

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В ЗАДАЧАХ ВІДЕОСПОСТЕРЕЖЕННЯ ТА МОНІТОРИНГУ

Костянтин Суковенко

ORCID: <https://orcid.org/0009-0002-8109-9382>

Дніпровський національний університет імені Олеся Гончара, Дніпро

Вступ

Постановка проблеми в контексті інформаційної технології підтримки прийняття рішень в задачах відеоспостереження та моніторингу полягає в ідентифікації та розв'язанні ряду викликів, що виникають у процесі використання цих технологій. Багато систем відеоспостереження використовують складні алгоритми для розпізнавання об'єктів та аналізу поведінки, проте, ефективність цих алгоритмів може бути обмежена в умовах обмежених ресурсів, або в складних умовах оточення, що потребує подальшого вдосконалення.

Одним із ключових аспектів є забезпечення точності та достовірності інформації, яка використовується для прийняття рішень. Навіть невеликі помилки у виявленні об'єктів, або аналізі поведінки можуть призвести до серйозних наслідків. Зі збільшенням обсягів зібраних даних зростає і значення етичних та правових аспектів, таких як: захист приватності, використання даних і зберігання інформації. Потрібно знайти баланс між користуванням цими даними та захистом прав людини.

Для більш ефективного прийняття рішень важливо забезпечити інтеграцію систем відеоспостереження з іншими джерелами інформації, такими як: системи датчиків, соціальні медіа, бази даних тощо. Оскільки системи відеоспостереження стають все більш підключеними до мережі, вони стають уразливими перед кібератаками та зовнішнім впливом «третіх осіб», які можуть спричинити фізичне пошкодження обладнання. Забезпечення стійкості до атак та кібербезпеки є ключовим завданням для збереження інформаційної безпеки та недопущення небажаних втручання у процесі прийняття рішень.

Таким чином, створення ефективної та надійної інформаційної технології підтримки прийняття рішень в задачах відеоспостереження та моніторингу вимагає комплексного підходу, що враховує технічні, етичні, правові та кібербезпечні аспекти. Для досягнення цієї мети необхідно забезпечити високу якість та безпеку обробки відеоданих.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Одним із ключових елементів інформаційної технології відеоспостереження є автоматизований відео аналіз. Ця технологія використовує алгоритми штучного інтелекту для розпізнавання об'єктів, аналізу поведінки та виявлення аномалій у відео потоці. Наприклад, системи можуть автоматично виявляти рухливі об'єкти, розпізнавати номерні знаки автомобілів або визначати людську поведінку на вулиці чи в приміщенні. [3]

Здатність обробляти великі обсяги відеоданих у реальному часі є неймовірно важливим пунктом у інформаційній технології підтримки прийняття рішень в задачах відеоспостереження та моніторингу. Завдяки швидкому розвитку технологій обчислювальної техніки та програмного забезпечення, сучасні системи ефективно аналізують великі потоки відеоданих і витягують корисну інформацію для прийняття рішень. Також варто згадати про інтеграцію відеоданих з геопросторовою інформацією. Ця інтеграція дозволяє створювати комплексні системи моніторингу, які забезпечують не лише візуальну інформацію, але й контекстуалізують її у просторі. Наприклад, системи автоматично визначають місцезположення подій на карті, що допомагає в оперативному реагуванні на надзвичайні ситуації. Проте, разом з потужними можливостями інформаційної технології виникають і виклики. Один із найбільших серед них - захист приватності, збір та аналіз великих обсягів відеоданих може порушувати приватність громадян, тому важливо розробляти та застосовувати ефективні заходи захисту даних. Машинне навчання та нейронні мережі є ключовими компонентами сучасних систем відеоаналізу. Шляхом тренування на великих наборах даних, ці алгоритми стають все більш точними і ефективними у виявленні об'єктів та аналізі поведінки на відео. [1-3]

У сучасному світі, де робота стає все більш монотонною та вимагає постійного навантаження, важливо визнати наслідки, які це може мати на якість та ефективність рішень, які приймають люди. Ця проблема виявляється досить актуальною у різних сферах, включаючи виробництво, інженерію, та інші. Постійне навантаження та монотонна робота можуть впливати на психічний стан працівників та їх загальну продуктивність. Втрата концентрації та втома можуть перешкоджати здатності до обґрунтованого прийняття рішень. Довготривала монотонність може призвести до втрати мотивації та інтересу до виконання роботи, що додатково ускладнює процес прийняття рішень. [1]

Крім того, постійна рутинність може призвести до застосування шаблонних підходів до рішень, що у свою чергу може призвести до

втрати гнучкості та неспроможності адаптуватися до нових ситуацій. Недостатність часу для вивчення нових питань чи аналізу альтернативних шляхів також може призвести до недостатності інформації для прийняття обґрунтованих рішень. [1]

Для запобігання цим ризикам, важливо регулярно оптимізувати робочий процес та шукати можливості для вдосконалення. Розвиток інформаційних технологій надає можливість використання різних алгоритмів та методів у такій діяльності. Одним із способів підтримки прийняття рішень є використання систем підтримки прийняття рішень (СППР), які допомагають зменшити вплив навантаження та монотонності на якість прийнятих рішень. [1] Таким чином, урахування ризиків, пов'язаних із постійним навантаженням та монотонною роботою, важливе для забезпечення ефективного та обґрунтованого прийняття рішень у сучасному світі.

Методологія розробки СППР за моделлю швидкого прототипування, запропонована [2], включає такі етапи:

Ідентифікація цілей та завдань: На цьому етапі ретельно уточнюються цілі розробки СППР, планується процес розробки, визначається склад розробників та джерела знань.

Отримання знань: Здійснюється процес передачі знань від експертів до інженера зі знань (когнітолога), що включає в себе накопичення та систематизацію експертних знань.

Концептуалізація (структуризація) знань: На цьому етапі визначається структура отриманих знань про предметну область, що допомагає у подальшому формалізувати ці знання для використання в системі.

Формалізація знань: Етап формалізації передбачає побудову формалізованого представлення концепцій про предметну область на основі обраної (або розробленої) моделі представлення знань.

Реалізація прототипу: На цьому етапі розробляється прототип СППР на базі вибраних або розроблених програмно-технічних засобів.

Тестування результатів реалізації: Етап тестування спрямований на перевірку та оцінку роботи СППР відповідно до реальних вимог та запитів користувачів. [3,4]

Ця методологія забезпечує систематичний та ефективний підхід до розробки СППР, що дозволяє забезпечити якісну та функціональну систему, відповідну потребам користувачів. Використання структурованих методів та інтеграція різноманітних аспектів забезпечують розробку надійних і безпечних СППР, які здатні ефективно підтримувати процес прийняття рішень у різних галузях, який підвищує довіру до системи та її загальну ефективність.

МЕТА ДОСЛІДЖЕННЯ

Розглянути етичні та правові питання, пов'язані з використанням відеоданих, та розробити рекомендації щодо забезпечення захисту приватності та дотримання норм безпеки даних.

Викладення основного матеріалу дослідження

Використання відеоданих в системах відеоспостереження та моніторингу породжує ряд етичних питань, які потребують уваги та вирішення з метою забезпечення захисту приватності та інших прав громадян.

Інформаційна технологія підтримки прийняття рішень (ІТППР) у сфері відеоспостереження та моніторингу є ключовою складовою для оптимізації процесів аналізу, обробки та використання відеоданих. Ця технологія використовується для автоматизації та покращення прийняття рішень на основі інформації, отриманої з відеозаписів. Основна мета цієї технології - забезпечити операторам та системам відеоспостереження потужні інструменти для автоматичного виявлення подій, об'єктів та паттернів у відеопотоці, що допомагає у прийнятті ефективних та обґрунтованих рішень.

Метод використання технологій комп'ютерного зору на основі даних з відеонагляду в поєднанні з системами підтримки прийняття рішень (СППР) є важливим напрямком вдосконалення процесів управління та контролю в різних сферах. Це дозволяє зменшити навантаження на персонал, оптимізувати процеси аналізу та виявлення подій, а також покращує результативність виконання завдань. Технології комп'ютерного зору надають можливість автоматизувати процеси аналізу відеоданих, а СППР допомагають приймати обґрунтовані рішення на основі цієї інформації. [1]

Ключовою складовою використання технологій комп'ютерного зору є використання систем відео аналітики, яка виявляє об'єкти, розпізнає обличчя, виявляє рух та аналізує аномальні події на відеозаписах. Перед тим як комп'ютер може виявити об'єкти на зображенні, вихідне зображення піддається попередній обробці, що включає зменшення шуму та підвищення контрастності. Після цього відбувається виділення особливих ознак, таких як кольори, текстури або форми, та класифікація цих об'єктів на основі навчених моделей. Зокрема, для цих цілей використовуються згорткові нейронні мережі (CNN), які є одним з базових підходів у глибокому навчанні для розпізнавання об'єктів на зображеннях. Такий підхід полягає в застосуванні паттернів для розпізнавання об'єктів на зображеннях. [1-3]

Класифікація зображень є однією з найбільш поширених задач в області комп'ютерного зору. Вона базується на класифікації об'єктів та локалізації їх на зображенні, що дозволяє визначити їх координати та положення на фреймі. Існує багато методів виявлення об'єктів, проте важливими характеристиками є швидкість обробки та якість виявлення. Таким чином, використання технологій комп'ютерного зору в поєднанні з системами підтримки прийняття рішень у сфері відеоспостереження та моніторингу є перспективним напрямком для покращення ефективності та точності виявлення об'єктів, розпізнавання облич та аналізу подій.

Приватність та конфіденційність осіб, що зображені на відео, становлять одне з найбільш важливих етичних питань у контексті використання систем відеоспостереження. Збирання та обробка відеоданих стає джерелом порушення особистої приватності, це в свою чергу, часто викликає серйозні застереження та негативну реакцію громадськості. Проблема захисту приватності осіб на відеозаписах та системах моніторингу постає через можливість використання цих даних для ідентифікації осіб, їх руху та поведінки без їхньої згоди, що є дуже важливим, оскільки в сучасному світі людина не може цього уникнути. Це особливо актуально у випадках, коли відеоспостереження проводиться у публічних місцях, таких як вулиці, парки, аеропорти та інші об'єкти загального користування.

Щоб забезпечити захист приватності осіб на відео, необхідно вжити ряд заходів. По-перше, важливо обмежувати збір та зберігання відеоданих лише до необхідного мінімуму, обмежуючи термін їх зберігання та обробки. Деякі системи вже використовують технології анонімізації або маскуванню обличчя для захисту приватності осіб, зображених на відео. Додатково, дуже важливим аспектом є регулярна оцінка ризиків порушення приватності та вдосконалення технологій захисту даних для мінімізації можливих загроз.

Спрямованість та масштаб відеоспостереження є ключовими аспектами, які впливають на етичність та ефективність використання систем відеоспостереження. Вони визначають, наскільки точно та широко відбувається моніторинг певних територій або об'єктів та які групи людей стають об'єктом спостереження. Спрямованість відеоспостереження визначається цілями та завданнями, які передбачаються застосовувати систему, наприклад, вона може бути спрямована на забезпечення безпеки громадських місць, контроль за дотриманням правил на робочих майданчиках, або використовуватися для виявлення злочинців чи запобігання крадіжкам. Важливо, щоб спрямованість відеоспостереження була чітко визначена та обмежена відповідно до завдань, що стоять перед системою. Масштаб же

відеоспостереження, визначає, наскільки великою або обмеженою є територія, що піддається спостереженню, а також які об'єкти або особи знаходяться під наглядом. Тому масштаб може варіюватися від великих публічних майданчиків до вузьких промислових коридорів. Масштаб відеоспостереження також може бути тимчасовим, наприклад, під час масових заходів або екстрених ситуацій, або постійним, для постійного моніторингу конкретних місць.[4]

Етичні аспекти спрямованості та масштабу відеоспостереження включають забезпечення пропорційності між необхідністю спостереження та захистом приватності, а також запобігання випадковому або систематичному спостереженню за конкретними групами людей або об'єктами. Наприклад, система великого масштабу відеоспостереження на громадському майданчику повинна бути спрямована на загальну безпеку та запобігання злочинності, а не на систематичне відстеження конкретних осіб без обґрунтованих підстав.

Розглянувши приватність, конфіденційність, спрямованість та масштаб важливо зрозуміти що кожен з цих пунктів має об'єднуватися між собою, до того ж важливо згадати про транспарентність та інформованість громадян. Транспарентність та інформованість громадян про наявність та функціонування систем відеоспостереження є необхідними складовими для забезпечення етичного використання цих технологій. Особи що знаходяться під впливом цих технологій мають право знати, що їхнє оточення може бути об'єктом відеоспостереження та які дані можуть бути зібрані, збережені та використані. Перш за все, важливо забезпечити транспарентність відносно розташування камер відеоспостереження та їх функціонування. Інформація про місце розташування камер, їх орієнтацію та обсяг спостереження повинна бути доступною для громадськості. Це може бути досягнуто через встановлення видимих позначень на місцях, де відбувається відеоспостереження, а також через публікацію інформації на веб-сайтах муніципалітетів або організацій, що відповідають за встановлення камер.

Далі, важливо забезпечити інформованість громадян про правила використання та обробки відеоданих. Громадяни повинні мати змогу отримати інформацію про те, як вони можуть впливати на процеси відеоспостереження та їх власні дані.

ВИСНОВКИ

Інформаційна технологія підтримки прийняття рішень в задачах відеоспостереження та моніторингу відіграє важливу роль у забезпеченні безпеки та ефективності в різних сферах життя. З розвитком

технологій штучного інтелекту, обробки великих даних та машинного навчання, ми можемо очікувати подальшого покращення функціональності та ефективності цих систем. Проте, важливо також враховувати етичні та правові аспекти, забезпечуючи захист приватності та дотримання норм безпеки даних. Розумне поєднання технологій та правового регулювання допоможе забезпечити оптимальний баланс між забезпеченням безпеки та захистом особистої свободи.

З метою забезпечення захисту приватності осіб на відео, важливо вживати ряд заходів. Слід обмежувати збір та зберігання відеоданих лише до необхідного мінімуму, а також обмежувати термін їх зберігання та обробки.

Захист приватності осіб на відео, вимагає комплексного підходу, що поєднує технологічні, організаційні та правові заходи. Лише таким чином можна забезпечити баланс між безпекою та приватністю. Дуже важливо ретельно обмірковувати та обмежувати спрямованість та масштаб відеоспостереження з етичних позицій, забезпечуючи баланс між безпекою та захистом прав та приватності громадян.

Щоб забезпечити етичне використання відеоспостереження, важливо забезпечити пропорційність між необхідністю спостереження та захистом приватності, а також забезпечити транспарентність та інформованість громадян про функціонування систем відеоспостереження. Тільки шляхом узгодженого застосування цих принципів можна забезпечити ефективно та етично використання відеоспостереження в сучасному суспільстві.

Посилання

1. Романець, В., & Бісікало, О. (2023). Information technology in customer service: use of computer vision and decision support systems. *SWorldJournal*, 1(21-01), 65–72. <https://doi.org/10.30888/2663-5712.2023-21-01-046>

2. Субботін, С. О., Олійник, А. О., & Гофман, Є. О. (2012). У Інтелектуальні інформаційні технології проектування автоматизованих систем діагностування та розпізнавання образів (с. 317). м. Харків ТОВ «Компанія Сміт».

3. Пустоваров, В. В. (2021). Інформаційна технологія розробки системи підтримки прийняття рішення про розпізнавання будівель на космічних та аерофотознімках. (с. 26). Черкаси.

4. Пустовіт, Я., & Гбур, З. (2024). Аналіз існуючих стратегій у державному управлінні щодо використання штучного інтелекту в обороні. Успіхи і досягнення у науці, (1 (1)). [https://doi.org/10.52058/3041-1254-2024-1\(1\)-172-185](https://doi.org/10.52058/3041-1254-2024-1(1)-172-185)