АНАЛІЗ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПІДВИЩЕННЯ ФІЗИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ

Буграк Б.В., Чакрян В.Х., Андрушко Д.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: bohdan.buhrak@nure.ua
vadym.chakrian@nure.ua
dmytro.andrushko@nure.ua

Abstract

The article examines the effectiveness of artificial intelligence (AI) technologies in video surveillance systems for enhancing the physical security of facilities. A comparative analytical method was used to assess the effectiveness, which allowed comparing the key indicators of traditional and intelligent systems. It analyses current ISO standards governing video surveillance in security systems. Recommendations are made for the implementation of AI technologies, taking into account aspects of confidentiality and cybersecurity.

У сучасних умовах зростання кіберфізичних загроз питання фізичної безпеки об'єктів критичної інфраструктури (ОКІ), дата-центрів та мережевої інфраструктури набуває особливої актуальності. Традиційні системи відеоспостереження, які залежать від оператора, демонструють обмежену ефективність через високу ймовірність помилки та затримки реагування.

З поширенням технологій комп'ютерного зору та глибокого навчання з'явилась можливість інтегрувати штучний інтелект (ШІ) у відеоаналітику, що суттєво підвищує рівень автоматизації моніторингу та знижує навантаження на персонал

Основи застосування штучного інтелекту у відеоспостереженні

Сучасні системи штучного інтелекту (ШІ) для відеоспостереження використовують алгоритми комп'ютерного зору та глибокі нейронні мережі, які дозволяють виявляти об'єкти, розпізнавати обличчя, ідентифікувати транспортні засоби та аналізувати поведінкові патерни [1]. У низці досліджень підтверджено можливість автоматичного виявлення підозрілої поведінки, включно з проникненням у заборонені зони, залишенням предметів та аномальними переміщеннями [2].

Інтеграція з сенсорами Інтернету речей (руху, звуку, температури) формує багаторівневі системи безпеки, які забезпечують комплексну оцінку ситуацій у режимі реального часу [1]. Для ОКІ це важливо, адже несанкціонований доступ до серверних приміщень, телекомунікаційних вузлів або енергетичних об'єктів часто є першою фазою складних кібератак.

Також важливим питанням є обробка відеоданих, особливо критичним це є для об'єктів із високими вимогами до конфіденційності. Обробка прямо на відеоконтролері або безпосередньо на камері, яку можна віднести до Edge-AI, зменшує залежність від каналів зв'язку та мінімізує ризик витоку відео, що рекомендовано для дата-центрів та енергетичних об'єктів [3]. Хмарна ж обробка забезпечує масштабованість та централізований аналіз великих масивів даних, але законодавчі та безпекові вимоги часто обмежують її використання для об'єктів критичної інфраструктури (ОКІ) [4], [5].

Порівнювання ефективності традиційних і розумних систем відеоспостереження

Для комплексної оцінки переваг інтелектуальних систем відеоспостереження доцільно порівняти традиційні рішення та системи на базі штучного інтелекту за низкою ключових критеріїв. Серед основних показників ефективності виділяють точність виявлення подій, кількість хибних тривог, час реагування на інциденти та потребу у присутності персоналу. Таке порівняння дозволяє оцінити не лише технічні характеристики систем, але й їхній вплив на загальний рівень безпеки об'єктів.

Дані порівняння традиційних та інтелектуальних систем ґрунтуються на результатах експериментів, наведених у роботах [1], [6]. Зведені показники подано у таблиці 1.

Таблиця 1. Порівнювання характеристик систем відеоспостереження

Показник	Традиційна система	Система з ШІ
Точність виявлення подій	60–70%	90–96%
Час реагування	30–60 с	3–5 с
Хибні тривоги	Високий рівень	Зниження до 40–70%
Потреба в операторі	Постійна	Часткова
Можливість прогнозування	Відсутня	Присутня

Таким чином, інтелектуальні системи демонструють вищу точність, швидшу реакцію та кращу масштабованість, що особливо актуально для дата-центрів і критичної телекомунікаційної інфраструктури, де будь-які затримки можуть призвести до значних збитків.

Роль ШІ у захисті дата-центрів, мережевої інфраструктури та об'єктів критичної інфраструктури

Дата-центри, телекомунікаційні вузли та об'єкти критичної інфраструктури є основою цифрової стійкості держави. В Україні до ОКІ належать системи енергетики, зв'язку, транспорту, ІТ, фінансового сектору та інші об'єкти, порушення роботи яких може призвести до значних національних ризиків. Оскільки значна частина інцидентів у дата-центрах та мережевій інфраструктурі пов'язана з несанкціонованим фізичним доступом або внутрішніми порушеннями [5], системи відеоспостереження з модульною ШІ-аналітикою відіграють важливу роль у запобіганні таким загрозам.

Інтелектуальні системи на основі комп'ютерного зору здатні автоматично виявляти проникнення у серверні кімнати, вузлові приміщення обміну трафіком, телекомунікаційні шафи чи інші ізольовані зони. ШІ розпізнає обличчя, оцінює відповідність доступу, фіксує спроби несанкціонованого проникнення і визначає появу осіб або предметів, нетипових для конкретної зони. Для ОКІ це є критично важливим, оскільки стороннє втручання в мережеве чи енергетичне обладнання часто стає першою фазою складних комбінованих кібератак.

Алгоритми поведінкового аналізу дозволяють відстежувати маршрути персоналу та виявляти аномальні дії: відвідування заборонених зон, необґрунтоване перебування біля обладнання, повторювані нетипові переміщення або спроби уникнути поля зору камер [2]. Такі функції особливо потрібні для об'єктів енергетики, телекомунікацій та промисловості, де інсайдерські загрози становлять значну частку ризиків.

ШІ-відеоспостереження може інтегруватись із системами контролю доступу, Security Information and Event Management (SIEM) та Security Orchestration, Automation and Response (SOAR), створюючи єдиний контур кіберфізичної безпеки. Це забезпечує кореляцію відеоподій із журналами доступу та мережевими логами, а також дозволяє автоматично виконувати реакційні дії, наприклад, блокувати двері чи вимикати мережеві порти у разі інциденту [7].

Важливою перевагою для ОКІ є здатність ШІ виявляти маніпуляції з мережевим та серверним обладнанням: відкриття шаф, заміну модулів, підключення сторонніх пристроїв, порушення кабельних трас. Алгоритми порівнюють реальні зображення з еталонними схемами та фіксують будь-які зміни, що можуть свідчити про саботаж або спробу перехоплення трафіку.

Розвиток локальної обробки відеопотоку, без передачі в хмару, відповідає вимогам конфіденційності для українських ОКІ. Локальний аналіз забезпечує мінімальну затримку, швидку реакцію та стійкість до атак на канали зв'язку .

Поєднання ШІ з принципами «нульової довіри» формує нову модель фізичної безпеки: кожна дія перевіряється, особа верифікується багаторазово, а системи автоматично блокують підозрілі сценарії.

Завдяки цьому ШІ стає важливим компонентом захисту дата-центрів, мережевих вузлів та української критичної інфраструктури, підсилюючи їхню здатність протистояти сучасним кіберфізичним загрозам.

Ризики виокристання штучного інтелекту у процесах відеоспостереження

Впровадження інтелектуальних систем відеоспостереження супроводжується низкою ризиків. Найбільш критичним є дотримання вимог у сфері захисту персональних даних, зокрема відповідність положенням General Data Protection Regulation (GDPR) [8] та українському законодавству щодо обробки відеоданих, біометрії та зберігання інформації. Іншим важливим аспектом є можливість кіберзагроз, спрямованих безпосередньо на мережеві камери, відеореєстратори та сервери відеоаналітики. Компрометація таких пристроїв може надати зловмисникам доступ до внутрішньої мережі або дозволити маніпулювати сигналами відеоспостереження. Крім того, впровадження комплексних ШІ-рішень, особливо для великих ОКІ, пов'язане зі значними витратами на обладнання, апгрейд мережевих сегментів, навчання персоналу та сертифікацію систем.

Застосування ШІ-систем повинно відповідати чинній міжнародній та національній нормативній базі. Стандарт ISO/IEC 27001:2022 регламентує вимоги до систем управління інформаційною безпекою, включно зі зберіганням та захистом відеоданих [9]. ISO 22341:2021 визначає принципи безпечного проєктування середовища Crime Prevention Through Environmental Design (CPTED), що охоплюють інтеграцію відеоспостереження, контролю доступу та інших фізичних засобів захисту [4]. Стандарт ISO/IEC 30128 містить вимоги до функціональності та точності систем відеоаналітики, включаючи алгоритми розпізнавання та виявлення аномалій [3]. В Україні регуляторними документами для об'єктів критичної інфраструктури є вимоги НБУ щодо захисту інформації в фінансовій сфері, стандарти та методичні рекомендації ДССЗЗІ, а також нормативи Міністерства цифрової трансформації, що визначають підходи до кіберзахисту державних інформаційних ресурсів [10],[11].

Таким чином, використання ШІ у системах відеоспостереження забезпечує підвищення ефективності захисту, але потребує належного врахування ризиків та чіткого дотримання міжнародних і національних регуляторних вимог. Це дозволяє впроваджувати технології безпеки таким чином, щоб вони не лише покращували захист об'єкта, а й залишалися юридично та технічно обґрунтованими.

Література

1. Бурієнко О. В. Зарубіжний досвід використання правоохоронними органами систем відеоспостереження у протидії злочинності // Науковий вісник Ужгородського національного університету. Серія «Право». 2025. №3(88). С. 30–38. DOI: https://doi.org/10.24144/2307-3322.2025.88.3.30.

2. Чуян І. О., Оникієнко Ю. О. Система відеоспостереження з функцією розпізнавання та з двома каналами передавання інформації // Електронна та Акустична Інженерія. 2020. Т. 3, №2. С. 53-57 Режим доступу: https://feltran.kpi.ua/article/view/198747.

3. ISO/IEC 30128:2014. Information technology – Security techniques – Code of practice for security management of surveillance camera systems.

4. ISO 22341:2021. Security and resilience – Protective security – Guidelines for crime prevention through environmental design. International Organization for Standardization.

5. Ronchieri, E., Pacinelli, F., Giommi, L., Duma, D. C., Costantini, A., Salomoni, D. (2023). Anomaly Detection in Data Center IT Infrastructure using Natural Language Processing and Time Series Solutions. ISGC & HEPiX Workshop, 2023. DOI: https://doi.org/10.22323/1.434.0024.

6. Korytkov, D., Kosenko, V., Kovalenko, D. (2023). Object Detection Performance Indicator in Video Surveillance Systems. Radio Electronics, Computer Science, Control, № 2. DOI: https://doi.org/10.15588/1607-3274-2023-2-8.

7. Ribeiro, J., Calheiros, R. (2021). Integration of Video Analytics with SIEM Architectures for Critical Infrastructure Protection. Computers & Security. DOI: https://doi.org/10.1016/j.cose.2021.102453.

8. Barnoviciu, E., Ghenescu, V., Carata, Ș., Ghenescu, M. (2019). GDPR Compliance in Video Surveillance and Video Processing Application. Режим доступу: https://www.researchgate.net/publication/337527760_GDPR_compliance_in_Video_Surveillance_and_Video_Processing_Application.

9. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. International Organization for Standardization.

10. Міністерство цифрової трансформації України. (2021–2024). Методичні рекомендації з кіберзахисту об'єктів критичної інфраструктури. Режим доступу: https://cip.gov.ua.

11. Національний банк України (НБУ). Положення про організацію кіберзахисту в банківській системі України. 2022. Режим доступу: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text.