

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДЛЯ ПІДТРИМКИ РІШЕНЬ У СФЕРІ ВІДЕОСПОСТЕРЕЖЕННЯ

Анотація. У статті досліджується концепція створення сучасної інформаційної технології, яка забезпечує ефективну підтримку прийняття рішень у сфері відеоспостереження. З огляду на зростаючий обсяг відеоданих, що генеруються системами моніторингу, особливо в умовах урбанізованого середовища, виникає потреба у високопродуктивних рішеннях, здатних працювати в режимі реального часу. Основна увага приділяється аналізу технологічних підходів до обробки відеопотоків із застосуванням штучного інтелекту, методів машинного навчання, обчислень на периферії (edge computing) та хмарних рішень. У межах дослідження представлено архітектурну модель багаторівневої інформаційної системи, яка включає модулі збору даних, попередньої обробки, аналітики та прийняття рішень. Особливу увагу приділено алгоритмам виявлення подій та класифікації поведінкових шаблонів, що дозволяє знизити залежність від людського фактору при аналізі потоків спостереження.

В роботі також розглянуто аспекти інтеграції таких систем з іншими інформаційно-аналітичними платформами, зокрема базами біометричних даних, геоінформаційними системами, системами контролю доступу. Обґрунтовано переваги використання edge-архітектур, які дозволяють зменшити затримки при обробці відео, підвищити автономність системи та зменшити навантаження на центральну інфраструктуру. Результати дослідження можуть бути використані для створення інтелектуальних систем безпеки нового покоління, зокрема в рамках концепції Smart City. Представлений підхід може бути адаптований до потреб органів місцевого самоврядування, правоохоронних структур, а також приватного сектору, що займається охороною об'єктів критичної інфраструктури. Отримані результати демонструють практичну цінність застосування новітніх IT-рішень у сфері безпеки та моніторингу.

Ключові слова: відеоспостереження, інформаційна технологія, підтримка прийняття рішень, безпека, AI, машинне навчання, edge computing, аналітика даних, інтеграція систем, автоматичне виявлення.

Постановка проблеми. У сучасному суспільстві, що характеризується зростанням урбанізації, техногенного навантаження та загроз безпеці різного походження, системи відеоспостереження відіграють надзвичайно важливу роль у захисті громадського порядку, інфраструктури та приватної власності. Традиційні підходи до відеомоніторингу, що передбачають переважно фіксацію та зберігання відеозаписів, поступово

втрачають свою ефективність. З огляду на стрімке зростання кількості джерел відеоінформації, ручний перегляд і аналіз відеопотоків стає фізично неможливим і економічно затратним. Це зумовлює необхідність створення нових інформаційних технологій, які забезпечують автоматизовану обробку великих обсягів відеоданих і здатні оперативно реагувати на критичні події.

Ключова проблема полягає в тому, щоб трансформувати відеоспостереження із пасивного інструменту фіксації подій у активну інтелектуальну систему підтримки прийняття рішень. Така система повинна не лише виявляти потенційно небезпечні ситуації в реальному часі, а й аналізувати їх контекст, надавати рекомендації операторам або навіть автоматично ініціювати відповідні дії. У цьому контексті особливого значення набуває застосування штучного інтелекту, машинного навчання, edge computing та інтеграції з іншими інформаційно-аналітичними системами. Таким чином, актуальність дослідження обумовлена потребою у створенні ефективної, гнучкої та масштабованої інформаційної технології, здатної забезпечити прийняття рішень на основі відеоаналітики в умовах динамічного та складного середовища.

Аналіз останніх досліджень і публікацій. У світовій науковій спільноті активно досліджуються можливості застосування інтелектуальних технологій у сфері відеоспостереження, зокрема в контексті автоматичного розпізнавання подій та аномальної поведінки. У роботі Y. Zhang, F. Liu та M. Wang представлено модель виявлення аномалій у режимі реального часу, яка ґрунтується на глибоких згорткових нейронних мережах і спрямована на підвищення точності в урбанізованих середовищах. Gupta і Jain досліджують ефективність використання штучного інтелекту у системах відеоаналітики, приділяючи особливу увагу проблемам класифікації та масштабованості таких рішень. У статті T. Chen та L. Chen розглянуто концепцію обчислень на периферії (edge computing) як засобу підвищення швидкодії систем відеоспостереження при збереженні високого рівня безпеки. Дослідження A. Luna, M. Tortonesi та M. Paganelli акцентує увагу на інтеграції відеоаналітики з хмарними сервісами та інтернетом речей, що відкриває нові можливості для адаптивного управління інформаційними потоками. Усі згадані роботи засвідчують високий науковий інтерес до тематики, проте більшість з них зосереджена на вузьких аспектах - таких як алгоритми розпізнавання або окремі архітектурні рішення - тоді як комплексна концепція технології підтримки рішень у сфері відеоспостереження потребує подальшої систематизації та міждисциплінарного підходу.

Мета дослідженн. Метою цього дослідження є розробка та теоретичне обґрунтування концепції інформаційної технології, здатної забезпечити ефективну підтримку прийняття рішень у сфері відеоспостереження на основі сучасних досягнень у галузях штучного інтелекту, машинного навчання, обчислень на периферії (edge computing) та інтеграційних цифрових платформ. Зокрема, дослідження спрямоване на визначення структури і функціональної архітектури такої системи, її основних модулів, методів збору, обробки, аналізу та візуалізації відеоданих, а також способів інтеграції з іншими інформаційними системами безпеки. Особливу увагу приділено завданням розробки алгоритмів виявлення аномальних подій у реальному часі, мінімізації затримок у пере-

дачі й обробці інформації, а також забезпеченню високої надійності, масштабованості та гнучкості у змінних середовищах функціонування системи. У межах роботи також передбачається оцінка можливостей практичного застосування запропонованої концепції в умовах «розумного міста» та інших безпекових сценаріїв.

Викладення основного матеріалу. Інформаційна технологія для підтримки прийняття рішень у сфері відеоспостереження передбачає створення комплексної багаторівневої системи, що поєднує в собі фізичні засоби збору інформації, інтелектуальні алгоритми її обробки та механізми прийняття рішень у режимі реального часу. Така система повинна бути гнучкою, масштабованою та сумісною з іншими цифровими платформами, що забезпечують безпеку, аналітику та управління міською або промисловою інфраструктурою. У центрі розробки стоїть ідея переходу від традиційного, реактивного відеоспостереження до проактивного, прогнозного та адаптивного моніторингу на основі аналітики даних.

Архітектура запропонованої системи будується за принципом ієрархічної багаторівневої моделі. На першому, сенсорному рівні, здійснюється первинний збір даних за допомогою відеокамер, тепловізійних сенсорів, детекторів руху, акустичних та інших спеціалізованих датчиків. Важливо, що всі пристрої повинні мати можливість безперервної роботи, автономного енергозабезпечення та бути захищеними від зовнішніх втручань. На цьому етапі формується первинний відеопотік, що надалі обробляється у проміжному обчислювальному контурі.

Другий рівень – обчислювальний – виконує попередню обробку даних. З метою зменшення обсягів інформації, що передається до центрального вузла, застосовується стискання, сегментація відео, фільтрація шумів, а також шифрування даних відповідно до політик інформаційної безпеки. Для цього залучаються edge-сервери, розміщені поблизу сенсорного рівня. Це дозволяє суттєво скоротити час реакції системи та уникнути перевантаження магістральних каналів зв'язку.

Третій рівень – аналітичний – є ядром технології підтримки прийняття рішень. Тут застосовуються методи штучного інтелекту, зокрема convolutional neural networks (CNN), які забезпечують розпізнавання об'єктів, а також recurrent neural networks (RNN), що дозволяють моделювати часові залежності у відеопотоці. Додатково застосовуються моделі виявлення аномалій (anomaly detection models), які навчаються на основі історичних даних та формують алгоритми ідентифікації підозрілої або небезпечної поведінки. Це можуть бути моделі виявлення падіння людини, залишених предметів, натовпу в забороненій зоні тощо.

Аналітична підсистема також повинна включати механізми самонавчання, щоб адаптуватися до нових умов і сценаріїв. Наприклад, у громадському транспорті система може адаптуватися до типових годин пік, виключаючи хибнопозитивні спрацювання. При цьому вона повинна зберігати здатність до виявлення дійсно небезпечних ситуацій, що відхиляються від норми, включаючи конфлікти, спроби крадіжок або вандалізм.

Інтерфейс управління забезпечує зручну взаємодію оператора з системою. Він має включати візуалізацію відеопотоків, підсвічування критичних подій, систему тривожних повідомлень та рекомендацій щодо дій. Наприклад, у випадку виявлення несанкціонованого входу в заборонену зону система може автоматично запропонувати виклик служби безпеки або поліції, зафіксувати інцидент, зберегти фрагмент відео та внести запис до журналу подій.

Особливу увагу слід приділити обчисленням на периферії (edge computing), які суттєво підвищують ефективність функціонування системи. Виконання аналітики безпосередньо на edge-пристроях дозволяє не лише зменшити затримку, а й покращити рівень автономності. У разі аварійного відключення мережі або центрального сервера система продовжуватиме працювати в локальному режимі, що критично важливо для об'єктів стратегічного значення.

У сучасних реалізаціях таких систем все більше використовуються гібридні моделі, що комбінують edge-аналітику з хмарними технологіями (cloud computing). Наприклад, первинне виявлення події може виконуватись локально, а глибокий аналіз і архівування – на віддаленому сервері. Це дозволяє балансувати між швидкістю обробки, точністю моделей і економічністю рішень.

Інтеграція з іншими інформаційними системами є важливою умовою ефективності запропонованої технології. Система підтримки прийняття рішень має взаємодіяти з базами біометричних даних, системами контролю доступу, реєстрами транспортних засобів, геоінформаційними системами тощо. Це забезпечує ширший контекст для аналізу ситуацій та дає змогу здійснювати перехресну верифікацію інформації.

Управління безпекою даних є критичним аспектом систем відеоспостереження. Потрібно забезпечити конфіденційність, цілісність і доступність відеоданих шляхом застосування методів шифрування, цифрових підписів, політик контролю доступу, журналювання дій користувачів та регулярного аудиту систем. У системах з високими вимогами безпеки варто також реалізовувати функції автоматичного виявлення атак або втручання у відеопотоки.

Ще однією важливою складовою є адаптивність системи до середовища функціонування. Наприклад, в умовах великого міста з високим рівнем шуму та постійною змінюваністю освітлення, система має динамічно регулювати чутливість, частоту кадрів та параметри алгоритмів розпізнавання. Такі можливості забезпечуються за рахунок поєднання сенсорних даних із аналітичними модулями, що самооновлюються.

Для забезпечення масштабованості платформи доцільно використовувати модульну структуру програмного забезпечення, що дозволяє легко оновлювати або замінювати окремі компоненти без порушення роботи всієї системи. Це спрощує технічне обслуговування, адаптацію до нових нормативів та швидке впровадження інновацій.

Реалізація описаної інформаційної технології може істотно підвищити рівень безпеки у місцях масового скупчення людей, транспортній інфраструктурі, навчальних закладах, промислових об'єктах та житлових комплексах. Водночас вона здатна забезпе-

чити більш ефективну реакцію на надзвичайні ситуації, зменшити кількість хибних викликів і підвищити довіру громадян до систем відеомоніторингу.

Удосконалення представленої системи можливе шляхом впровадження технологій глибокого навчання з підкріпленням (reinforcement learning), які дозволяють системі самостійно навчатися приймати оптимальні рішення на основі досвіду взаємодії з навколишнім середовищем. Наприклад, у транспортній інфраструктурі така система може автоматично змінювати правила контролю трафіку або пріоритети сигналів у разі виявлення заторів, аварій чи скупчення пішоходів. Це підвищує адаптивність системи та дозволяє розширити її функціональність за межі традиційного спостереження.

Значна роль у розвитку інформаційної технології для відеоспостереження належить інтеперабельності, тобто здатності ефективно взаємодіяти з іншими цифровими системами – охоронними, екстреними, логістичними, екологічними тощо. Забезпечення міжсистемної сумісності потребує дотримання міжнародних протоколів обміну даними (ONVIF, RTSP, MQTT) та підтримки відкритих API, що дозволяє уникати технологічної ізоляції і полегшує масштабування. Така сумісність особливо важлива в умовах реалізації проєктів Smart City, де відеоспостереження є лише однією зі складових великої інфраструктурної екосистеми.

Крім того, одним з перспективних напрямів є впровадження прогнозової аналітики, яка базується на використанні історичних даних для передбачення потенційних подій, що можуть мати негативні наслідки. Наприклад, система може аналізувати динаміку поведінки у певній локації та на основі шаблонів минулих подій формувати прогноз щодо ймовірності правопорушення або аварійної ситуації. Це дає можливість органам правопорядку та адміністраціям об'єктів не лише реагувати на події, а й запобігати їм завдяки випереджувальним діям.

Не менш важливим є забезпечення етичного аспекту функціонування системи відеоспостереження. Широке впровадження технологій автоматичного розпізнавання облич, поведінкової аналітики та біометричної ідентифікації викликає занепокоєння з боку правозахисників і громадянського суспільства. Тому розробники та впроваджувачі таких рішень повинні дотримуватися принципів прозорості, підзвітності та відповідності чинному законодавству щодо захисту персональних даних (GDPR, Закон України «Про захист персональних даних» тощо).

Важливо також враховувати роль користувача у загальній структурі системи. Хоча автоматизація є ключовим елементом сучасної аналітики, людський фактор залишається визначальним у прийнятті остаточного рішення у складних або непередбачуваних ситуаціях. Тому оператори систем мають бути належним чином підготовлені до взаємодії з інтерфейсом, розуміти логіку роботи аналітичних модулів та вміти коректно трактувати надану інформацію. Це вимагає системного підходу до навчання персоналу, впровадження симуляційних тренажерів і розробки адаптивних навчальних програм.

Висновки. У процесі дослідження було доведено, що сучасні виклики у сфері безпеки потребують принципово нових підходів до організації відеоспостереження, зокрема — переходу від пасивного спостереження до активної підтримки прийняття

рішень. Запропонована інформаційна технологія базується на багаторівневій архітектурі, що включає сенсорний рівень збору даних, обчислювальні вузли з елементами edge-обробки, аналітичні модулі з використанням алгоритмів штучного інтелекту, а також засоби інтерфейсної взаємодії з користувачем. Важливою перевагою такого підходу є здатність системи до функціонування в реальному часі, адаптації до змін середовища, самонавчання, а також інтеграції з іншими цифровими екосистемами. Впровадження технології дозволяє автоматизувати виявлення загроз, оптимізувати ресурси операторів, зменшити кількість хибних спрацьовувань і забезпечити вищу якість реагування на критичні події.

Комплексність розробленої концепції полягає у її здатності об'єднувати технічну, програмну, організаційну та етичну складові функціонування сучасної системи відеоспостереження. У статті обґрунтовано, що поєднання AI-аналітики, edge computing, інтеграційних можливостей з геоінформаційними системами, базами даних, модулями біометрії та контролю доступу створює основу для створення нової генерації безпекових рішень. Представлена інформаційна технологія є перспективною для використання в умовах реалізації концепції «розумного міста», захисту об'єктів критичної інфраструктури, автоматизованих логістичних центрів та об'єктів підвищеного ризику. Подальші дослідження доцільно спрямувати на апробацію моделі в реальних умовах, розробку універсальних протоколів взаємодії та створення нормативного регулювання щодо її впровадження з урахуванням стандартів конфіденційності та захисту персональних даних.

ЛІТЕРАТУРА

1. Alshammari M., Ahmad M.W., Shah S.A.A. Deep learning-based person re-identification and anomaly detection for smart surveillance systems // *IET Image Processing*. – 2023. – Vol. 17, Issue 4. – P. 259–273. – Режим доступу: <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.12720>
2. Pratt I. Artificial Intelligence and Video Surveillance // *Philosophical Archive*. – 2023. – Режим доступу: <https://philarchive.org/archive/PRAAIV-2>
3. Hanwha Vision. Public Surveillance and AI: The Challenges of Balancing Safety and Ethics in Smart Cities // *Hanwha Vision News Center*. – 2024. – Режим доступу: <https://www.hanwhavision.com/vn/news-center/1576882>
4. Luna A., Tortonesi M., Paganelli F. A Cloud-based Architecture for Smart Video Surveillance // *ResearchGate*. – 2017. – Режим доступу: https://www.researchgate.net/publication/320039476_A_CLOUD-BASED_ARCHITECTURE_FOR_SMART_VIDEO_SURVEILLANCE
5. Журомська М.В. Технологічне підґрунтя та виклики відеоаналітики в міському просторі // *Науковий журнал «Інформаційні технології та проектування»*. – 2020. – № 1(8). – С. 44–49. – Режим доступу: http://journal.nitip.com.ua/media/uploads/documents/8_1_20.pdf
6. Вакалюк Т.А. Інформаційні технології інтелектуального відеоспостереження: проблеми та перспективи // *Modern Development of Education and Science*. – 2023. – № 5. – Режим доступу: <https://mdes.khmnu.edu.ua/index.php/mdes/article/view/446>

REFERENCES

1. Alshammari M., Ahmad M.W., Shah S.A.A. Deep learning-based person re-identification and anomaly detection for smart surveillance systems // IET Im-age Processing. – 2023. – Vol. 17, Issue 4. – P. 259–273. – Rezhym dostupu: <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.12720>
2. Pratt I. Artificial Intelligence and Video Surveillance // Philosophical Archive. – 2023. – Rezhym dostupu: <https://philarchive.org/archive/PRAAIV-2>
3. Hanwha Vision. Public Surveillance and AI: The Challenges of Balancing Safety and Ethics in Smart Cities // Hanwha Vision News Center. – 2024. – Re-zhym dostupu: <https://www.hanwhavision.com/vn/news-center/1576882>
4. Luna A., Tortonesi M., Paganelli F. A Cloud-based Architecture for Smart Vid-eo Surveillance // ResearchGate. – 2017. – Rezhym dostupu: https://www.researchgate.net/publication/320039476_A_CLOUD-BASED_ARCHITECTURE_FOR_SMART_VIDEO_SURVEILLANCE
5. Zhuromska M.V. Tekhnolohichne pidgruntia ta vyklyky videoanalyky v miskomu prostori // Naukovyi zhurnal «Informatsiini tekhnolohii ta proiektuvannia». – 2020. – № 1(8). – S. 44–49. – Rezhym dostupu: http://journal.nitip.com.ua/media/uploads/documents/8_1_20.pdf
6. Vakaliuk T.A. Informatiini tekhnolohii intelektualnoho videospostere-zhennia: problemy ta perspektyvy // Modern Development of Education and Science. – 2023. – № 5. – Rezhym dostupu: <https://mdes.khmnu.edu.ua/index.php/mdes/article/view/446>

Received 30.05.2025.

Accepted 03.06.2025.

Information technology for decision support in the field of video surveillance

The article explores the concept of developing a modern information technology system designed to provide effective decision support in the field of video surveillance. Given the increasing volume of video data generated by monitoring systems, especially in urban environments, there is a growing need for high-performance solutions capable of operating in real time. The focus is placed on analyzing technological approaches to video stream processing using artificial intelligence, machine learning methods, edge computing, and cloud-based solutions. The study presents an architectural model of a multi-level information system that includes modules for data collection, preprocessing, analytics, and decision-making. Special attention is given to event detection algorithms and the classification of behavioral patterns, which helps reduce dependence on human intervention during surveillance analysis.

The paper also examines aspects of integrating such systems with other information-analytical platforms, including biometric databases, geographic information systems, and access control systems. The advantages of edge architectures are substantiated, as they reduce video processing latency, enhance system autonomy, and lower the load on central infrastructure. The research findings can be applied to the development of next-generation intelligent security systems, particularly within the framework of the Smart City concept. The proposed approach can be adapted to meet the needs of local authorities, law enforcement agencies, and private sector entities involved in the protection of critical infrastructure. The results

demonstrate the practical value of implementing advanced IT solutions in the domains of security and monitoring.

Keywords: video surveillance, information technology, decision support, security, AI, machine learning, edge computing, data analytics, system integration, automatic detection.

Суковенко Костянтин Георгійович - аспірант кафедри кібербезпеки та комп'ютерно-інтегрованих технологій Дніпровського національного університету ім.Олеся Гончара.

Sukovenko Kostyantyn - postgraduate of Department of Cyber Security and Computer-Integrated Technologies of Dnipro National University Oles Honchar.