


УДК 351.74:[621.397:004.032.26](477)«364»

DOI: <https://doi.org/10.32631/pb.2024.1.07>

ДМИТРО ОЛЕГОВИЧ ЖАДАН,


*Харківський національний університет внутрішніх справ,
науково-дослідна лабораторія з проблем інформаційних
технологій та протидії злочинності у кіберпросторі;*

 <https://orcid.org/0000-0001-8184-4800>,

e-mail: dmttro.zhadan23@gmail.com;

МИКОЛА ВОЛОДИМИРОВИЧ МОРДВИНЦЕВ,


*кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
науково-дослідна лабораторія з проблем інформаційних
технологій та протидії злочинності у кіберпросторі;*

 <https://orcid.org/0000-0002-7674-3164>,

e-mail: lukoly@ukr.net;

ДМИТРО ВАЛЕНТИНОВИЧ ПАШНЄВ,

*кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
науково-дослідна лабораторія з проблем інформаційних
технологій та протидії злочинності у кіберпросторі;*

 <https://orcid.org/0000-0001-8693-3802>,

e-mail: dvpashnev@gmail.com

ВІДСТЕЖЕННЯ ПРОТИПРАВНИХ ДІЙ ЗА ДОПОМОГОЮ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ: ОГЛЯД СУЧАСНОГО СТАНУ ДОСЛІДЖЕНЬ

Розглянуто сучасний стан досліджень використання нейронних мереж в умовах воєнного стану для ідентифікації вчинення правопорушниками протиправних дій, попередження актів тероризму, боротьби з диверсійними групами в містах, відстеження зброї та контролю за дорожнім рухом. Проаналізовано методи розпізнавання протиправних дій, зброї, облич та порушень правил дорожнього руху за допомогою камер відеоспостереження. Запропоновано впровадження досліджених методів у роботу «розумних» систем відеоспостереження в населених пунктах України.

Найбільш дієвим засобом для зменшення кількості правопорушень є невідворотність юридичної відповідальності, тому багато зусиль у правоохоронній сфері спрямовано на їх попередження. Поряд із забезпеченням публічного порядку патрульною поліцією відеоспостереження є дієвим способом запобігання протиправній діяльності в суспільстві. Збільшення зони покриття камер та їх кількості сприяє забезпеченню публічної безпеки там, де ці камери використовують. Але збільшення кількості камер створює іншу проблему – великі обсяги відеоданих, які потрібно обробляти. Для вирішення проблеми обробки відеоданих використовують різні методи, найбільш сучасним з яких є використання штучного інтелекту задля фільтрації великого обсягу даних із відеокамер, застосування різноманітних алгоритмів їх обробки. Можливість одночасно обробляти відеодані з багатьох камер відеоспостереження без участі людини не лише сприяє забезпеченню публічної безпеки, а й покращує роботу патрульної поліції. Впровадження «розумних» систем відеоспостереження дозволяє проводити моніторинг ситуації у громадських місцях цілодобово, навіть якщо в цьому районі відсутній наряд поліції.

У розглянутих дослідженнях систем відеоспостережень для відстеження протиправних дій, злочинців та зброї використовують нейронні мережі, зокрема MobileNet V2, YOLO, mYOLOv4-tiny, навчання яких проводиться на великих обсягах відео- та фотоданих. З'ясовано, що раніше нейронні мережі потребували великої обчислювальної потужності, а зараз вони можуть застосовуватися в системах Інтернету речей та смартфонах, і це сприяє тому, що для моніторингу ситуації можна залучати більше пристроїв відеоспостереження.

Ключові слова: відеоспостереження, штучний інтелект, нейронні мережі, безпека, відстеження зброї, боротьба з тероризмом.

Оглядова стаття

ВСТУП. Стрімкий розвиток науки допомагає у вирішенні багатьох питань, одним з яких є боротьба зі злочинністю. Окрім допомоги у вирішенні надскладних завдань, пов'язаних із визначенням особи, яка скоїла злочин, не менш значною є робота з попередження неправомірних дій правопорушників. Вивченню результатів упровадження систем відеоспостереження присвячено чимало робіт. Так, у деяких роботах зазначається, що впровадження камер відеоспостереження не принесло значних результатів (Gerell, 2016; Lim, 2016). В інших працях дослідники дійшли висновку, що використання камер відеоспостереження сприяє зменшенню злочинності. Зокрема, дослідження А. Густава (2017) показує зниження рівня злочинності на вулицях та станціях метро на 24–28 %. У своїй праці Дж. Раткліфф, Т. Танігучі та Р. Тейлор (2009) зауважують, що рівень злочинності в місті Філадельфія, штат Пенсильванія, США зменшився на 13 % після впровадження камер відеоспостереження. У дослідженні Е. Пізи, Б. Велша, Д. Фаррінгтона й А. Томас (2019) зазначається, що використання систем відеоспостереження сприяє значному зменшенню злочинності, а найбільший позитивний вплив спостерігався в місцях паркування автомобілів. У своїй роботі С. Маклін, Р. Ворден і М. Кім (2013) проаналізували впровадження камер відеоспостереження в місті Скенектаді, штат Нью-Йорк, США та зробили висновок, що це сприяло покращенню безпекової ситуації в районі ведення відеоспостереження. Вивчення аналогічної ситуації в місті Катовіце Республіки Польща показало зниження рівня злочинності з введенням «розумної» системи відеоспостереження (Socha, Kogut, 2020).

Таким чином, упровадження інтелектуальних систем відеоспостереження сприяє зниженню рівня злочинності, тому з'являється необхідність у подальшому вдосконаленні, розвитку та ширшому впровадженні вказаних систем. Відстеження поведінки людей, виявлення зброї, контроль дорожнього руху – все це та багато іншого можуть виконувати інтелектуальні системи відеоспостереження з розробкою відповідних нових алгоритмів. Не менш важливим є оптимізація роботи таких систем з можливістю використання пристроїв обробки відеоданих з меншими вимогами до обчислювальної спроможності комп'ютерних систем. Все вищезазначене обґрунтовує актуальність теми дослідження.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Метою роботи є аналіз сучасного стану наукових

розвідок у галузі відеоспостереження, систем штучного інтелекту (далі – ШІ), спрямованих на виявлення протиправних дій та зброї, визначення подальших напрямів досліджень для збільшення ефективності забезпечення публічного порядку та впровадження цих засобів в Україні задля забезпечення безпеки громадян. Досягнення поставленої мети передбачає виконання такого завдання, як аналіз сучасного стану наукових досліджень у галузі відеоспостереження, можливостей застосування сучасних досліджень у сфері ШІ для забезпечення публічної безпеки в Україні.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. З метою повного, всебічного, узагальнюючого дослідження вказаної проблеми було використано кілька методів наукового пізнання. З використанням методу аналізу, що являє собою метод розділення цілого на складові, було проаналізовано механізми використання ШІ в системах відеонагляду. За допомогою методу порівняння вивчено розробки в галузі відеоспостереження та результативність їх роботи. Методом дедукції, що є методом логічного доведення, зроблено висновок щодо впровадження досліджень у сфері ШІ для забезпечення публічної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Використання нейронних мереж, здатних ідентифікувати події та різні предмети, у системах відеоспостереження може покращити їхню продуктивність. Виходячи з цього, розробка нейронних мереж, що можуть виявляти протиправні дії, зброю або злочинців, є дуже важливим аспектом забезпечення публічної безпеки. Тому дослідники пропонують упровадження системи для автоматичної ідентифікації злочинців за допомогою розпізнавання обличчя з відеоматеріалів, знятих камерами відеоспостереження. Система працює з трьома базами даних (далі – БД) (Aroorva et al., 2019). Перша БД містить дані про громадян: зображення та унікальні ідентифікатори всіх громадян, які проживають у країні. Друга – локальна БД списку спостереження, в якій містяться зображення (мінімум 10) і деталі (унікальний ідентифікатор, ім'я, стать, релігія, скоєні злочини тощо) кожного злочинця, який проживає в країні. І третя – міжнародна БД списку спостереження, до якої входять зображення (мінімум 10) і деталі (унікальний ідентифікатор, ім'я, стать, релігія, скоєні злочини тощо) злочинців, які не є громадянами країни. Для розпізнавання обличчя відео з камер спостереження розділяється на кадри, і якщо в кадрі виявляється обличчя, то

воно попередньо обробляється. Далі за допомогою каскаду Хаара та гістограми локальних бінарних шаблонів проводиться вилучення особливостей обличчя, за якими воно порівнюється з обличчями в БД громадян країни. Якщо знайдено збіг, то результат додатково перевіряється за БД місцевих злочинців. У разі позитивного результату поліцейським надсилається повідомлення з усіма деталями та часом потрапляння особи в поле зору відеокамери. Якщо особу не виявлено в БД громадян країни, її зображення порівнюють з міжнародною БД. У разі виявлення збігу поліцейським направляється повідомлення з даними про особу та часом її перебування під спостереженням відеокамери.

Модулі, які використовують для розпізнавання обличчя на відеозображеннях, отриманих з камер спостереження в реальному часі, – це cv2 та NumPy. Оскільки відеоряд зображень має формат GIF, а модуль OpenCV не підтримує цей формат, використовується модуль зображень з PIL (Python Imaging Library) для зчитування зображень у відтинках сірого. Для зберігання даних використовується масив NumPy. Для розпізнавання обличчя застосовують гістограму локальних бінарних шаблонів (LBPН), яка надається модулем OpenCV. LBPН фокусується на вилученні локальних особливостей із зображення. Алгоритм розпізнавання обличчя шукає конкретні особливості Хаара і складається з чотирьох кроків. Перший крок – це вибір функції Хаара. Після надходження даних (зображень) у систему починається процес отримання об'єктів Хаара. Функції Хаара, подібні до вікон, розміщуються на зображенні для обчислення однієї функції. Далі йде другий крок – відбувається процес створення цілісного зображення. Для цього застосовується концепція інтегрального зображення, що полягає в тому, щоб знайти суму пікселів у кожному вікні функції, для чого здійснюється обчислення на основі чотирьох кутових значень. Потім розпочинається третій крок відбору найкращих функцій, для чого використовується алгоритм машинного навчання AdaBoost, який вибирає лише ті функції, які мають достатню ймовірність класифікації. На четвертому кроці використовується каскадний класифікатор, він групує об'єкти в окремі підвікна та визначає, чи є підвікно обличчям. Якщо воно не є обличчям, то воно буде видалене разом з функціями, в іншому разі підвікно переходить до наступних етапів роботи з БД.

У роботі Р. Війейкіса, В. Раудоніса та Г. Дервініса (2022) запропонована архітектура для виявлення насильства за допомогою камер

відеоспостереження. Основна мета запропонованої моделі – підтримувати продуктивність на рівні з найсучаснішими моделями виявлення насильства, водночас зменшуючи обчислювану складність для розгортання на периферійних пристроях малої потужності (<20 Вт).

Запропонований алгоритм поділяється на три етапи: 1) екстрактор просторових характеристик (розподілений у часі U-Net); 2) екстрактор часових характеристик; 3) класифікатор.

Модель отримує пакет із 30 відеокадрів з камери спостереження, що відповідає фрагменту відеозапису тривалістю 1 секунда. Цей пакет передається для обробки мережі, яка використовує архітектуру MobileNet V2, подібну до U-Net, як шифрувальник, що застосовується для вилучення статичних просторових характеристик одного кадру послідовно розподіленим у часі способом. Отримана черга характеристик кадрів передається на другий етап для виокремлення часових характеристик. Довга короткочасна пам'ять (LSTM) використовується для отримання інформації з послідовних фрагментів відео. Маючи цю інформацію, двошаровий класифікатор, заснований на щільних шарах, визначає події як насильницькі або ненасильницькі.

Використання попередньо підготовленої архітектури MobileNet V2 пов'язане з меншою кількістю обчислень та параметрів, що записуються, при цьому зберігається гарна точність.

Кодер, що використовується в моделі, попередньо навчений на наборі даних ImageNet. Це покращує ефективність навчання за рахунок нерозмічених просторових даних у кадрі. Крім того, обстановка навкруги, записана з камер відеоспостереження, відрізняється, тому забезпечення ефективного та дієвого екстрактора загальних просторових характеристик зменшує складність навчання до порівняння цих характеристик у часі з випадками насильницької поведінки. Використання складного реального масиву даних з камер відеоспостереження на основі RWF-2000 показало середню точність $0,82 \pm 2\%$ та прецизійність $0,81 \pm 3\%$.

Не викликає сумніву, що одним із важливих напрямів роботи правоохоронних органів є контроль обігу зброї в Україні. Вчасне виявлення зброї може запобігти вчиненню злочинів та врятувати життя. Незаконний обіг зброї в Україні є одним із найприбутковіших напрямів злочинної діяльності. І вирішення цієї проблеми набуло актуальності саме у воєнний час. Отже, виникає необхідність досліджувати та впроваджувати нові способи і методики моніторингу обігу зброї. Допомогти в цій

справі можуть камери відеоспостереження з інтегрованим ШІ, що зможуть визначати наявність зброї в людини. Так, О. Колесницький, Є. Янковський, І. Денисов та І. Арсенюк (2023) у своїй роботі представили інформаційну технологію виявлення озброєних людей, для чого використовували нейронну мережу YOLO. Нейронна мережа складалась із трьох частин: хребта (backbone), шиї (neck) та голови (head). Хребет – модифікована версія архітектури CSPDarknet53, що містить модуль SPPF (Spatial Pyramid Pooling Fusion), який слугує для об'єднання вхідних карт ознак. Шийна частина – комбінація FPN (мережа піраміди ознак) і PAN (мережа агрегації шляхів). Головна частина керувала призначенням завдань для порівняння позитивних та негативних зразків. Запропонована програма мала достовірність на рівні 98,51 %, влучність – 97,13 % та повноту – 96,9 %.

Крім того, було проведено дослідження інтеграції методів глибокого навчання з архітектурою програмно-конфігурованих мереж для виявлення зброї в режимі реального часу (Fathy, Saleh, 2022). Запропонована модель складається з чотирьох основних компонентів: рівень пристроїв Інтернету речей, рівень периферійних обчислювальних пристроїв, рівень базової програмно-конфігурованої мережі, рівень додатку QoS (набір методів для управління ресурсами пакетних мереж). IP-камери відеоспостереження (рівень пристроїв Інтернету речей) генерують безперервний відеосигнал з контрольованої ділянки, який потім передається на одноплатний комп'ютер Raspberry Pi, що реалізує моделі ШІ глибокого навчання (периферійні обчислювальні пристрої). Результатом роботи Raspberry Pi є невеликий відеофайл, що містить кадри з виявленою зброєю. Він направляється через комутатори програмно-конфігурованої мережі OpenFlow, що реалізують адаптивний алгоритм QoS. Комутатор OpenFlow класифікує трафік на основі номера порту призначення та розподіляє пропускну здатність для різних класів трафіку на основі таблиці лічильників, встановленої RYU контролером у кожному комутаторі. Таблиця лічильників складається із записів лічильників, які визначаються для кожного потоку. У своєму наборі інструкцій запис потоку може визначити лічильник, який відстежує та контролює сукупну швидкість всіх входів потоку, до яких він підключений. Пакети, що надходять, пересилаються до лічильника, який зазначено відповідним записом таблиці потоку. Налаштування таблиці лічильників надають пріоритет відеофайлам, які містять зброю, для забезпечення швидкої

доставки через комутатор OpenFlow до органів влади для зменшення жертв або запобігання злочинам.

В одному з досліджень було запропоновано метод ефективної класифікації, визначення місцезнаходження та виявлення різних типів зброї та ножів у реальному часі, заснований на ресурсно-обмеженій та легкій згортковій нейронній мережі (Ingle, Kim, 2022).

Багатокласова архітектура згорткової нейронної мережі (MSD-CNN) виявлення підкласів має дві повністю з'єднані гілки, кожна з яких виконує конкретне завдання класифікації. Оскільки є дві окремі гілки, то гілка на першому краю відповідає за класифікацію ненормальних зображень, таких як пістолети, автоматичні та напіваавтоматичні гвинтівки, ножі, кухонні ножі та армійські ножі, а гілка другого краю – за класифікацію звичайних зображень, наприклад ходьба, їзда на велосипеді, робота в офісі та робота по дому.

Методологія MSD-CNN складається з класифікації кадрів, локалізації та виявлення. Виявлення кадру в основному використовується для точного визначення розташування та розміру об'єкта на зображенні, що є важливим для класифікації кадру. Положення й масштаб об'єкта визначаються локалізацією кадру. Після визначення архітектури алгоритм навчання нейронної мережі використовує в основному покрокове обчислення коефіцієнтів кожного визначеного рівня.

Для виявлення об'єктів використовувалися мультиракурсні камери. Через те, що модель MSD-CNN – це доволі легка мережа, яка дозволяє створити декілька екземплярів MSD-CNN, це так само допомагає виявляти аномальний об'єкт на кількох камерах одночасно без збільшення витрат на обчислення. Кожен екземпляр відповідає за виявлення, класифікацію та локалізацію об'єкта у відповідному кадрі.

Набір даних для аномальних та нормальних класів отримували з набору даних ImageNet та IMFDB. Загалом було отримано 75 000 зображень зброї. Із загального набору даних 75 % використовувалось для навчання, 15 % – для перевірки, 10 % – для тестування. Найкраща точність запропонованого методу для виявлення зброї становила 97,5 % в базі даних ImageNet та IMFDB, 90,5 % – на відкритій базі даних зображень та 90,7 % – на наборі даних з мультиракурсних камер.

Ще одним напрямом діяльності правоохоронних органів, у якому доцільне застосування методів ШІ, – це безпека дорожнього руху. У роботі Д. Сватюка, О. Сватюк та О. Белея (2020) розроблено алгоритм програми

розпізнавання об'єктів у відеопотоці. За допомогою програми та пристрою з операційною системою Android 7.0 проводиться отримання відеопотоку для виявлення транспортного засобу (далі – ТЗ) та його номерного знака. Обробку та аналіз отриманих кадрів проводили в бібліотеці Open ALPR та за допомогою згорткової нейронної мережі типу SSD. Навчання моделі проводилось за допомогою набору даних COCO (Common Objects in Context), але зі зменшеною до однієї кількістю вхідних класів для адаптації під розпізнавання номерних знаків. Наданий у роботі алгоритм та програма на його основі можуть використовуватись патрульною поліцією для аналізу транспортних потоків та виявлення ТЗ, що перебувають у розшуку. При виявленні номерних знаків точність методу становила 98,2 % на мобільному пристрої, а час обробки одного кадру – не більше 0,05 секунд. При розпізнаванні хаотичних зображень точність становила 80 %, швидкість – 1,43 секунди (для відео тривалістю 30 секунд на обчислювальному модулі з GPU).

У своїй роботі Ч. Лін і Ц. Цзян (2022) запропонували систему інтелектуального моніторингу дорожнього руху, засновану на принципі YOLO та згортковій нечіткій нейронній мережі (CFNN), яка записує інформацію про обсяг дорожнього руху і тип ТЗ. Для класифікації ТЗ пропонуються дві моделі – CFNN і Vector-CFNN, а також метод об'єднання мережевого відображення. У експериментах запропонований метод досяг точності 90,45 % на відкритому наборі даних Пекінського технологічного інституту.

Схема інтелектуальної системи моніторингу дорожнього руху складається з кількох етапів. Спочатку в режимі реального часу отримують зображення з камер дорожнього руху. Далі модель mYOLOv4-tiny використовується для визначення положення ТЗ. Для вирішення проблеми повторного запису одного й того ж ТЗ у різних кадрах уведено алгоритм розрахунку для відстеження, тобто ТЗ признається однаковий ідентифікатор у різних кадрах. Перед виконанням алгоритму розрахунку віртуальна зона виявлення цільового ТЗ (зона у відео, в якій проводиться виявлення) екранується, щоб зменшити обчислювальне навантаження. На останньому етапі показники ТЗ, що проходять через зону віртуального виявлення, обчислюються і класифікуються.

Описаний метод виявлення об'єктів YOLO можна використовувати для ідентифікації ТЗ та інформації про його місцезнаходження за одним зображенням. Щоб прибрати можливість повторної ідентифікації одного й того ж

ТЗ у різних кадрах, було запропоновано спеціальний метод ідентифікації. Це метод багатоб'єктного підрахунку (Bewley et al., 2016), який використовує інформацію про положення автомобіля з попереднього кадру, отриманого за допомогою методу виявлення автомобіля, для прогнозування його положення в поточному кадрі шляхом застосування фільтра Калмана. Потім фактичне положення ТЗ, виявлене в поточному кадрі, та реальне положення ТЗ, оцінене за допомогою фільтра Калмана, використовують для розрахунку їх перетину з урахуванням різниці відстані. Нарешті, для порівняння ТЗ із метою їх відстеження застосовують Угорський алгоритм.

Ще в одній роботі досліджено можливість використання камер відеоспостереження для розпізнавання номерних знаків та повторної ідентифікації ТЗ (González-Cepeda, Ramajo, Armingol, 2022). Описана модель має три модулі: виявлення об'єктів, розпізнавання номерних знаків, повторна ідентифікація ТЗ. Модуль виявлення об'єктів являє собою YOLOv5, модуль, відповідальний за виявлення та розпізнавання номерного знака, – це YOLOv5 multi-stage. Для повторної ідентифікації ТЗ використовують FastReid. Використання YOLOv5 задля розпізнавання номерних знаків ТЗ зумовлене швидкістю його роботи, що дає можливість розпізнавання в режимі реального часу. Виявлення номерного знака проводиться двома згортковими нейронними мережами: перша розпізнає ТЗ, друга – номерний знак. Повторна ідентифікація ТЗ базується на вилученні таких характеристик, як форма, перспектива, колір. Після виявлення ТЗ та його номерного знака загальне зображення обрізають для вилучення зображення ТЗ і проводиться повторна ідентифікація. Для розпізнавання ТЗ навчання моделі проводилось на двох наборах даних, що відтворюють реальні сценарії використання. Перший набір даних був розмічений вручну. Він складався з 2 035 зображень, 2 531 номерного знака та понад 15 000 символів та масштабом зображення 640×640 пікселів.

Повторна ідентифікація ТЗ виконувалась за допомогою FastReid, що вже має різні попередньо підготовлені та оптимізовані архітектури, а як основу навчання застосовували EfficientNet з різними стратегіями навчання.

Загалом розроблена у вказаній роботі модель відслідковування номерів ТЗ та проведення їх ідентифікації мала точність 93,1 % при виявленні номерного знака та 98,4 % – при виявленні ТЗ.

Не менш важливими є дослідження методів та способів оптимізації нейронних мереж.

Так, у роботі Є. Зінов'єва та І. Арсенюка (2020) запропоновано метод зі зниження вимог до обчислюваних ресурсів без великих втрат точності за допомогою використання додаткового проміжного шару згортки. Дослідники вивчали оптимізацію роботи згорткових нейронних мереж для розпізнавання емоцій людини. За результатами дослідження, додавання проміжного згорткового шару допомогло зменшити вимоги до обчислювальних ресурсів. Точність системи становила 90 % на відформатованому наборі даних та 64 % – на невідформатованому.

Також не менш значущими є дослідження, спрямовані на подолання проблеми перспективних спотворень геометричних параметрів, які викликані розташуванням камер з неідеальними кутами. У своїй роботі Д. Марчук (2023) дослідив використання афінних перетворень для корекції зображень, які отримують з камер відеоспостереження з урахуванням геометричних параметрів у реальному часі, розробив математичну модель для перетворення зображення й запропонував метод, що спрощує виявлення, сегментацію та розпізнавання об'єктів.

Розробка підходів розпізнавання об'єктів є надзвичайно важливим завданням через те, що така можливість надає чимало варіантів її застосування. У роботі К. Кірей (2021) представлена система розпізнавання об'єктів навколишнього світу. Створено декілька моделей згорткової нейронної мережі: *precise*, *precise2* та *fast*. Навчання моделей проводили в СОСО. Запропонована система аналізує одразу ціле зображення та виконує передбачення за один цикл, що значно підвищує її швидкість. Найбільш точною є модель *precise*. *Precise2* має трохи меншу точність, проте більшу швидкість. Модель *fast* в рази швидше, ніж *precise2*, але має меншу точність.

Систему виявлення аномалій у системі відеоспостереження досліджували В. Ле та Й. Кім (2023). Вони запропонували мережу для виявлення аномалій у відео з використанням підходу прогнозування наступного кадру. Вхідними даними є послідовність кадрів у відео, а мережа намагається передбачити наступний кадр. Загальну структуру моделі становлять кодер і декодер: перший призначений для захоплення інформації про зовнішній вигляд і рух у вхідних відеокadraх, другий – для прогнозування наступного кадру за допомогою вилучених просторово-часових характеристик, обчислених кодером. Кодер за допомогою глибокої та широкої згорткової нейронної мережі виокремлює із заданої послідовності ка-

дрів високорівневі ознаки. Для використання просторової та часової інформації відеокadрів остання карта ознак, отримана з глибокої згорткової нейронної мережі, пропускається через дві гілки: просторову та часову. У часовій гілці часовий зсув застосовується для моделювання часових характеристик у кількох вхідних кадрах, тоді як отримані характеристики вхідних кадрів об'єднуються для підтримки просторової інформації у просторовій гілці. Потім вихідні дані двох гілок комбінуються за допомогою поелементної суми та подаються в декодер для прогнозування відповідного наступного кадру. Комбіновані характеристики пропускаються через декодер для відновлення деталей та просторової роздільної здатності прогнозованого кадру. Кожен рівень декодера є послідовністю блоків, враховуючи зворотну розгортку, пакетну нормалізацію та функцію активації зрізаного лінійного вузла (ReLU). Для використання каналу зв'язку функцій канална увага застосовується після кожного блоку зворотної розгортки. Крім того, вхідні характеристики каналної уваги об'єднуються з відповідними видобутими глибокою згортковою нейронною мережею низькорівневими характеристиками, які мають однакову просторову роздільну здатність. Потім виконується зворотна розгортка для збільшення дискретизації функції до роздільної здатності вхідного кадру.

Операція часового зсуву в часовій гілці виконується вздовж часового виміру. Частина каналів зсувається до наступного кадру, зберігаючи частину, що залишилася. Далі ознака поточного кадру поєднується з ознакою попереднього.

У просторовій гілці ознаки, отримані з глибокої згорткової нейронної мережі, агрегуються по кадрах. Для зменшення складності обчислень застосовують згортку 1×1 до комбінованих функцій, щоб зменшити кількість каналів, оскільки агреговані функції містять їх велику кількість.

Мета запропонованої мережі – передбачити майбутній кадр \hat{I}_{t+1} з послідовності $\{I_1, I_2, \dots, I_t\}$. Оскільки кожен кадр складається з багатьох пікселів і кожен піксель має інтенсивність, то обмеження інтенсивності та градієнта можуть бути важливим фактором для мінімізації помилки передбачення. Таким чином, подібність усіх пікселів у просторі RGB може бути забезпечена обмеженням інтенсивності, яке порівнює кожне значення пікселя між прогнозованим кадром і базовим кадром.

Для виявлення аномалій використовували оцінку аномалії $S(t)$, яка застосовується для

вимірювання різниці між основним істинним кадром І та прогнозованим кадром \hat{I} . Результати роботи запропонованого методу були такими: 97,4 % – для UCSD Ped2, 86,7 % – для CUNK Avenue і 73,6 % – для набору даних ShanghaiTech.

Також поза увагою не залишаються системи відстеження руху об'єктів у реальному часі.

У дослідженні колективу авторів (Alotaibi et al., 2022) було подано новий алгоритм гармонійного пошуку на основі обчислюваного інтелекту для виявлення та відстеження об'єктів у реальному часі в системах відеоспостереження задля забезпечення безпеки у громадських місцях. Техніка, описана в цій роботі, містить покращений модуль виявлення об'єктів на основі Refinedet та використовує алгоритм Adagrad оптимізації гіперпараметрів моделі. Крім того, використовується алгоритм гармонійного пошуку з моделлю двосторонньої опорної векторної машини для класифікації об'єктів, що призводить до покращення результатів фіксації. Аналіз продуктивності моделі проводили за допомогою еталонного набору даних UCSD, який складається з двох випробувальних стендів: Pedestrian-1 і Pedestrian-2. Випробувальні стенди Pedestrian-1 і Pedestrian-2 склалися з 360 кадрів тривалістю 12 секунд. Загалом запропонована модель досягла середньої точності 91,51 % та 94,32 % згідно з тестовими наборами даних Pedestrian-1 і Pedestrian-2.

Ефективним варіантом підвищення публічної безпеки є широке залучення громадян до інформування правоохоронних органів про підозрілі події та осіб. Так, С. Василенко та С. Гнатюк (2022) пропонують створити застосунок, який може встановити на свій телефон кожний громадянин країни і за допомогою якого буде проводитись відео- та фотофіксація правопорушень. Відео- та фотодані, отримані з телефону, будуть надсилатися до органів поліції. Використання такого застосунку дозволить розширити зону спостереження за рахунок користувачів смартфонів, що може допомогти поліції в забезпеченні публічної безпеки.

Вивчення зазначених вище праць свідчить, що для побудови високоякісних систем відеоспостереження, здатних розпізнавати протиправні дії, контрольовані об'єкти та предмети або розшукуваних осіб, застосовують різні модулі, в основі архітектури яких лежать принципи ШІ, зокрема MobileNet V2, YOLO, mYOLOv4-tiny тощо. Використовуючи ж великі БД із фото- та відеоданими, проводиться ма-

шинне навчання нейронних мереж для розвитку їх можливостей у виявленні шуканих об'єктів або осіб. Сукупність всіх цих технологій, а також методів їх оптимізації для використання у пристроях малої потужності є сьогодні основними напрямками розвитку відеоспостереження. Також не зайвим буде згадати широкий вжиток IP-камер відеоспостереження, які зараз встановлюються в багатьох містах. Розробка більш оптимізованих та розвинутих нейронних мереж дозволить обробляти ще більшу кількість інформації з камер відеоспостереження для забезпечення якомога більшого рівня безпеки населення.

Як зазначає у своїй роботі О. Острогляд (2020), запобігання корисливим злочинам базується на покращенні численних аспектів, одним з яких є оснащення вулиць системами відеоспостереження. Крім того, деякі дослідники зауважують на необхідності створення державної програми публічної безпеки із залученням ШІ (Коршенко та ін., 2020). Розглянуті в цій роботі дослідження спрямовані на підвищення публічної безпеки на основі вдосконалення систем її моніторингу із залученням різних моделей нейронних мереж, що можуть відстежувати протиправну діяльність, джерела підвищеної небезпеки, проводити масовий аналіз обличчя людей для пошуку злочинців та виконувати інші технічні допоміжні функції у правоохоронній діяльності. Впровадження таких систем відеоспостереження в населених пунктах України допомогло б суттєво покращити рівень безпеки, що є особливо актуальним у воєнний час. Через великий масштаб воєнних дій у місцях бойових зіткнень на деокупованих територіях можуть розташовуватися місця з покинутою зброєю, якою можуть заволодіти цивільні особи, а подальше її використання ними неможливо спрогнозувати. У цьому разі системи відеоспостереження, навчені виявляти зброю, можуть допомогти протидіяти незаконному її обігу.

Не менш важливою є робота із протидії проникненню диверсійних груп на територію країни. Можливість використання камер відеоспостереження з модулями виявлення руху та наявності зброї сприятимуть покращенню охорони кордону. Для цього необхідно розробити цілий комплекс засобів задля відстеження ситуації на державному кордоні України.

Іншим прикладом є використання камер відеоспостереження для запобігання протиправним вчинкам громадян. Можливість цілодобового моніторингу ситуації на вулицях сприяла б зменшенню злочинності. У своїй

роботі П. Єпринцев (2021) обґрунтував встановлення смарт-зупинок з камерами відеонагляду для моніторингу простору навколо зупинки. Це також повинно сприяти в пошуку осіб, причетних до вчинення злочинів.

Попри те, що системи відеоспостереження мають і безліч переваг, але одним з їх недоліків є наявність сліпих зон, тобто ділянок місцевості, де не може проводитись відеоспостереження. З огляду на це проводяться дослідження, що вивчають можливості оптимального розташування камер відеоспостереження, але для кращого моніторингу обстановки необхідні розробки та впровадження систем відеоспостереження на базі безпілотних літальних апаратів для моніторингу більших за площею ділянок, які неможливо охопити стаціонарними камерами.

ВИСНОВКИ. Підвищення рівня публічної безпеки за допомогою застосування новітніх розробок зараз досліджується багатьма вченими. Пропонуються різноманітні розробки на базі ШІ та створення застосунків, що можуть залучати громадськість до підтримки правопорядку. Розвиток технологій ШІ дозволив розширити можливості камер відеоспостереження для нагляду й допомоги в забезпеченні публічної безпеки. Для покращення роботи камер відеоспостереження роботу оператора більше перекладають на ШІ, що покращує роботу системи загалом, оскільки можливості людини є обмеженими. Здатність нейронних мереж до навчання створює безліч можливостей їх використання. Їх тренування за допомогою баз даних з різноманітними відео- та фотоданими дозволяє проводити аналіз відео на наявність зброї, неправомірного поведіння людей та виявлення осіб, що перебувають у розшуку. Також нейронні мережі дозволяють скоротити витрату ресурсів на їх роботу завдяки можливості використання менш енер-

говитратного обладнання. Наявність різноманітних баз із зображеннями та відеоматеріалами з протиправними елементами і поточною рутинною дозволяють навчати нейронні мережі розрізняти різні сценарії поведінки людини в повсякденному житті. Не менш важливими є дослідження контролю дорожнього руху за допомогою камер з можливістю спостереження та ідентифікації транспортних засобів, що рухаються в режимі реального часу. Загалом всі розглянуті в роботі способи відстеження неправомірної поведінки людей, зброї та розшукуваних осіб показують гарні результати в лабораторних дослідженнях з використанням різноманітних даних з відео та фотоматеріалами. Важливою запорукою покращення роботи камер відеоспостереження є їх оптимальне розташування на місцевості, що також постійно привертає увагу дослідників. В усіх вищезазначених дослідженнях науковці акцентували увагу на покращенні розпізнавальних якостей відеоспостереження, тобто на вивченні можливостей тренування нейронних мереж для виявлення зброї або протиправної поведінки. Але у всіх цих систем є свої недоліки, одним з яких є наявність сліпих зон, тобто ділянок, де спостереження не проводиться. І хоча існують пропозиції з вирішення проблеми сліпих зон, але це не усуває проблему повністю. Тому доцільним було б вивчити питання створення систем моніторингу публічного порядку додатковими засобами, окрім патрулів та камер відеоспостереження. Це може бути інтеграція технологій ШІ у пристрої, здатні до моніторингу більших за площею ділянок, які не можуть охопити наземні засоби. Зокрема, як приклад можна розглядати безпілотні літальні апарати з інтеграцією в них моделей нейронних мереж задля відстеження публічного порядку.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Василенко С., Гнатюк С. Відео та фотофіксація адміністративних правопорушень громадян. *Copernicus Political and Legal Studies*. 2022. Vol. 1, Iss. 4. Pp. 18–26. DOI: <https://doi.org/10.15804/CPLS.20224.02>.
2. Єпринцев П. С. Взаємодія підрозділів Національної поліції щодо запобігання розбоям вчиненим організованими злочинними групами. *Правові новели*. 2021. № 15. С. 182–190. DOI: <https://doi.org/10.32847/ln.2021.15.23>.
3. Зінов'єв Є. В., Арсенюк І. Р. Розпізнавання емоцій людини за допомогою згорткової нейронної мережі // Інтернет – Освіта – Наука – 2020 : матеріали XII Міжнар. наук.-практ. конф. (м. Вінниця, 26–29 трав. 2020 р.) / підгот. до друку: Т. О. Савчук, С. І. Петришин. Вінниця : ВНТУ, 2020. С. 202–206.
4. Кірей К. О. Система розпізнавання об'єктів навколишнього світу на основі нейронної мережі. *Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова*. 2021. № 1 (484). С. 86–91. DOI: [https://doi.org/10.15589/znp2021.1\(484\).12](https://doi.org/10.15589/znp2021.1(484).12).
5. Колесницький О. К., Янковський Є. В., Денисов І. К., Арсенюк І. Р. Виявлення озброєних людей у відеопотоці з використанням згорткових нейронних мереж. *Оптико-електронні інформаційно-енергетичні технології*. 2023. № 2, т. 46. С. 76–83. DOI: <https://doi.org/10.31649/1681-7893-2023-46-2-76-83>.

6. Коршенко В. А., Чумак В. В., Мордвинцев М. В., Пашнєв Д. В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України. *Право і безпека*. 2020. № 2 (77). С. 86–92. DOI: <https://doi.org/10.32631/pb.2020.2.12>.
7. Марчук Д. К. Використання афінних перетворень для корекції зображень з подальшим використанням у системах розпізнавання. *Технічна інженерія*. 2023. № 2 (92). С. 125–130. DOI: [https://doi.org/10.26642/ten-2023-2\(92\)-125-130](https://doi.org/10.26642/ten-2023-2(92)-125-130).
8. Остроглядів О. І. Кримінологічна характеристика та запобігання корисливим злочинам проти власності у великому місті Причорноморського регіону. *Південноукраїнський правничий часопис*. 2020. № 3. С. 86–94. DOI: <https://doi.org/10.32850/sulj.2020.3.16>.
9. Сватюк Д. Р., Сватюк О. Р., Белей О. І. Застосування згорткових нейронних мереж для безпеки розпізнавання об'єктів у відеопотоці. *Кібербезпека: освіта, наука, техніка*. 2020. № 8, т. 4. С. 97–112. DOI: <https://doi.org/10.28925/2663-4023.2020.8.97112>.
10. Alotaibi M. F., Omri M., Abdel-Khalek S., Khalil E., Mansour R. F. Computational Intelligence-Based Harmony Search Algorithm for Real-Time Object Detection and Tracking in Video Surveillance Systems. *Mathematics*. 2022. Vol. 10, Iss. 5. DOI: <https://doi.org/10.3390/math10050733>.
11. Apoorva P., Impana H. C., Siri S. L., Varshitha M. R., Ramesh B. Automated Criminal Identification by Face Recognition using Open Computer Vision Classifiers // 3rd International Conference on Computing Methodologies and Communication (ICCMC) : conference presentation proceedings (Erode, India, 27–29 March 2019). Erode, 2019. Pp. 775–778, DOI: <https://doi.org/10.1109/ICCMC.2019.8819850>.
12. Bewley A., Ge Z., Ott L., Ramos F., Upcroft B. Simple online and real-time tracking // 2016 IEEE International Conference on Image Processing : conference presentation proceedings (Phoenix, AZ, USA, 25–28 September 2016). Phoenix, 2016. Pp. 3464–3468. DOI: <https://doi.org/10.1109/ICIP.2016.7533003>.
13. Fathy C., Saleh S. N. Integrating Deep Learning-Based IoT and Fog Computing with Software-Defined Networking for Detecting Weapons in Video Surveillance Systems. *Sensors*. 2022. Vol. 22, No. 14. DOI: <https://doi.org/10.3390/s22145075>.
14. Gerell M. Hot Spot Policing with Actively Monitored CCTV Cameras: Does it Reduce Assaults in Public Places? *International Criminal Justice Review*. 2016. Vol. 26, Iss. 2. Pp. 187–201. DOI: <https://doi.org/10.1177/1057567716639098>.
15. González-Cepeda J., Ramajo A., Armingol J. M. Intelligent video surveillance systems for vehicle identification based on multinet architecture. *Information*. 2022. Vol. 13, Iss. 7. DOI: <https://doi.org/10.3390/info13070325>.
16. Gustav A. Surveillance cameras and crime a review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*. 2017. Vol. 18, Iss. 2. Pp. 210–222. DOI: <https://doi.org/10.1080/14043858.2017.1387410>.
17. Ingle P. Y., Kim Y.-G. Real-Time Abnormal Object Detection for Video Surveillance in Smart Cities. *Sensors*. 2022. Vol. 22, Iss. 10. DOI: <https://doi.org/10.3390/s22103862>.
18. Le V.-T., Kim Y.-G. Attention-based residual autoencoder for video anomaly detection. *Applied Intelligence*. 2023. Vol. 53. Pp. 3240–3254. DOI: <https://doi.org/10.1007/s10489-022-03613-1>.
19. Lim H. Crime-Reduction Effects of Open-street CCTV: Conditionality Considerations. *Justice Quarterly*. 2016. Vol. 34, Iss. 4. Pp. 597–626. DOI: <https://doi.org/10.1080/07418825.2016.1194449>.
20. Lin C.-J., Jhang J.-Y. Intelligent Traffic-Monitoring System Based on YOLO and Convolutional Fuzzy Neural Networks. *IEEE Access*. 2022. Vol. 10. Pp. 14120–14133. DOI: <https://doi.org/10.1109/ACCESS.2022.3147866>.
21. McLean S. J., Worden R. E., Kim M. Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder. *Criminal Justice Review*. 2013. Vol. 38, Iss. 3. Pp. 303–334. DOI: <https://doi.org/10.1177/0734016813492415>.
22. Piza E. L., Welsh B. C., Farrington D. P., Thomas A. L. CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis. *Criminology & Public Policy*. 2019. Vol. 18, Iss. 1. Pp. 135–159. DOI: <https://doi.org/10.1111/1745-9133.12419>.
23. Ratcliffe J. H., Taniguchi T., Taylor R. B. The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach. *Justice Quarterly*. 2009. Vol. 26, Iss. 4. Pp. 746–770. DOI: <https://doi.org/10.1080/07418820902873852>.
24. Socha R., Kogut B. Urban Video Surveillance as a Tool to Improve Security in Public Spaces. *Sustainability*. 2020. Vol. 12, Iss. 15. DOI: <https://doi.org/10.3390/su12156210>.
25. Vijeikis R., Raudonis V., Dervinis G. Efficient Violence Detection in Surveillance. *Sensors*. 2022. Vol. 22, Iss. 6. DOI: <https://doi.org/10.3390/s22062216>.

Надійшла до редакції: 12.01.2024

Прийнята до опублікування: 25.03.2024

REFERENCES

1. Alotaibi, M. F., Omri, M., Abdel-Khalek, S., Khalil, E., & Mansour, R. F. (2022). Computational Intelligence-Based Harmony Search Algorithm for Real-Time Object Detection and Tracking in Video Surveillance Systems. *Mathematics*, *10*(5). <https://doi.org/10.3390/math10050733>.
2. Apoorva, P., Impana, H. C., Siri, S. L., Varshitha, M. R., & Ramesh, B. (2019, March 27–29). *Automated Criminal Identification by Face Recognition using Open Computer Vision Classifiers* [Conference presentation abstract]. 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India. <https://doi.org/10.1109/ICCMC.2019.8819850>.
3. Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016, September 25–28). *Simple online and real-time tracking* [Conference presentation abstract]. 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA. <https://doi.org/10.1109/ICIP.2016.7533003>.
4. Fathy, C., & Saleh, S. N. (2022). Integrating Deep Learning-Based IoT and Fog Computing with Software-Defined Networking for Detecting Weapons in Video Surveillance Systems. *Sensors*, *22*(14). <https://doi.org/10.3390/s22145075>.
5. Gerell, M. (2016). Hot Spot Policing with Actively Monitored CCTV Cameras: Does it Reduce Assaults in Public Places? *International Criminal Justice Review*, *26*, 187–201. <https://doi.org/10.1177/1057567716639098>.
6. González-Cepeda, J., Ramajo, A., & Armingol, J. M. (2022). Intelligent video surveillance systems for vehicle identification based on multinet architecture. *Information*, *13*(7). <https://doi.org/10.3390/info13070325>.
7. Gustav, A. (2017). Surveillance cameras and crime a review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *18*(2), 210–222. <https://doi.org/10.1080/14043858.2017.1387410>.
8. Ingle, P. Y., & Kim, Y.-G. (2022). Real-Time Abnormal Object Detection for Video Surveillance in Smart Cities. *Sensors*, *22*(10). <https://doi.org/10.3390/s22103862>.
9. Kirei, K. O. (2021). System of image recognition of surrounding objects with neural networks. *Collection of Scientific Papers of Admiral Makarov National University of Shipbuilding*, *1*(484), 86–91. [https://doi.org/10.15589/znp2021.1\(484\).12](https://doi.org/10.15589/znp2021.1(484).12).
10. Kolesnytsky, O. K., Yankovsky, E. V., Denisov, I. K., & Arsenyuk, I. R. (2023). Detection of armed people in a video stream using convolutional neural networks. *Optoelectronic Information-Power Technologies*, *2*(46), 76–83. <https://doi.org/10.31649/1681-7893-2023-46-2-76-83>.
11. Korshenko, V. A., Chumak, V. V., Mordvintsev, M. V., & Pashniev, D. V. (2020). Security systems' status with the use of technical means of video recording and video surveillance: international experience, perspectives for implementation in the activities of the National police of Ukraine. *Law and Safety*, *2*(77), 86–92. <https://doi.org/10.32631/pb.2020.2.12>.
12. Le, V.-T., & Kim, Y.-G. (2023). Attention-based residual autoencoder for video anomaly detection. *Applied Intelligence*, *53*, 3240–3254. <https://doi.org/10.1007/s10489-022-03613-1>.
13. Lim, H. (2016). Crime-Reduction Effects of Open-street CCTV: Conditionality Considerations. *Justice Quarterly*, *34*(4), 597–626. <https://doi.org/10.1080/07418825.2016.1194449>.
14. Lin, C.-J., & Jhang, J.-Y. (2022). Intelligent Traffic-Monitoring System Based on YOLO and Convolutional Fuzzy Neural Networks. *IEEE Access*, *10*, 14120–14133. <https://doi.org/10.1109/ACCESS.2022.3147866>.
15. Marchuk, D. K. (2023). The use of affine transformations for image correction with further use in recognition systems. *Technical Engineering*, *2*(92), 125–130. [https://doi.org/10.26642/ten-2023-2\(92\)-125-130](https://doi.org/10.26642/ten-2023-2(92)-125-130).
16. McLean, S. J., Worden, R. E., & Kim, M. (2013). Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder. *Criminal Justice Review*, *38*(3), 303–334. <https://doi.org/10.1177/0734016813492415>.
17. Ostroglyadov, O. I. (2020). Criminological characteristic and prevention of mercenary crimes against property in a big city of the Black Sea region. *South Ukrainian Law Journal*, *3*, 86–94. <https://doi.org/10.32850/sulj.2020.3.16>.
18. Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, *18*(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>.
19. Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. (2009). The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach. *Justice Quarterly*, *26*(4), 746–770. <https://doi.org/10.1080/07418820902873852>.
20. Socha, R., & Kogut, B. (2020). Urban Video Surveillance as a Tool to Improve Security in Public Spaces. *Sustainability*, *12*(15). <https://doi.org/10.3390/su12156210>.

21. Svatiuk, D. R., Svatiuk, O. R., & Belei, O. I. (2020). Application of convolutional neural networks for the security of the object recognition in a video stream. *Cybersecurity: education, science, Technique*, 4(8), 97–112. <https://doi.org/10.28925/2663-4023.2020.8.97112>.
22. Vasylenko, S., & Hnatiuk, S. (2022). Video and Photo Recording of Administrative Offenses by Citizens. *Copernicus Political and Legal Studies*, 1(4) 18–26. <https://doi.org/10.15804/CPLS.20224.02>.
23. Vijeikis, R., Raudonis, V., & Dervinis, G. (2022). Efficient Violence Detection in Surveillance. *Sensors*, 22(6). <https://doi.org/10.3390/s22062216>.
24. Yepryntsev, P. S. (2021). Cooperation of the units of the National Police regarding the prevention of robberies committed by organized criminal groups. *Legal Novels*, 15, 182–190. <https://doi.org/10.32847/ln.2021.15.23>.
25. Zinoviev, Ye. V., & Arseniuk, I. R. (2020, May 26–29). *Recognition of human emotions using a convolutional neural network* [Conference presentation proceedings]. XII International Scientific and Practical Conference “Internet – Education – Science – 2020”, Vinnytsia, Ukraine.

Received the editorial office: 12 January 2024

Accepted for publication: 25 March 2024

DMYTRO OLEHOVYCH ZHADAN,

*Kharkiv National University of Internal Affairs,
Research Laboratory on the Problems of Information
Technologies and Combating Crime in Cyberspace;
ORCID: <https://orcid.org/0000-0001-8184-4800>,
e-mail: dmttro.zhadan23@gmail.com;*

MYKOLA VOLODYMYROVYCH MORDVYNTSEV,

*Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Research Laboratory on the Problems of Information
Technologies and Combating Crime in Cyberspace;
ORCID: <https://orcid.org/0000-0002-7674-3164>,
e-mail: lukoly@ukr.net;*

DMYTRO VALENTYNOVYCH PASHNIEV,

*Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Research Laboratory on the Problems of Information
Technologies and Combating Crime in Cyberspace;
ORCID: <https://orcid.org/0000-0001-8693-3802>,
e-mail: dvpashnev@gmail.com*

**TRACKING ILLEGAL ACTIVITIES USING VIDEO SURVEILLANCE SYSTEMS:
A REVIEW OF THE CURRENT STATE OF RESEARCH**

The current state of research on the use of the neural networks under martial law to identify offenders committing illegal acts, prevent acts of terrorism, combat sabotage groups in cities, track weapons and control traffic is considered. The methods of detecting illegal actions, weapons, face recognition and traffic violations using video surveillance cameras are analysed. It is proposed to introduce the studied methods into the work of “smart” video surveillance systems in Ukrainian settlements.

The most effective means of reducing the number of offences is the inevitability of legal liability for offences, so many efforts in law enforcement are aimed at preventing offences. Along with public order policing by patrol police, video surveillance is an effective way to prevent illegal activities in society. Increasing the coverage area of cameras and their number helps to ensure public safety in the area where they are used. However, an increase in the number of cameras creates another problem which is the large amount of video data that needs to be processed. To solve the problem of video data processing, various methods are used, the most modern of which is the use of artificial intelligence to filter a large amount of data from video cameras and the application of various video processing algorithms. The ability to simultaneously process video data from many CCTV cameras without human intervention not only contributes to public safety, but also improves the work of patrol police. The introduction of smart video surveillance systems allows monitoring the situation in public places around the clock, even if there is no police presence in the area.

In the reviewed studies of video surveillance systems, neural networks, in particular MobileNet V2, YOLO, mYOLOv4-tiny, are used to track illegal actions, criminals and weapons, which are trained on large amounts of video and photo data. It has been found that although neural networks used to require a lot of computing power, they can now be used in IoT systems and smartphones, and this contributes to the fact that more video surveillance devices can be used to monitor the situation.

Key words: *video surveillance, artificial intelligence, neural networks, security, weapons tracking, counter-terrorism.*

Цитування (ДСТУ 8302:2015): Жадан Д. О., Мордвинцев М. В., Пашнев Д. В. Відстеження протиправних дій за допомогою систем відеоспостереження: огляд сучасного стану досліджень. *Право і безпека*. 2024. № 1 (92). С. 78–89. DOI: <https://doi.org/10.32631/pb.2024.1.07>.

Citation (APA): Zhadan, D. O., Mordvyntsev, M. V., & Pashniev, D. V. (2024). Tracking illegal activities using video surveillance systems: a review of the current state of research. *Law and Safety*, 1(92), 78–89. <https://doi.org/10.32631/pb.2024.1.07>.