2. Mollakuqe E: Comparative analysis of identity management, access control, and authorization practices in public and private universities. [Dataset], 2024. http://www.doi.org/10.17605/OSF.IO/5P9KE.

3. Grata E. G., Deshpande A., Lopes R. T., Laghari A. A., Khan A. A., Jenice Aroma R., Jumani, A. K. (2024). Artificial intelligence for threat anomaly detection using graph Data bases a semantic outlook. Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 249-278.

Штучний інтелект у сфері відеоспостереження

УДК 004.056.5:004.08

Марк Хіленко[1], Максим Фесенко[2]

Державний університет інформаційно-комунікаційних технологій,

[1]markhilenko@gmail.com

Постановка задачі. На сьогоднішній день безпека є одним із пріоритетних напрямків для громадян та організацій. Неодмінною складовою у сфері безпеки та охорони є системи відеоспостереження зі штучним інтелектом.

Один із ключових аспектів систем відеоспостереження із штучним інтелектом є їх можливість аналізувати великі обсяги даних у реальному часі. Нейронні мережі та інші алгоритми машинного навчання можуть обробляти величезні потоки інформації з камер відеоспостереження, датчиків руху, систем виявлення вторгнень та інших джерел, що дозволяє виявляти аномалії та надзвичайні ситуації в реальному часі.

Дослідники постійно працюють над створенням більш точних та ефективних моделей, які можуть розпізнавати нові типи загроз та адаптуватися до змінних умов навколишнього середовища. Отже, зростання потенціалу виявлення загроз завдяки використанню штучного інтелекту є ключовою тенденцією, яка сприяє покращенню безпеки та ефективності охоронних систем [1].

Мета дослідження. Дослідити дані щодо застосування технологій штучного інтелекту в сучасних системах відеоспостереження та визначити практичну їх реалізацію.

Результати дослідження. У роботі проведено аналіз сфер застосування сучасних безпекових та охоронних систем із штучним інтелектом.

• Виявлення загроз.

Системи відеоспостереження зі штучним інтелектом здатні виявляти підозрілу поведінку, залишені предмети, зброю та інші потенційні загрози, що дозволяє оперативно реагувати на інциденти. Наприклад, компанія Bosch Security Systems використовує AI-аналітику для виявлення блокування аварійних виходів, неправильного паркування та інших порушень безпеки [2].

• Розпізнавання обличчя та номерних знаків.

Інтеграція алгоритмів розпізнавання обличь та номерних знаків дозволяє ідентифікувати осіб та транспортні засоби, що сприяє ефективному розслідуванню правопорушень. Наприклад, компанія Flock Safety пропонує автоматизовані системи розпізнавання номерних знаків, які використовуються

в понад 5000 громадах США для виявлення викрадених автомобілів та інших правопорушень [3].

• Прогнозування інцидентів.

Використання штучного інтелекту дозволяє прогнозувати можливі інциденти на основі аналізу поведінки та історичних даних, що підвищує превентивні заходи безпеки. Наприклад, компанія Knightscope розробляє автономні роботи для патрулювання, які можуть виявляти аномальні звуки, зміни температури та інші показники, що свідчать про потенційні загрози [4].

Висновки та перспективи. В результаті дослідження, було виявлено, що використання систем відеоспостереження з штучним інтелектом демонструє значну продуктивність та здатність виявляти загрози. Приклади компаній Bosch Security Systems, Flock Safety та Knightscope показують, що впровадження нейронних мереж та інтеграція з відеоспостереженням значно підвищують ефективність виявлення загроз та зменшує кількість хибних спрацювань.

Подальші дослідження мають бути зосереджені на підвищенні точності, зменшенні помилок та захисті персональних даних.

1. Тенденції у використанні штучного інтелекту для покращення реагування охоронних систем на загрози. URL: https://mindscope.biz.ua/tendenczіyi-u-vykorystanni-shtuchnogo-intelektu-dlya-pokrashhennya-reaguvannya-ohoronnyh-system-na-zagrozy (дата звернення 16.0.2025).

2. Javier Finance, Artificial Intelligence for video surveillance (Use cases). URL: https://javierfinanc e.com/blog/ai-video-surveillance-use-cases/ (дата звернення 16.0.2025).

3. Louise Matsakis, Flock Safety Says Its License Plate Readers Reduce Crime. It's Not That Simple. URL: https://www.wired.com/story/flock-safety-license-plate-readers-crime/ (дата звернення 16.0.2025).

4. How Autonomous Robots are Revolutionizing Public Safety**.** URL: https://knightscope.com/blog/autonomous-security-robots-upgrading-public-safety (дата звернення 16.0.2025).

Аналіз елементів класичної моделі передачі інформації

УДК 519.72

Юрій Хлапонін[1], Володимир Вишняков[2]

Київський національний університет будівництва та архітектури,

[1]y.khlaponin@gmail.com, [2]volodymyr.vyshniakov@gmail.com

Класична модель процесу передачі інформації (запропонована в 1948 році засновником теорії інформації Клодом Шенноном) показана на рис. 1.