраці відноситься розширення клієнтської бази за рахунок обміну авдиторіями та підвищення впізнаваності бренду. При використанні цього підходу збільшується прибуток і водночас скорочуються рекламні витрати завдяки взаємовигідній угоді. Основою колаборації є довіра авдиторії до бренду, з яким планується колаборація. Саме це дозволяє авдиторії довіряти бренду-посереднику.

В результаті дослідження виявлено, що кожен підхід є унікальним, і більшість з них можна застосовувати комплексно, що значно підвищить активність взаємодії клієнтів з мережею кав'ярень. Розроблено рекомендації щодо використання заходів для досягнення конкретних бізнес-цілей. Ці рекомендації сприяють оптимізації планування маркетингових заходів відповідно до запиту кав'ярень, допомагаючи даному бізнесу зрозуміти, який саме підхід зможе краще привернути увагу клієнтів.

Список використаних джерел:

1. Іванина Р., Клімак Ю. Таргетована реклама в соцмережах: види, формати та особливості. URL: https://elit-web.ua/ua/blog/targetirovannaya-reklama (дата звернення: 25.02.2025).

2. Felix Rose-Collins. Персоналізація в e-mail-маркетингу: Стратегії для покращення залучення. Ranktracker: The all-in-one platform for effective SEO. URL: https://www.ranktracker.com/uk/blog/personalization-in-e-mail-marketing-strategies-for-improved-engagement/ (дата звернення: 25.02.2025).

УДК 004.7:37]:004.056.5

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У ТРАФІКУ КОМП'ЮТЕРНИХ МЕРЕЖ ОСВІТНІХ ЗАКЛАДІВ

Радоуцька А.К., Панфьорова І.Ю.
e-mail: anna.radoutska@nure.ua, iryna.panforova@nure.ua
Харківський національний університет радіоелектроніки, каф. ІУС
м. Харків, Україна

Educational institutions increasingly rely on computer networks, making them vulnerable to cyberattacks that can compromise data and disrupt operations. AI-powered approaches enhance cybersecurity by analyzing behavioral patterns and identifying anomalies without manual configuration. Different AI methods offer various advantages where supervised learning predicts threats based on historical data, anomaly detection identifies deviations from normal behavior, clustering finds hidden connections between threats, and reinforcement learning adapts security responses in real time. This article shows how to choose the correct method depending on specific security needs.

В умовах військового стану організація роботи освітніх закладів вимагає розвиненої ІТ-мережі. Це робить інформаційні системи закладів вищої освіти (ЗВО) привабливими цілями для кібератак, які можуть порушити роботу ЗВО, скомпрометувати персональні дані здобувачів освіти та співробітників або завдати фінансових збитків. Тому при розробці інформаційних систем ЗВО постає питання про вибір підходів і методів, які б дозволили своєчасно виявляти стандартні та нестандартні загрози. Наразі в подібних ситуаціях використовуються традиційні ідентифікатори загроз з використанням системи виявлення втручань (IDS), систем управління інцидентами та подіями безпеки (SIEM) тощо, робота яких зазвичай супроводжується спеціалізованою командою безпеки.

IDS – це система виявлення атак (вторгнень), яка може бути представлена як програмне забезпечення або пристрій, що відстежує мережу на наявність зловмисних дій хакерів. Інформація про зловмисну діяльність або порушення збирається централізовано за допомогою системи керування інформаційною безпекою. Широко використовуються IDS на основі сигнатур, які є найпоширенішими системами виявлення шкідливих дій через мережевий трафік. Коректність роботи IDS залежить від її інформованості про те, як виглядає загрозлива діяльність [1].

SIEM – це клас систем, які надають централізоване рішення для управління подіями безпеки. Вони мають функціонал для збору, агрегування, зберігання та корелювання подій за допомогою різних інструментів. Різноманітні складові утворюють загальну платформу поєднання сучасних операційних центрів безпеки, корелюють події безпеки та надають синтетичні представлення сповіщень про загрози та стан безпеки [1].

З часом системи стають неадаптованими до нових методів атак і можуть неефективно фільтрувати аномальну активність, оскільки працюють за фіксованим набором правил. Для налаштування під нові, активно виникаючі загрози, потрібна система, яка могла б навчатись на попередньому досвіді.

В роботі пропонується один з можливих підходів до вирішення цієї задачі, який базується на використанні систем штучного інтелекту (ШІ).

Використання ШІ дозволяє аналізувати поведінкові патерни та виявляти нові загрози без необхідності ручного налаштування. Для створення систем відстежування аномалій функціонування комп'ютерної мережі використовують методи машинного та глибокого навчання, які пропонується класифікувати за критеріями, які враховують підходи до навчання та їх алгоритмічну природу [2].

Контрольоване навчання використовує алгоритм машинного навчання, який працює із розміченими даними для передбачення загроз. Системи, які використовують цей метод, дозволяють моделювати попередні атаки та визначати нові загрози, схожі на відомі сценарії, що робить їх ефективними, коли існує достатня база попередніх загроз.

Дерева рішень – це метод класичного машинного навчання, який використовує деревоподібну структуру для ухвалення рішень. Він підходить для класифікації загроз тоді, коли атаки мають чітко визначені характеристики й тому забезпечують високу інтерпретованість результатів, але менш ефективні у виявленні складних або невідомих атак.

Виявлення аномальних загроз базується на аналізі історичних даних для створення моделі нормальної поведінки. Всі нові події оцінюються відносно цієї моделі. Це допомагає виявити загрози, навіть якщо вони не відповідають відомим шаблонам атак.

При використанні кластеризації система захисту групує подібні події та аномальні активності у кластери, і при подальшому аналізі це дає змогу знаходити приховані зв'язки між загрозами. Такий підхід використовується в системах безпеки, де важливо виявити аномалію і зрозуміти її походження, і набір даних є розміченим.

Навчання з підкріпленням дозволяє системі самостійно навчатися реагувати на загрози в реальному часі, так як в основі знаходиться алгоритм, який адаптує поведінку системи залежно від результатів її дій. Це дозволяє створювати динамічні системи безпеки, які можуть самостійно активно підлаштовуватись під нові види загроз.

У випадку, якщо жоден з підходів не задовольняє вимогам захисту повною мірою, то пропонується комбінувати наведені методи, використовуючи гібридний підхід для отримання кращого результату. Такий спосіб інтегрує традиційні засоби інформаційної безпеки з можливостями ШІ для підвищення ефективності виявлення загроз та реагування на них.

Для визначення методу ШІ, який швидше виявляє загрози для комп’ютерної мережі, було розроблено дерево рішень, яке представлено на рисунку 1.

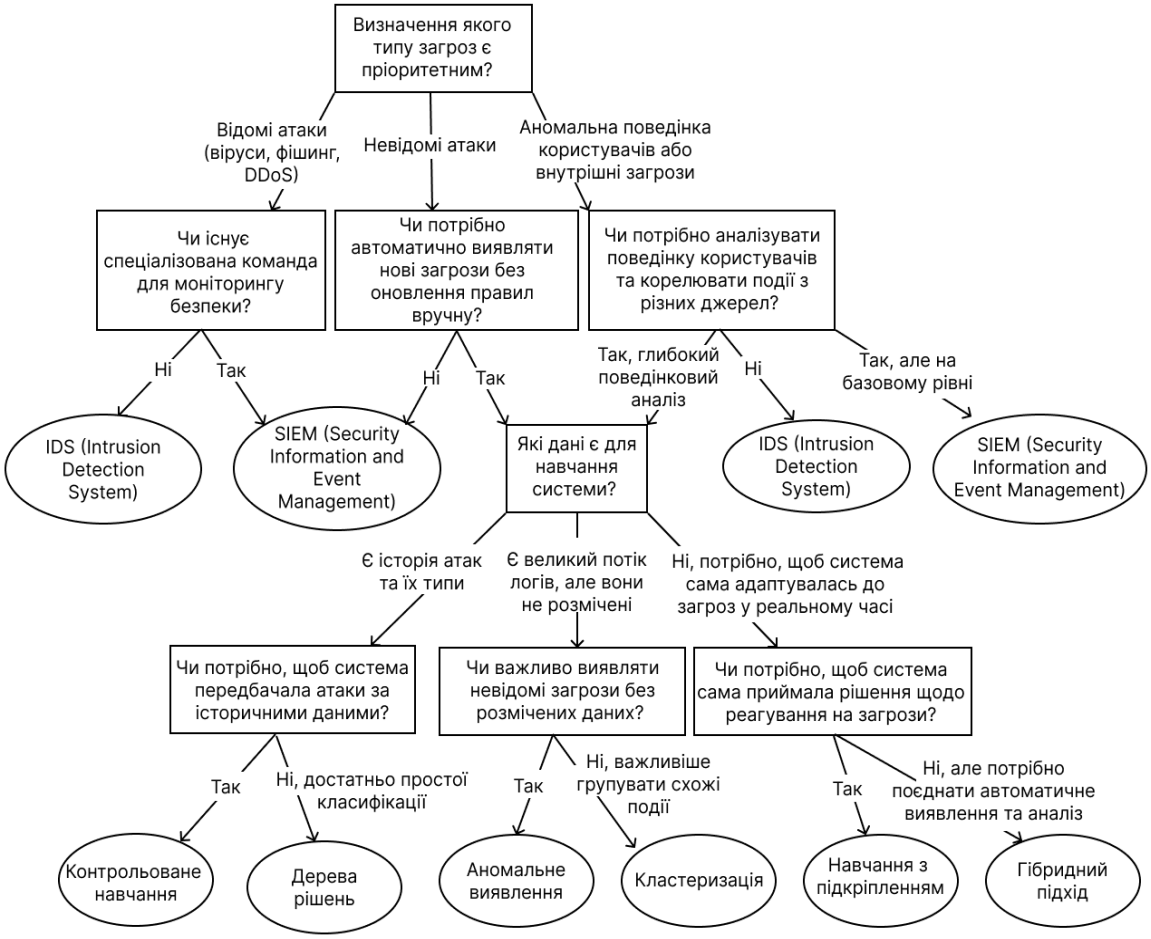

Рисунок 1 – Дерево рішень для визначення методу виявлення аномалій у трафіку комп’ютерної мережі

В роботі визначено, що використання дерева рішень дає можливість формального вибору методу ШІ, який може бути використаний в мережі для виявлення аномалій у трафіку комп’ютерної мережі, а також попередження подальшого проникнення у систему злочинцями.

Список використаних джерел:

1. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. URL : https://pubmed.ncbi.nlm.nih.gov/34300500/ (дата звернення: 17.01.2025).

2. Janiesch C., Zschech P., Heinrich K. Machine learning and deep learning. April 2021. URL : https://arxiv.org/abs/2104.05314 (дата звернення: 18.01.2025).