Мамонов Анатолій Сергійович, Мороз Юрій Павлович,

Фетько Степан Іванович, бакалаври

Західноукраїнський національний університет, м. Тернопіль

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ, ІНТЕРНЕТ РЕЧЕЙ І ВЕЛИКИХ ДАНИХ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ В РОЗУМНИХ МІСТАХ, СОЦІАЛЬНИХ ТА КОМП'ЮТЕРНИХ МЕРЕЖАХ

У сучасну епоху стрімкого розвитку технологій, інтеграція передових технологій стає ключовим фактором для забезпечення безпеки та ефективності в різних сферах життя. Це включає в себе розумні міста, соціальні мережі та комп'ютерні мережі, де штучний інтелект (AI), Інтернет речей (IoT) та великі дані (Big Data) відіграють важливу роль.

Штучний інтелект відкриває нові горизонти для автоматизації процесів, аналізу даних та прийняття рішень. Він здатний обробляти величезні обсяги інформації значно швидше та точніше, ніж людина, що робить його незамінним інструментом у багатьох сферах.

Інтернет речей забезпечує з'єднання різних пристроїв та систем, створюючи мережу, яка дозволяє збирати та обмінюватися даними в режимі реального часу. Це відкриває нові можливості для оптимізації процесів та підвищення ефективності.

Великі дані є основою для аналізу та прийняття рішень у багатьох сферах. Вони дозволяють виявляти закономірності, прогнозувати тенденції та робити інформовані рішення. Big Data стають все більш важливими у науці, маркетингу, охороні здоров’я та ін.

У цій статті розглянемо три основні напрямки, які ілюструють впровадження цих технологій для вирішення актуальних проблем безпеки.

У розумних містах візуальний нагляд є важливою складовою забезпечення правопорядку та безпеки. Традиційні системи спостереження, які покладаються на ручний аналіз відеопотоків, стикаються з проблемами через людську обмеженість у здатності залишатися уважними протягом тривалих періодів. У відповідь на ці виклики, нова галузь штучного інтелекту речей (AIoT) поєднує AI та IoT для створення мережі сенсорів, що можуть ефективно спілкуватися, обробляти та аналізувати дані на різних рівнях (edge, fog, cloud). Впровадження AIoT у системи відеоспостереження дозволяє автоматично виявляти аномальні події, такі як дорожні аварії, бійки та пограбування, що підвищує загальну ефективність та надійність систем відеоспостереження у розумних містах [1].

Однак ручний аналіз таких відео є складним завданням для людей, які схильні до помилок через їхню обмежену здатність залишатися уважними і активними протягом тривалих періодів часу. У реальних ситуаціях нагляду виявлення аномалій, таких як дорожні аварії, бійки та пограбування, залишається головним викликом для дослідників комп'ютерного зору.

Для вирішення цих проблем пропонується підхід на основі глибоких нейронних мереж та AIoT, що дозволяє ефективно аналізувати відеопотоки в реальному часі. Це передбачає використання архітектури нейронної мережі, яка включає в себе як просторові, так і часові характеристики для покращення точності виявлення аномалій. Запропонована система дозволить автоматично виявляти аномальні події, зменшуючи навантаження на операторів і підвищуючи загальну ефективність системи відеоспостереження.

З розвитком інтернет-технологій та прискореною глобалізацією, кількість пристроїв у розумних мережах зросла, що призвело до вибухового зростання обсягу даних в інтернеті [2]. У соціальних мережах, таких як QQ, WeChat та Weibo, користувачі часто стикаються з проблемами безпеки, включаючи атаки, витоки приватних даних та крадіжку конфіденційної інформації [3]. Традиційні методи пошуку інформації мають труднощі з вчасним пошуком та вилученням даних, що робить необхідним розробку нових моделей для забезпечення безпеки даних. Використання глибоких згорткових нейронних мереж дозволяє ефективно добувати теми безпеки та аналізувати продуктивність безпеки даних у соціальних мережах, забезпечуючи високу точність прогнозування та ефективну передачу даних.

Зі зростанням кількості підключених пристроїв та обсягу переданих даних, моніторинг та аналіз мережевого трафіку стали критично важливими для забезпечення стабільного, безпечного та ефективного функціонування мереж. Використання технологій штучного інтелекту та великих даних дозволяє створювати ефективні інструменти для перехоплення мережевих пакетів, виявлення аномалій та несанкціонованих дій у мережі [4, 5]. Це сприяє оперативному реагуванню на загрози та попередженню потенційних атак, що є ключовим для забезпечення кібербезпеки. Розробка програмного забезпечення для моніторингу та аналізу мережевого трафіку сприяє покращенню продуктивності та безпеки комп'ютерних мереж.

Інтеграція передових технологій, таких як AIoT, глибокі нейронні мережі та великі дані, є вирішальною для підвищення ефективності та безпеки в різних сферах життя. У розумних містах це дозволяє автоматизувати процеси відеоспостереження, в соціальних мережах – забезпечувати безпеку даних, а в комп'ютерних мережах – покращувати продуктивність та захист від кіберзагроз. Подальший розвиток цих технологій відкриває нові горизонти для інновацій та вдосконалення існуючих систем.

**Література**

1. Muhammad K., Obaidat M.S., Hussain T., Ser J.D., Kumar N., Tanveer M., *et al.* Fuzzy logic in surveillance big video data analysis: Comprehensive review, challenges, and research directions. ACM Comput. Surv. 2021. Vol. 54. Pp. 1-33.
2. Mulia D., Shihab M.S. Strategy to maintain the cinema industry in the middle of development of internet technology. JM. 2020. Vol. 24 (1). Pp. 124-138.
3. Valeri M., Baggio R. Italian tourism intermediaries: a social network analysis exploration. Curr. Issue Tour. 2021. 24 (9). Pp. 1270-1283.
4. Komar M., Sachenko A., Bezobrazov S., Golovko V. Intelligent Cyber Defense System. CEUR-WS. 2016. Vol. 1614. Pp. 534-549.
5. Komar M., Sachenko A., Bezobrazov S., Golovko V. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques. Communications in Computer and Information Science. 2017. Vol. 783. Рp. 36-55.