МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА КРИМІНАЛЬНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Калугін В.Ю.
Форос Г.В.

ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ ТА ВІДЕОСПОСТЕРЕЖЕННЯ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

НАУКОВО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Одеса
2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА КРИМІНАЛЬНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Калугін В.Ю.
Форос Г.В.

ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ ТА ВІДЕОСПОСТЕРЕЖЕННЯ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

НАУКОВО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

ОДЕСА 2025

УДК 351.74(072)(477)
Рекомендовано до друку Науково-методичною радою
Одеського державного університету внутрішніх справ
(протокол №6 від 19 червня 2025 р.)

Авторський колектив:
Калугін В.Ю. - кандидат юридичних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС
Форос Г.В. – кандидат юридичних наук, доцент, завідувачка кафедри кримінального аналізу та інформаційних технологій ОДУВС

Рецензенти:
Олексій ВОЛОШКО – начальник УКА ГУНП в Одеській області, полковник поліції
Карен ІСМАЙЛОВ – заступник начальника 5-го відділу (інформаційних технологій та програмування в південному регіоні) (м. Одеса) 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції Національної поліції України, підполковник поліції, кандидат юридичних наук, доцент

В42 Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України: науково-практичні рекомендації./Калугін В.Ю., Форос Г.В. — Одеса: ОДУВС, 2025. — 84 с.

Науково-практичні рекомендації призначені для ознайомлення з правовими та етичними аспектами використання відеоаналітики, ознайомлення з видами та можливостями систем відеоаналітики, вивчення практик застосування відеоаналітики в охороні громадського порядку, розвитку навичок оцінювання й використання відеоданих у процесі досудового розслідування.

Науково-практичні рекомендації можуть бути корисними для практичних працівників Національної поліції, а також при підготовці майбутніх правоохоронців.

ЗМІСТ

ВСТУП

В умовах стрімкого науково-технічного прогресу та інноваційного оновлення технологічного середовища перед правоохоронними органами постає дедалі складніше завдання розслідування злочинів, що потребує комплексного підходу та застосування сучасних методів інформаційно-аналітичного забезпечення. Останнє охоплює широкий спектр аналітичних інструментів і методологій, спрямованих на підвищення ефективності процесів виявлення, документування та розслідування кримінальних правопорушень.

Розвиток штучного інтелекту та вдосконалення спеціалізованого програмного забезпечення сприяли виокремленню окремого, хоча й не абсолютно нового напряму аналітичної діяльності – відеоаналітичних досліджень (відеоаналітики). Активізація цього напряму безпосередньо пов'язана зі швидкою еволюцією комплексних систем відеоспостереження, які вже стали невід'ємним елементом функціонування підрозділів Національної поліції України. Водночас актуалізується необхідність удосконалення правових механізмів регламентації застосування методів кримінального аналізу у процесі оперативно-розшукової діяльності та досудового розслідування, що вимагає системного підходу до їх правового забезпечення та нормативної адаптації.

Більшість розвинених країн зрозуміли ситуацію у якому перебуває суспільство, а тому зосередилися на використанні новітніх технологій в управлінській та правоохоронній діяльності. Адаптація вже наявного досвіду розробників інтелектуальних систем, у тому числі відеонагляду допоможе міським службам та правоохоронним органам організувати свою діяльність більш раціонально, спрямовуючи людські ресурси на

опрацювання меншого масиву даних отриманих з вулиць. А весь масив інформації, за визначеними сценаріями буде опрацьовувати інтелектуальна система, у разі порушення алгоритмів буде відбуватися попередження відповідних служб.

Використання отриманої інформації відеоаналітичних технологій для вирішення подальших важливих питань, таких як припинення, розкриття та запобігання злочинів та правопорушень працівниками Національної поліції.

Сьогодні в Україні існує потреба в удосконаленні матеріалів відео аналітики для сучасного розслідування, а також подальшого розвитку практичних можливостей використання відеофіксаціїї з метою ефективної реалізації завдань працівниками Національної поліції.

1. Загальні положення та основні напрями використання відеоаналітики

Аналіз відеоконтенту (англ. Video content analysis або video content analytics, VCA), також відомий як аналіз відео або відеоаналітика (VA) - це можливість автоматичного аналізу відео для виявлення та визначення часових і просторових подій.

Відеоаналітика - це сукупність технологій обробки відеозображень у режимі реального часу або з архівних записів із застосуванням алгоритмів штучного інтелекту, машинного навчання, розпізнавання образів тощо. Вона дозволяє автоматизувати процес моніторингу, аналізу ситуацій і виявлення правопорушень.

Підвищення ефективності роботи правоохоронних органів шляхом впровадження сучасних засобів відеоаналітики для попередження, виявлення та розслідування правопорушень.

Дослідження відеоматеріалів проводиться постійно підрозділами кримінального аналізу, починаючи з появи перших камер відеоспостережень, а з розбудовою масштабних систем відеоспостереження поліція отримала можливість розкривати злочини майже в режимі онлайн.

Оскільки нові технології, які приносять результат під час розслідування, неможливо було ігнорувати, аналітики стали першопроходьцями в даному векторі розвитку.

Сучасна діяльність підрозділів кримінального аналізу передбачає систематичне та професійне використання розгалужених систем відеоспостереження, що дозволяє обробляти та аналізувати величезні обсяги відеоматеріалів, які вимірюються сотнями терабайтів. Отже, становлення відеоаналітичних досліджень як окремого напряму було лише питанням часу та потребувало відповідного імпульсу для повноцінної інтеграції в оперативно-розшукову та аналітичну діяльність.

Виникнення підвищеного попиту на відеоаналітику пов'язане, насамперед, з гонкою дозволів, збільшенням обсягу отриманої інформації з камер відеоспостереження на жорстких дисках, необхідністю спростити пошук оператором необхідних даних для економії часу, своєчасно відреагувати на потенційні загрози та позаштатні ситуації.

Сама по собі відеоаналітика є новаторським рішенням у системах відеоспостереження, вона використовує алгоритми штучного інтелекту для самостійного аналізу, збирання та обробки необхідної інформації про об'єкти, які потрапили в поле зору камер, при цьому не включаючи у цей процес участь людини. Це означає, що система відеоаналітики сама аналізує зміни, що відбуваються в кадрі, порівнює їх із встановленими параметрами, і записує лише потрібну інформацію на жорстких дисках.

***Основні терміни, які вживаються для розуміння відеоаналітики*:**

- інтегрована система відеоспостереження та відеоаналітики - сукупність інформаційно-телекомунікаційних систем (ІТС- далі Система), які у процесі обробки інформації діють як єдине ціле;

- інформація (дані) - будь-які відомості, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді та знаходяться в комплексній системі відеоспостереження;

- обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в Системі за допомогою технічних та програмних засобів;

- інформаційна послуга - дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

- інформаційний продукт (продукція) - інформація, зібрана та оброблена в Системі, захищена від стороннього втручання і в подальшому підготовлена адміністратором та призначена для задоволення потреб користувачів та/або запитувачів інформації;

- доступ до інформації в системі - окремий авторизований вхід до Системи, який дає можливість самостійно використовувати ресурси в межах наданих повноважень (в межах наданого рівня доступу);

- рівень доступу до інформації в Системі - чітко визначений перелік інформації, до якої користувачу Системи надається доступ відповідно до нормативних положень;

- пріоритетний рівень доступу до інформації в Системі - різновид доступу до Системи, який включає можливість виконання чітко визначених операцій, а саме перегляду в режимі реального часу, введення, перетворення, зчитування та отримання інформації відповідно до напрямку діяльності відповідного користувача;

- загальний рівень доступу до інформації в Системі - різновид доступу до Системи, який включає можливість перегляду інформації (відеозапису) в режимі реального часу та отримання в автоматичному режимі статистичних зведень, без права обробляти інформацію в Системі;

- несанкціоновані дії щодо інформації в Системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

- блокування інформації в Системі - дії адміністратора, внаслідок яких унеможливлюється доступ користувачів до інформації в Системі;

- захист інформації в Системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в Системі;

- криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення

інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

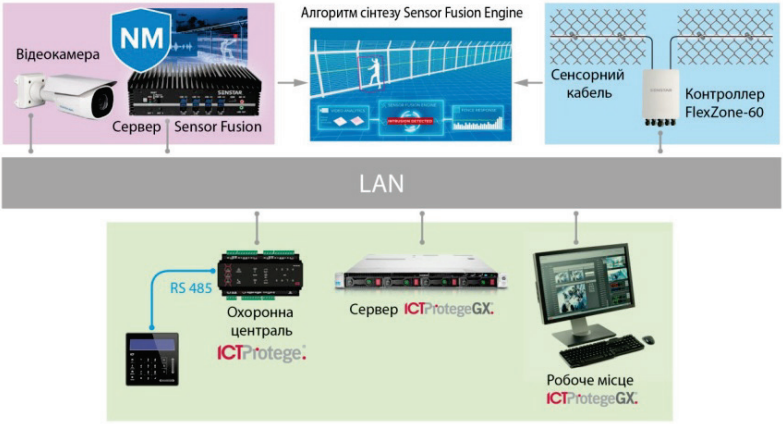
- програмно-апаратний комплекс - сукупність взаємопов'язаного серверного обладнання та програмного забезпечення, яке забезпечує накопичення та обробку інформації Системи;

- інші технічні засоби - засоби вимірювання, прилади візуалізації (в тому числі тепловізори) тощо;

- автентифікація - процедура встановлення належності користувачу інформації в системі наданого ним ідентифікатора;

- ідентифікація - процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою;

- засоби відеофіксації - технічні засоби, призначені для збирання, зберігання та первісної обробки відеоданих (переробки), а також за наявності технічних можливостей - відтворення відеоданих (зображення у русі) транспортних засобів, детектування обличчя, охорони периметру, керування трафіком, визначення задимлення, вибухів, несанкціонованого залишення предметів тощо).



2. Законодавче регулювання використання відеоспостереження

Встановлення і правильна експлуатація сучасних систем відеоспостереження має високу практичну цінність направлену на виявлення потенційної загрози ще до того, як вона призведе до серйозного інциденту, фіксації в режимі реального часу того, що відбувається на об'єкті або закритій території.

Сучасні відеокамери дозволяють одержати максимально деталізовану динамічну картинку. Відео записується на обрані носії (жорсткі диски, хмарні сервіси), що дозволяє переглядати його, коли виникне така необхідність.

Тут і виникає логічне питання, а чи не є відеозйомка посяганням на особисте життя і конфіденційність тих осіб, що потрапляють у поле зору камер?

В Україні немає єдиного закону про відеоспостереження у громадських місцях. Проте це ще не означає, організація відеозйомки людей у публічних закладах не регулюється на законодавчому рівні. Відповідно до статті 32 Конституції України кожному громадянину України гарантоване право на приватність, а саме: захист особистого і сімейного життя від зазіхань зі сторони третіх осіб; перешкоджання збору, зберіганню, розповсюдженню конфіденційної інформації про людину без її попередньої згоди за виключенням випадків, що визначені законом, проте лиш в інтересах національної безпеки.

Також слід звернутися до 301 й 302 статей Цивільного Кодексу, які регламентують невід'ємне право на приватне життя і недопущення розголошування інформації про нього, якщо це не суперечить національній безпеці, правам інших людей і економічному добробуту.

Стаття 307 Цивільного Кодексу містить положення, згідно яких проведення фото-, кіно-, теле-, відеозйомки громадянина вимагає попередньої згоди останнього. Але тут є важливе уточнення: фізична особа у будь-який момент може вимагати припинити зйомку, якщо остання представляє собою зазіхання на невід'ємне право на особисте життя. Проте при цьому допускається, що згода на зйомку вже отримана, якщо вона організовується на публічних заходах, на вулиці, зборах, конференціях, мітингах. Але й тут є важливий нюанс – встановлення і експлуатація камер відеоспостереження у громадських місцях потребує попереднього узгодження з державними службами. Також обов'язковим є інформаційне сповіщення людей про відеозйомку. Інформацію необхідно подати на спеціальних табличках, встановлених на видимих зонах об'єкту, наприклад, біля входу. При цьому увага при відеофіксації повинна фіксуватися на об'єкті (обмеженій площі чи території), а не на суб'єктах (людях).

Також слід звернутися до Кримінального Кодексу. Стаття 182 встановлює кримінальну відповідальність за втручання за втручання в особисте життя. При цьому у статті 359 мова йде про незаконне використання спеціальних технічних засобів прихованого отримання інформації.

Відповідно до ст. 40. Закону України «Про Національну поліцію» (Застосування технічних приладів, технічних засобів та спеціалізованого програмного забезпечення) передбачає:

1. Поліція для виконання покладених на неї завдань та здійснення повноважень, визначених законом, може застосовувати такі технічні прилади, технічні засоби та спеціалізоване програмне забезпечення:

1) фото- і відеотехніку, у тому числі техніку, що працює в автоматичному режимі, технічні прилади та

технічні засоби з виявлення та/або фіксації правопорушень;

2) технічні прилади та технічні засоби з виявлення радіаційних, хімічних, біологічних та ядерних загроз;

3) безпілотні повітряні судна та спеціальні технічні засоби протидії їх застосуванню;

4) спеціальні технічні засоби перевірки на наявність стану алкогольного сп'яніння;

5) спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото- і відеоінформації, у тому числі для встановлення осіб та номерних знаків транспортних засобів.

Технічні прилади та технічні засоби, передбачені пунктами 1 і 2 цієї частини, поліція може закріплювати на однострої, у/на безпілотних повітряних суднах, службових транспортних засобах, суднах чи інших плавучих засобах, у тому числі тих, що не мають кольорографічних схем, розпізнавальних знаків та написів, які свідчать про належність до поліції, а також монтувати/розміщувати їх по зовнішньому периметру доріг і будівель.

Поліція може використовувати інформацію, отриману за допомогою фото- і відеотехніки, технічних приладів та технічних засобів, що перебувають у чужому володінні.

2. Інформація про змонтовані/розміщені технічні прилади, технічні засоби повинна бути розміщена на видному місці.

Законодавчі аспекти відео спостереження у громадських місцях

У місцях масового скупчення людей зростає ризик різноманітних інцидентів: розбійних нападів, терактів, крадіжок, конфліктів на підґрунті особистої неприязні, переслідувань. Тому у громадських місцях доцільно

організовувати ефективні системи відеоспостереження, тобто технічні комплекси із камер, відео реєстраторів, носіїв інформації, на які записуються відеофайли, і комплектуючих.

Встановлення і правильна експлуатація сучасних систем відеоспостереження має високу практичну цінність щодо виявлення потенційної загрози ще до того як вона призведе до серйозного інциденту а також фіксації в режимі реального часу того, що відбувається на об'єкті або закритій території.

Сучасні відеокамери дозволяють одержати максимально деталізовану динамічну картинку. Відео записується на обрані носії (жорсткі диски, хмарні сервіси), що дозволяє переглядати його, коли виникне така необхідність.

Але, виникає логічне питання, а чи не є відеозйомка посяганням на особисте життя і конфіденційність тих осіб, що потрапляють у поле зору камер? До загальних актів, що регулюють застосування відеоспостереження у громадських місцях, належать: Конституція України (ч. 2 ст. 3, ст. 32), Конвенція про захист прав людини й основоположних свобод (ст. 8), Резолюція Парламентської Асамблеї Ради Європи щодо здійснення відеоспостереження у громадських місцях, Конвенція Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних, закони України «Про захист персональних даних», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та Цивільний кодекс України. Спеціальні акти, які регулюють застосування відеоспостереження, включають закони України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про державну охорону органів державної влади України та посадових

осіб», Кодекс України про адміністративні правопорушення.

Український парламент 6 липня 2010 року ратифікував Страсбурзьку конвенцію про захист фізичних осіб щодо автоматичної обробки персональних даних №108 («Конвенція 108»). Основні принципи цієї конвенції були впроваджені в національне законодавство Законом України від 1 червня 2010 року № 2297-VI «Про захист персональних даних» у редакції від 2 жовтня 2021 року.

Захист інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок регламентується ст. 307 Цивільного кодексу України від 16 січня 2003 року № 435-IV в редакції від 28 жовтня 2021 року. У ч. 1 цієї статті зазначається, що фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру. При цьому відповідно до ч. 3 даної норми знімання фізичної особи таємно, без її згоди може бути проведене лише у випадках, встановлених законом. Однак ці положення не обов'язково застосовуються до процесу розпізнавання обличчя.

Аналіз стану дотримання вимог законодавства про захист персональних даних в Україні під час здійснення відеоспостереження

Асоціацією українських моніторів дотримання прав людини (УМДПЛ) за підтримки Міжнародного фонду «Відродження» було представлено результати дослідження створення та функціонування систем відеоспостереження в Україні, що проводилося протягом 2019 року. Було розіслано близько 550 запитів до обласних, районних центрів, міст і селищ. Запитувалася інформація стосовно кількості встановлених камер відеоспостереження,

витрачених на це коштів, а також того, хто саме здійснює керування камерами і кому можуть бути надані зроблені відеозаписи.

Результати моніторингу показали, що по всій країні встановлено близько 18 тис. камер. У містах Дніпро, Київ, Одеса, Чернівці, Чернігів майже 30 % злочинів розкривається саме за допомогою новітніх технологій відеоспостереження. За підсумками дослідження організатори виявили суттєві недоліки захисту інформації в системах: органи місцевого само врядування нехтують нормами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Аналіз також показав, що майже ніде в Україні немає попереджень про відеозйомку, хоча є відповідне роз'яснення Уповноваженого з прав людини про їх обов'язковість із зазначенням того, хто знімає і як з такою особою можна зв'язатися, у тому числі з метою отримання необхідної інформації.

Київська міська рада прийняла Положення про функціонування комплексних систем відеоспостереження, яким було врегульовано питання захисту персональних даних, мети та функціонального призначення систем відеоспостереження, питання доступу до системи з переліком можливих користувачів, їх правами та обов'язками. Одним з основних користувачів системи є правоохоронні органи, які отримують доступ до системи в режимі перегляду персональних даних, а, наприклад, комунальні користувачі отримують доступ тільки в режимі знеособлення персональних даних.

Велика палата Конституційного Суду України розпочала розгляд об'єднаних конституційних скарг трьох громадян щодо відповідності Основному закону статті 14-2 Кодексу України про адміністративні правопорушення, яка передбачає відповідальність власників автомобілів за

порушення правил дорожнього руху, зафіксовані в автоматичному режимі. Національна асоціація адвокатів України також направила до Конституційного Суду України офіційну позицію щодо конституційності положень частини першої статті 142, частини п'ятої статті 279-1 Кодексу України про адміністративні правопорушення. Ідеться про відповідальність за адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані в автоматичному режимі, та за порушення правил зупинки, стоянки, паркування транспортних засобів, зафіксовані в режимі фотозйомки (відеозапису).

Право на захист персональної інформації є фундаментальною цінністю для кожної демократичної держави. Водночас, Україна у 2011 році однією з останніх серед пострадянських країн прийняла закон «Про захист персональних даних», який не був досконалим, мав багато недоліків, що не дало змоги сформувати ефективний механізм захисту песональної інформації. Ситуація ускладнилася тим, що у 2016 році було прийнято новий Регламент Європейськго Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС».

Відбулося також оновлення положень Конвенції Ради Європи «Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних».

Слід зазначити, що Україна взяла на себе зобов'язання адаптувати національне законодавство до законодавства ЄС у сфері захисту персональних даних до Загального регламенту про захист даних (General Data Protection Regulation; Regulation (EU) 2016/679)(GDPR), що передбачено статтею 15 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом,

Європейським Співтовариством з атомної енергії і їх державами-членами, з іншої сторони.

У Верховній Раді України зареєстровано два законопроекти, які стосуються реформи системи захисту персональних даних: проект закону № 5628 «Про захист персональних даних» (далі - законопроект), розроблений Міністерством цифрової трансформації України і проект закону № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації», яким передбачено створення незалежного регулятора зі сфери захисту персональних даних. Як зазначено в пояснювальній записці до законопроєкту, головна проблема у сфері захисту персональних даних полягає у відсутності законодавчих актів, які забезпечували б належний рівень їх захисту. Зважаючи на це Європейська комісія 21 квітня 2021 року представила перший у світі комплексний законопроект, присвячений посиленню та детальному регулюванню технологій штучного інтелекту, зокрема з розпізнаванням облич.

Технології штучного інтелекту поділяються залежно від ступеня ризику для безпеки, життя і прав громадян і їх використання будуть строго обмежувати або забороняти якщо вони становлять високий ризик. Так системи автоматичного розпізнавання облич не повинні використовувати для прикордонних перевірок чи у громадських місцях.

Європейський парламент вважає, що ЄС також повинен мати надійні гарантії при використанні інструментів штучного інтелекту в правоохоронних органах.

Як регулюється зйомка в громадських місцях на законодавчому рівні?

В Україні немає єдиного закону про відеоспостереження у громадських місцях. Проте це ще не

означає, організація відеозйомки людей у публічних закладах не регулюється на законодавчому рівні. Кожному громадянину України гарантоване право на приватність, а саме: захист особистого і сімейного життя від зазіхань зі сторони третіх осіб; перешкоджання збору, зберіганню, розповсюдженню конфіденційної інформації про людину без її попередньої згоди за виключенням випадків, що визначені законом, проте лиш в інтересах національної безпеки.

Особливості організації відеозйомки у громадських місцях: що можна і що не можна знімати

Загальні положення законодавчого регулювання відеоспостереження у громадських місцях розглянули. Отже, в Законі України «Про інформацію» можна знайти перелік ситуацій, відео фіксацію яких можна виконувати без обмежень. До них відносять: стан здоров'я населення; ДТП, аварії, небезпечні природні явища; порушення прав і свобод людини; незаконні дії посадових осіб, органів місцевої і державної влади; протиправні дії, які є посяганнями на життя і здоров'я громадян.

Загальнодоступність нових технологічних рішень у питанні розпізнавання облич дозволила муніципальним органам та поліції розвивати тему відео нагляду. Логічним кроком стала презентація поліцією Київської області в травні 2023 року системи публічної безпеки, оснащеної камерами з функцією розпізнавання облич та номерних знаків, а також аналітичним програмним забезпеченням, що дозволяє ідентифікувати осіб у режимі реального часу.

З правового погляду такі новітні системи залишаються поза межами регулювання закону, а тому централізований контроль щодо їхнього впровадження відсутній. Як наслідок, уже в січні 2024 року журналісти "Схем" опублікували розслідування, в якому наголосили на пов'язаних зі шпигуванням та хакерськими атаками

ризиках використання “розумних” камер і програмного забезпечення китайського походження, що встановлюють муніципальні органи в межах програм “Безпечне місто”.

Щоб зменшити загрози хаотичного та безсистемного розвитку муніципальних програм безпеки, ініціативна група депутатів за участю Міністерства внутрішніх справ подала 20 лютого 2024 року до Верховної Ради законопроєкт №11031 від 20.02.2024 “Про єдину систему відеомоніторингу стану публічної безпеки”.

У законопроєкті запропоновано:

- єдині функціональні й технічні вимоги до побудови та функціонування систем відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів, відомчих систем відеомоніторингу підприємств, установ, організацій, установлених у публічних місцях, порядок доступу до інформації, а також складу відеоданих, метаданих, аналітичних даних, відео архівів, сигналів тривога, що створюються ними;
- забезпечення єдиних правил інформаційного обміну на державному, регіональному та місцевому рівнях між суб’єктами єдиної системи відео моніторингу стану публічної безпеки через єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації;
- захист інформації, зокрема персональних даних у системах відео моніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів та відомчих системах відео моніторингу підприємств, установ, організацій, установлених у публічних місцях.

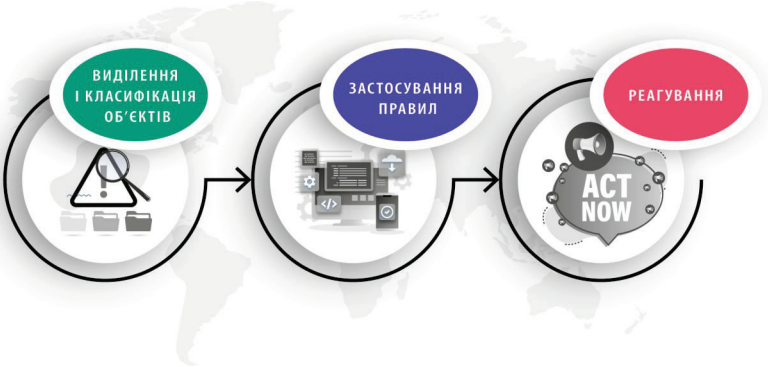
Рішенням Одеської Міської Ради від 19.09.2018 р. N 3610-VII було прийнято рішення «Про затвердження Положення про інтегровану систему відеоспостереження та відеоаналітики міста Одеси»

Відповідно до статті 25 Закону України "Про місцеве самоврядування в Україні", статті 4 Закону України "Про

захист інформації в інформаційно-телекомунікаційних системах", рішення Одеської міської ради від 15 березня 2017 року № 1778-VII "Про затвердження міської комплексної програми зміцнення законності, безпеки та порядку на території міста Одеси "Безпечне місто Одеса" на 2017 - 2019 роки", з метою визначення порядку використання та особливостей функціонування інтегрованої системи відеоспостереження та відеоаналітики міста Одеси, функціонування інтегрованої системи відеоспостереження та відеоаналітики міста Одеси.

Завданнями цієї Системи є виготовлення якісного інформаційного продукту, який може бути використаний з метою підвищення ефективності роботи виконавчих органів, підприємств та установ Одеської міської ради, правоохоронних органів, підприємств всіх галузей життєзабезпечення міста шляхом скорочення часу передачі необхідної інформації про події, правопорушення та злочини. Система призначена для надання дієвої допомоги при проведенні профілактичної роботи щодо попередження злочинів та може використовуватись для отримання доказової бази відносно подій і злочинів, що вже сталися, з метою долучення відеоматеріалів до кримінальних та адміністративних проваджень відповідно до чинного законодавства України.

3. Завдання та основні напрями використання відеоаналітики



Характер відеоспостереження, що розвивається, продовжує змінювати правила гри, коли справа доходить до розслідувань. Десятиліття тому впровадження традиційного відеоспостереження справило позитивний вплив на те, як правоохоронні органи проводять розслідування, надаючи поліцейським докази, отримані в режимі реального часу, а не ненадійні свідчення очевидців. І тепер відеоаналітика може підняти ці докази новий рівень. У той час як у поліцейських управлінь не бракує інцидентів для розслідування, їм часто не вистачає робочої сили, щоб розслідувати їх усе так швидко, як їм хотілося б, і саме тут у справу вступають камери відеоспостереження.

Типи та завдання відеоаналітики

Відеоаналітика може застосовуватися для різних завдань, що стоять перед системою безпеки. Так, можливо виділити кілька типів відеоаналітики:

1. *Ситуативна відеоаналітика*. На відміну від базових функцій, таких як виявлення руху або вторгнення в задану зону, ситуативна відеоаналітика використовує складні алгоритми для аналізу поведінки об'єктів, їх взаємодії між собою та з навколишнім середовищем. Вона

здатна розпізнавати нетипові ситуації, прогнозувати потенційні ризики та генерувати сповіщення в режимі реального часу.

Для охорони периметра об’єкта та у середині приміщення відеоаналітика застосовується з метою аналізу та запобігання несанкціонованому вторгненню зловмисників і сторонніх на територію об'єкта, для забезпечення безпеки та автоматизації контролю над ситуацією, що відбувається в реальному часі, збирає дані, зіставляє захоплені зображення об'єктів, що рухаються з архівом і автоматично реагує на можливі загрози, що виходять від об'єктів, які в минулому могли порушувати правила знаходження в приміщенні.

Ключовими характеристиками ситуативної відеоаналітики є:

- аналіз подій у їхньому часовому та просторовому контексті;
- виявлення не лише окремих об'єктів, але й їхньої поведінки та взаємодії;
- надання інформації для запобігання небажаним подіям, а не лише для їх фіксації;
- зниження навантаження на операторів завдяки автоматичному виявленню та класифікації подій;
- здатність налаштовуватися під конкретні потреби та сценарії використання.

Спектр застосування ситуативної відеоаналітики надзвичайно широкий. Виявлення підозрілої поведінки (залишені предмети, агресивна поведінка), контроль доступу, розпізнавання обличь, аналіз автомобільних номерів для виявлення викрадених або розшукуваних транспортних засобів.

Аналіз поведінки покупців (маршрути пересування, час перебування біля полиць, реакція на рекламні

матеріали), оптимізація розміщення товарів, контроль черг на касах, запобігання крадіжкам.

Моніторинг дорожнього руху, управління потоками транспорту, контроль за громадським транспортом, автоматичне виявлення інцидентів на залізничних коліях. Моніторинг громадського порядку, контроль за чистотою вулиць, управління паркуванням, аналіз скупчень людей.

Впровадження систем ситуативної відео аналітики надає значні переваги: швидке виявлення загроз та оперативне реагування на них; збір цінних даних для покращення ефективності бізнесу; автоматизація процесів та зменшення потреби в ручному моніторингу.

2. *Біометрична відеоаналітика* призначена для проведення аналізу відвідувача за унікальними біометричними показниками його обличчя.

При виявленні шуканої особи система автоматично визначає її власника, виділяючи з натовпу. Завдяки цьому можна швидко знайти злочинця в натовпі людей, які перебувають у розшуку.

Система безпеки створює власну базу біометричних даних, в якій можуть зберігатися тисячі знімків осіб за профілями відвідувачів. Тим самим можна налаштувати систему на автоматичне реагування з появою в полі зору камер небажаної або небезпечної персони.

Система відеоаналітики може розпізнати обличчя людини, за винятком таких змін у зовнішності, як вуса, стрижка, окуляри, головний убір або повноцінний грим, використовуючи тривимірну модель особи під час проведення біометричного аналізу обличчя людини.

3. *Загальна відеоаналітика* дозволяє підходити комплексно до реалізації різних завдань, поєднуючи між собою системи відеоспостереження, контроль доступу та електронний документообіг.

Єдина система безпеки може повноцінно працювати з усіма її складовими, прискорюючи обмін інформацією між системою відеоспостереження, контролем доступу та архівом даних. При цьому система безпеки зможе повністю проаналізувати ситуацію, що виникла, і вчасно відреагувати на загрозу. Завдяки відео аналітиці на підприємствах можливо створити електронну базу даних, за допомогою якої можна здійснювати обмін інформацією між підрозділами та службами.

Основними завданнями відеоаналітики можливо визначити:

1. Прискорення розслідувань після інцидентів. Час має вирішальне значення під час розслідування інциденту чи злочину. Поліцейським управлінням необхідно проводити розслідування якнайшвидше і точніше, але це традиційно включало «ручний» перегляд відеодоказів з камер відеоспостереження. Відеоаналітика робить відео доступним для пошуку, дієвим та піддається кількісній оцінці. Обробляючи відеодані за допомогою програмного забезпечення для відеоспостереження з відео аналітикою, правоохоронні органи можуть ідентифікувати, класифікувати та індексувати об'єкти на відеозаписи (автомобілі, вантажівки, автобуси, мотоцикли, велосипеди, жінки, чоловіки, діти та тварини). В результаті аналіз відео може значно скоротити час, необхідний для перегляду відео доказів, з годин або навіть днів до декількох хвилин, а також скоротити кількість помилок, пов'язаних з людським фактором.

Одним із способів, за допомогою якого програмне забезпечення з відеоаналітикою може допомогти співробітникам служби безпеки та поліції прискорити розслідування є розпізнавання осіб та номерних знаків. Оповіщення можна налаштувати для повідомлення правоохоронних органів про присутність заздалегідь

визначеного об'єкта, наприклад людини, в режимі поточного часу або під час перегляду відео після інциденту, що може допомогти правоохоронним органам швидше ідентифікувати та знайти підозрюваного. Наприклад, слідчі можуть ввести зображення підозрюваного або критерії ідентифікації такі як чоловік у синій сорочці, чорних штанах та чорній кепці. Оповіщення можна налаштувати для сповіщення слідчих щоразу, коли особа, яка відповідає цьому опису, виявляється в полі зору IP камери відеоспостереження або під час перегляду відео після інциденту.

Аналогічно, розпізнавання номерних знаків можна використовувати для швидкого повідомлення поліції в режимі реального часу про збіг з автомобілем підозрюваного або номерними знаками по вуличній IP-камері, і тому необхідні ресурси можуть бути розгорнуті в цьому районі.

2. Охорона громадського порядку**.** Міста та селища вже досить давно використовують камери відеоспостереження та вуличні камери для контролю дорожнього руху, а також часто співпрацюють із приватними підприємствами, які використовують відеоспостереження для перегляду своїх відео доказів, коли це необхідно. В останні роки персональні відео омофони та інші системи домашнього відеоспостереження стають все більш популярними у приватних будинках, що дає правоохоронним органам ще один інструмент в арсеналі, коли справа доходить до розслідувань інцидентів та аналізу відеозаписів.

Коли дозвіл надано, приватне комерційне або домашнє відеоспостереження може використовуватися декількома способами, такими як відстеження і пошук зниклих без вісті або ідентифікація підозрюваних.

допомогти слідчим швидко переглянути кілька годин відео та відточити ключові елементи свого розслідування.

Це партнерство між міськими жителями, підприємствами та місцевими органами громадської безпеки є основою громадської безпеки, важливою стратегією заохочення більш тісної співпраці між поліцією та членами співтовариства з метою запобігання злочинам, прискорення розслідувань та покращення якості життя. може взаємодіяти з мешканцями місцевої юрисдикції, зміцнювати довіру та співпрацювати в ініціативах, які забезпечують усім здоров'я, безпеку та комфорт.

3. Безпека та ефективність дорожнього руху. Щоб найкраще захистити водіїв та пішоходів, містобудівники та правоохоронні органи повинні виявляти точки перетину пішоходів та транспортних засобів. Знання того де і коли виникають затори на дорогах є ключем до того, щоб допомогти правоохоронним органам пом'якшити наслідки зіткнень чи заторів.

Відеоаналітику можна використовувати для відображення теплові карти як потужного інструменту веб аналітики, що вказують на зони з інтенсивним рухом як для водіїв, так і для пішоходів. Маючи цю інформацію, правоохоронці можуть швидко направити офіцерів для збору інформації про дорожній рух, щоб переконатися, що пішоходи у безпеці та що водії дотримуються правил дорожнього руху. У довгостроковій перспективі ця інформація може використовуватися містобудівниками для перегляду та оптимізації схеми руху, щоб зробити її безпечнішою та ефективнішою.

Моніторинг громадських місць: автоматичне виявлення підозрілої поведінки, скупчення людей, залишених предметів.

У сучасному світі питання безпеки в громадських місцях є одним із ключових для забезпечення

правопорядку, попередження злочинів і терористичних актів. З огляду на зростання кількості загроз, важливу роль відіграють інтелектуальні системи моніторингу, здатні в реальному часі аналізувати відео потоки та автоматично виявляти аномальну або підозрілу поведінку. До таких ситуацій належать скупчення людей, агресивні дії, залишені без нагляду речі тощо.

Відеомоніторинг є сучасним і ефективним засобом забезпечення безпеки та контролю. Він передбачає використання відеокамер для відстеження подій на об'єкті в реальному часі. Основні функції відео моніторингу включають:

Спостереження: відеокамери розташовуються у важливих точках для оптимального охоплення території та виявлення будь-яких можливих загроз.

Виявлення і реагування на небезпеку: оператори відео моніторингу виявляють будь-які підозрілі дії або ситуації, які можуть становити загрозу, і негайно реагують на них.

Відео моніторинг може *записувати відео* в реальному часі, а також *зберігати записи* для подальшого аналізу чи використання в судових процесах.

Деякі системи відеомоніторингу дозволяють операторам *віддалено переглядати відео* через Інтернет з будь-якого місця, що забезпечує постійний контроль.

Світові виробники постійно вдосконалюють наявні системи та адаптують їх до сучасних умов. Наразі спостерігається перехід від аналогових до цифрових відео систем, практикуються хмарні рішення, відеоаналітика на базі штучного інтелекту та багато іншого.

Технології штучного інтелекту здійснили справжній прорив у сфері відеоспостереження. Камери із цим софтом здатні аналізувати зображення й автоматично розпізнавати об'єкти або події в режимі реального часу. Сюди входить ідентифікація небажаних гостей у зазначеній користувачем

зоні обмеженого доступу, підрахунок людей і навіть аналіз їхньої поведінки. Аналітика допомагає автоматизувати спостереження і зробити його більш ефективним.

Зберігання відеоінформації в хмарному середовищі знижує потребу в локальних серверах і спрощує управління даними. Завдяки такому підходу сучасні системи відеоспостереження здебільшого пропонують віддалений моніторинг у мобільному додатку. Це дає змогу користувачеві отримати доступ до записів у реальному часі з будь-якого місця, де є можливість під'єднатися до інтернету, своєчасно виявляючи загрози та реагуючи на них. Візьміть до уваги, що виробники зосереджують зусилля на підвищенні безпеки цих систем, щоб запобігти злому й несанкціонованому доступу до інформації.

Завдяки під'єднанню до інтернету, вбудованим мікрофонам і динамікам користувачі можуть у будь-який час спілкуватися через відеокамери з тими, хто перебуває в полі зору об'єктива, - зі своєю сім'єю чи персоналом.

Завдяки розвитку штучного інтелекту, комп'ютерного зору та машинного навчання, системи спостереження можуть не лише передавати зображення, але й аналізувати його в реальному часі. Ключові функції таких систем: розпізнавання руху та об'єктів, виявлення підозрілих дій, оцінка скупчення людей, ідентифікація залишених або підозрілих предметів

Ці функції реалізуються за допомогою алгоритмів, які навчаються на великих масивах відеоданих для виявлення шаблонів аномальної поведінки.

Система аналізує рух людей, їхню швидкість, траєкторію та взаємодії. Підозрілою може вважатися: біг без очевидної причини, довге перебування в одній точці без руху, агресивні жести або бійки, спроби уникнути камер відеоспостереження

Сучасні алгоритми, зокрема нейронні мережі, здатні "вчитися" на прикладах поведінки, ідентифікуючи підозрілі ситуації з високою точністю.

Моніторинг скупчення людей Скупчення великої кількості людей в одному місці може свідчити як про планові події (акції, мітинги), так і про можливу небезпеку (паніку, тисняву, заворушення). Системи відео аналітики дозволяють оцінювати кількість людей у зоні спостереження, виявляти раптове збільшення щільності натовпу, надсилати тривожні сигнали при перевищенні безпечних меж. Це особливо важливо в транспортних вузлах, на стадіонах, у торгових центрах та під час масових заходів.

Виявлення залишених предметів Залишені предмети - це потенційні загрози, зокрема в контексті терористичних актів. Алгоритми спостереження дозволяють визначати об'єкти, що з'явилися у кадрі, але не були забрані тривалий час, співвідносити об’єкт з діями конкретної особи, надсилати повідомлення службам безпеки

Такі системи вже працюють в аеропортах, на вокзалах і в інших місцях із підвищеним рівнем загрози.

3.1. Розпізнавання обличчя, ідентифікація підозрюваних осіб або зниклих безвісти

Завдяки стрімкому розвитку штучного інтелекту, сьогодні системи відеоспостереження можуть не лише фіксувати події, а й автоматично ідентифікувати конкретних осіб. Це відкриває нові можливості для виявлення підозрюваних, попередження злочинів, а також для пошуку зниклих безвісти.

Ідентифікація людини за рисами обличчя – один із найдинамічніших напрямів у біометричній індустрії, яка постійно розвивається. Привабливість цього методу полягає в тому, що він найбільш наближений до звичайного людського розпізнавання індивідуумів.

Зростання мультимедійних технологій, зокрема всезростаюче використання відеокамер у громадських місцях таких, як міські вулиці та площі, аеропорти, авто- та залізничні вокзали й інші місця скупчення людей, зумовили необхідність розвитку цього напряму.

Основою будь-якої системи розпізнавання особи є застосування математичного методу кодування. Цей математичний метод заснований на аналізі локальних характеристик для представлення зображення особи у вигляді статистично обґрунтованих і стандартних блоків даних. Він ґрунтується на тому, що обличчя будь-якої особи може бути виокремлено з репрезентативної вибірки зображень лиця осіб із використанням сучасних статистичних прийомів. Отримуваний складний математичний код індивідуальної ідентичності обличчя містить інформацію, яка дозволяє з достатньою високою точністю відрізнити лице конкретної особи від мільйонів інших зображень обличчя. Тому нині біометричні технології, зокрема й методи розпізнавання за зображенням обличчя, і надалі є провідними інноваціями в індустрії безпеки, особливо в боротьбі зі злочинністю та тероризмом.

Для таких сфер практичного застосування, як прикордонний контроль, обслуговування та реєстрація пасажирів, робота з електронними ідентифікаційними документами та картками, попередження і розкриття злочинів за «гарячими» слідами, питання безпеки, нині неможливо обійтись без автоматизованих систем, що застосовують біометричні методи розпізнавання.

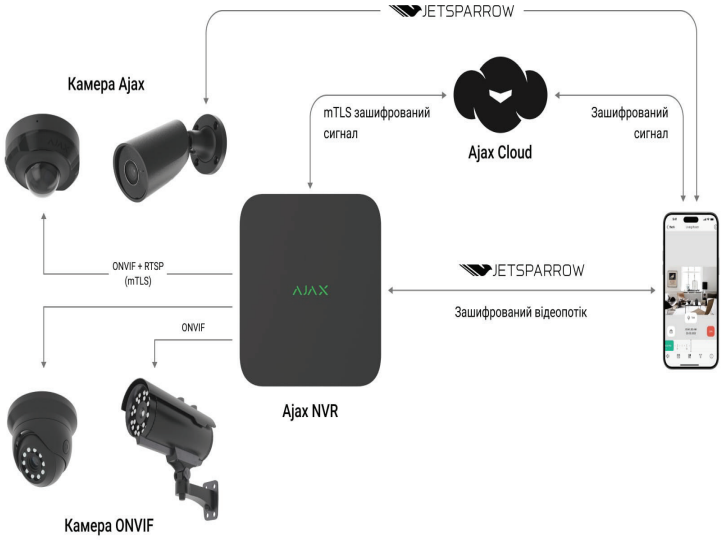
Технології сканування лиця осіб, як правило, працюють із відеозображеннями з розрішенням $320 \subseteq 240$ пікселів на дюйм зі швидкістю 3–5 кадрів у секунду. Можливість зйомки з більш високим розрішенням та частотою значно підвищують надійність впізнання. У разі

розпізнавання обличчя з великої відстані результат ідентифікації залежить від якості відеокамери.

Система розпізнавання обличчя працює за кількома етапами:

1. Захоплення зображення – фіксація обличчя через камеру або з фото.
2. Виділення біометричних ознак – визначення ключових точок обличчя (розташування очей, носа, губ, контурів).
3. Створення цифрового шаблону – унікальний набір параметрів, що описує зовнішність.
4. Порівняння з базою даних – зіставлення шаблону з уже наявними профілями.
5. Визначення збігу – встановлення особи з певним рівнем точності.

Критичні компоненти систем відеоспостереження



Ці етапи реалізуються за допомогою алгоритмів машинного навчання, особливо глибоких нейронних мереж.

Ідентифікація підозрюваних осіб. Системи розпізнавання обличчя активно застосовуються правоохоронними органами для: автоматичної ідентифікації підозрюваних у місцях масового скупчення людей (вокзали, стадіони, аеропорти); перевірки особистості затриманих осіб або учасників розслідувань; виявлення осіб, що перебувають у розшуку, через зіставлення з базами МВС або Інтерполу; моніторингу громадських місць у режимі реального часу. При цьому рівень точності сучасних систем може сягати понад 95%, особливо за умови якісного відео та правильної пози особи.

Пошук зниклих безвісти. Окремий і надзвичайно гуманний напрямок – використання технології для пошуку зниклих. Системи відеоспостереження в містах можуть виявити особу, яка тривалий час перебуває в розшуку, можливе виявлення дітей, людей похилого віку, осіб із психічними розладами.

У деяких країнах вже працюють національні бази даних із фото зниклих осіб, інтегровані з системами відеоспостереження.

Перевагами використання технології розпізнавання облич є швидкість і ефективність – ідентифікація займає долі секунди, можливість масового моніторингу – одночасна перевірка сотень людей у режимі реального часу, автоматизація процесу – зменшення навантаження на поліцейських і слідчих, та доказова база – підтвердження перебування особи у певному місці

Доцільно звернути увагу на застосування в ході відео аналізу біометричного програмного забезпечення FRT - яке математично відображає риси обличчя людини і

зберігає дані у вигляді відбитка обличчя. Програмне забезпечення використовує алгоритми глибокого навчання для порівняння знімка в реальному часі або цифрового зображення зі збереженим відбитком обличчя з метою перевірки особи.

FRT полягає у використанні комп'ютерів зі спеціальним програмним забезпеченням або відеокамер з вбудованою функцією інтелектуального розпізнавання обличчя. В основі використання різних видів устаткування лежить вирішення одного завдання - отримання якісного зображення людського обличчя (профіль або анфас). Штучний інтелект виявляє вузлові точки на обличчі та вимірює відстань між ними. Залежно від технології системі необхідно визначити до 80 таких точок. Після отримання зображення програма порівнює відбиток особи з інформацією, яка є в базах даних.

Основні стадії роботи алгоритму FRT:

1) виявлення обличчя;

2) аналіз зображення;

3) конвертування отриманої інформації в цифровий код;

4) порівняння отриманих даних із системною базою з упорядкуванням найбільш імовірних рис та пошук збігу.

Зроблений вибір передається людині-оператору, яка приймає рішення, наприклад, про загрозу безпеці.

Процес узгодження зображень, як частина FRT, потребує окремого аналізу, а очищення бази даних зображень теж є проблемою. Наприклад, підозрюваних розпізнають, якщо їхнє зображення зберігається в базі даних, що використовується для відповідності. Виникають питання, як ці зображення пов'язані з базою даних розпізнавання обличчя, чи всі учасники давали згоду на включення в базу даних і чи залишається мета обробки даних такою, якою була спочатку.

3.2. Розпізнавання номерних знаків, автоматичний контроль транспортних засобів

У контексті цифровізації безпеки дорожнього руху та транспортної інфраструктури особливу роль відіграють системи автоматичного розпізнавання номерних знаків (англ. ANPR - Automatic Number Plate Recognition). Ці системи дозволяють у режимі реального часу ідентифікувати транспортні засоби, контролювати їх пересування, а також підвищувати ефективність роботи правоохоронних органів, митниці, паркувальних служб і дорожніх операторів.

Процес розпізнавання номерних знаків складається з кількох етапів:

1. Захоплення зображення - відеокамера фіксує зображення автомобіля.
2. Локалізація номерного знака - програма визначає місце розташування номеру на зображенні.
3. Нормалізація зображення - вирівнювання та очищення кадру для підвищення чіткості.

4. Оптичне розпізнавання символів (OCR) - перетворення зображення символів у текстовий формат.

5. Порівняння з базами даних - виявлення співпадінь з інформацією про власників, страховку, штрафи тощо.

Сфери застосування:

1. *Контроль швидкісного режиму*. Контроль швидкісного режиму за допомогою систем ANPR є досить поширеною практикою в багатьох країнах, включаючи Україну. Такі системи використовують камери високої роздільної здатності, які фіксують номерні знаки автомобілів, а спеціальне програмне забезпечення розпізнає ці знаки. Потім ця інформація може зіставлятися з базами даних для різних цілей, Системи ANPR використовуються для автоматичного фіксування перевищення швидкості: транспортний засіб фіксується на в'їзді та виїзді із контрольної ділянки, і система обчислює середню швидкість.

В Україні системи ANPR використовуються для контролю швидкісного режиму, особливо на трасах державного значення та в містах. Інформація про зафіксовані порушення передається до відповідних органів для подальшого опрацювання та винесення штрафів.

2. *Розшук викрадених автомобілів*. Завдяки широкій мережі камер ANPR, особливо в великих містах та на ключових транспортних магістралях, значно підвищується ймовірність швидкого виявлення викрадених автомобілів. Це дозволяє скоротити час на їх розшук та мінімізувати збитки власників. Ефективність систем ANPR у розшуку викрадених автомобілів залежить від кількох факторів, включаючи: кількість та розташування камер - чим більше камер встановлено в стратегічно важливих місцях, тим вища ймовірність фіксації викраденого автомобіля; якість обладнання та програмного забезпечення, що забезпечує

чітке зображення номерних знаків навіть у складних погодних умовах або при високій швидкості руху. Ефективне програмне забезпечення гарантує швидке та точне розпізнавання номерних знаків; регулярне оновлення та повнота інформації в базах даних є критично важливими для успішного виявлення викрадених транспортних засобів.

Бази даних розшуку інтегруються з ANPR, що дозволяє миттєво виявляти авто, які перебувають у розшуку.

3. *Автоматизація паркувальних систем*. На платних паркінгах номер автомобіля використовується для відкриття шлагбаума, обліку часу та безконтактної оплати. Автоматизація паркувальних систем за допомогою систем ANPR є сучасним і ефективним рішенням, яке значно спрощує процес паркування як для водіїв, так і для операторів паркінгів. Основні аспекти цієї автоматизації:

Безконтактний в'їзд - замість використання паркувальних талонів або магнітних карт, камери ANPR на в'їзді автоматично розпізнають номерний знак автомобіля.

Якщо номерний знак зареєстрований у системі (наприклад, для резидентів, співробітників або попередньо оплачених парковок), шлагбаум автоматично відкривається, забезпечуючи швидкий і безперешкодний в'їзд. Система автоматично фіксує час в'їзду автомобіля, який прив'язується до розпізнаного номерного знаку.

Після виїзду автомобіля система автоматично визначає тривалість його перебування на паркінгу на основі часу в'їзду та виїзду. Через мобільні додатки або веб-сайти, прив'язані до номерного знаку. Для зареєстрованих користувачів може бути налаштоване автоматичне списання коштів з банківської картки. На виїзді або в спеціальних зонах можуть бути встановлені паркомати, які розпізнають номерний знак (введений

вручну або зчитаний камерою) і відображають суму до оплати.

Камери ANPR на виїзді розпізнають номерний знак автомобіля. Якщо оплата була здійснена або автомобіль має право на безкоштовний виїзд, шлагбаум автоматично відкривається. Система фіксує час виїзду автомобіля.

4. *Моніторинг транспорту на кордонах і митниці*. Використання систем ANPR для моніторингу транспорту на кордонах і митниці є надзвичайно важливим інструментом, який значно підвищує ефективність контролю, безпеку та швидкість проходження процедур. Основні аспекти застосування ANPR у цій сфері є: а) ідентифікація транспортних засобів -камери фіксують номерні знаки всіх транспортних засобів, що перетинають кордон; б) розпізнані номерні знаки автоматично звіряються з різними базами даних, включаючи: бази даних викрадених транспортних засобів , бази даних транспортних засобів, що перебувають у розшуку з інших причин (наприклад, пов'язаних з кримінальною діяльністю), бази даних транспортних засобів, щодо яких існують певні обмеження або застереження.

Система точно фіксує час і місце перетину кордону кожним транспортним засобом. У разі виявлення збігів з базами даних, система миттєво сповіщає прикордонні служби для вжиття необхідних заходів. Зібрані дані можуть використовуватися для аналізу інтенсивності руху через різні пункти пропуску, виявлення закономірностей та прогнозування можливих проблем.

На митниці ANPR використовується для ідентифікації транспортних засобів, що в'їжджають на митну територію або виїжджають з неї, а також може бути інтегрована з системами контролю контейнерів та інших вантажів, для перевірки митних декларацій. Система може допомогти виявити транспортні засоби, що намагаються

незаконно ввезти або вивезти товари, або ті, щодо яких є підозра у порушенні митних правил та сприяє автоматизації процесів оформлення та контролю, зменшуючи час очікування для легальних перевізників. Дозволяє збирати детальну статистику про переміщення товарів та транспортних засобів через митницю для аналізу та прийняття управлінських рішень. Крім того допомагає виявляти транспортні засоби, що можуть використовуватися для незаконного перевезення заборонених або нелегальних товарів.

5. *Облік громадського транспорту та спецтехніки*. Встановлення камер ANPR на ключових точках маршрутів дозволяє відстежувати фактичний рух автобусів, тролейбусів, трамваїв тощо. Система може фіксувати час проходження контрольних точок та порівнювати його з плановим розкладом, виявляючи запізнення або відхилення від маршруту.

Хоча ANPR безпосередньо не рахує пасажирів, аналіз частоти проходження громадського транспорту через певні точки в різний час може дати уявлення про пасажиропотік та допомогти оптимізувати графіки руху.

Система може фіксувати випадки використання службового транспорту не за призначенням або поза робочим часом. У разі виникнення інцидентів (наприклад, ДТП) записи ANPR можуть допомогти у встановленні обставин події та ідентифікації транспортних засобів.

Облік спецтехніки використовується для контролю місцезнаходження, часу виїзду на завдання та повернення на базу. транспорту комунальної техніки (сміттєвози, прибиральні машини), будівельної техніки, машин швидкої допомоги, пожежних машин тощо. Фіксація часу перебування спецтехніки на певних об'єктах може використовуватися для обліку виконаної роботи та контролю ефективності використання ресурсів.

На закритих територіях або будівельних майданчиках ANPR може використовуватися для контролю доступу спецтехніки.

Для екстрених служб (швидка допомога, пожежна охорона) ANPR може допомогти відстежувати рух автомобілів та аналізувати час реагування на виклики.

3.3. Трекінг об'єктів: відстеження переміщення осіб чи об’єктів по камерах відеоспостереження

Трекінг об’єктів (англ. object tracking) - це технологія, яка дозволяє визначати і супроводжувати об’єкт (людину, транспортний засіб, предмет) у послідовності відеокадрів. Система визначає координати об’єкта в кадрі, фіксує його переміщення, зміну швидкості, напряму та взаємодію з іншими об’єктами.

У сучасних умовах забезпечення безпеки та правопорядку, зокрема в громадських місцях, критичну роль відіграє технологія трекінгу об’єктів - автоматизованого відстеження руху людей або предметів за допомогою систем відеоспостереження.

Трекінг об’єктів - це ключовий інструмент сучасної системи відеоспостереження, який значно підвищує рівень безпеки, оперативності реагування та ефективності кримінального аналізу. Його впровадження має супроводжуватись технічним удосконаленням та чітким дотриманням етичних і правових норм, щоб забезпечити баланс між інноваціями та захистом прав людини.

Як працює система трекінгу:

1. Перший етап - виявлення об’єкта, ідентифікація об’єкта, який потрібно відстежувати (напр., людина в червоній куртці).
2. Кожному об’єкту надається унікальний ID.
3. Система аналізує послідовні кадри, вираховуючи нове положення об’єкта.

4. Мультикамерна синхронізація - якщо об’єкт виходить із зони однієї камери, система шукає його у полі зору наступної.

Для цього використовуються алгоритми штучного інтелекту, комп’ютерного зору, зокрема:

- DeepSORT, ByteTrack;
- YOLO (для виявлення об’єктів);
- CNN і Re-ID (для повторної ідентифікації).

Застосування трекінгу об’єктів. Відеоспостереження в режимі безпеки - виявлення осіб, що залишають підозрілі предмети, супровід підозрюваних на території вокзалів, аеропортів, торгових центрів, встановлення маршруту зниклої особи, відтворення пересування злочинця по місту, прогнозування тисняв або конфліктних ситуацій, відстеження автомобілів у міському середовищі та виявлення підозрілих або незареєстрованих транспортних засобів.

3.4.Аналіз дорожньо-транспортних пригод: реконструкція подій на основі відеозаписів

Аналіз дорожньо-транспортних пригод (ДТП) з використанням відеозаписів є надзвичайно цінним інструментом для реконструкції подій, встановлення причин та обставин аварії, а також визначення винних сторін. Відеозаписи з різних джерел, включаючи камери відеоспостереження (в тому числі системи ANPR), відеореєстратори автомобілів, камери мобільних телефонів та інші джерела, можуть надати ключову інформацію для відтворення картини події.

Етапи використання аналізу та реконструкції ДТП:

1. Збір та обробка відеоматеріалів. На початковому етапі слідчі та експерти збирають усі доступні відеозаписи, які могли зафіксувати момент ДТП або події, що йому передували. Це можуть бути записи з камер

відеоспостереження встановлених на будівлях, дорогах, перехрестях, автозаправних станціях тощо. Записи з камер ANPR можуть допомогти відстежити рух транспортних засобів до та після ДТП, а також зафіксувати номерні знаки учасників.

Записи з відеореєстраторів автомобілів - учасників або автомобілів-свідків є одним з найцінніших джерел інформації, оскільки фіксують безпосередньо дорожню обстановку з точки зору водія. Також записи з камер мобільних телефонів зняті очевидцями також можуть містити важливі деталі.

Отримані відеозаписи ретельно переглядаються для виявлення ключових моментів, таких як: положення транспортних засобів до, під час та після зіткнення, напрямок та швидкість руху учасників ДТП, дії водіїв (гальмування, маневрування, використання світлових сигналів), погодні умови та видимість на момент ДТП, наявність дорожніх знаків, розмітки та світлофорів, їхній стан, дії пішоходів або інших учасників дорожнього руху.

За необхідності використовуються спеціальні програми та методи для покращення якості відеозаписів (наприклад, підвищення чіткості, стабілізація зображення, корекція освітлення).

2. Детальний аналіз та реконструкція подій:

Детальний перегляд відео покадрово дозволяє зафіксувати послідовність подій з високою точністю, визначити фазу розвитку ДТП (початкова, кульмінаційна, завершальна).

За наявності на відео орієнтирів з відомими розмірами (наприклад, дорожні знаки, розмітка) та знаючи частоту кадрів відеозапису, експерти можуть приблизно розрахувати швидкість руху транспортних засобів. Системи ANPR також можуть фіксувати швидкість на певних ділянках.

Аналіз відео дозволяє встановити, які дії або бездіяльність учасників ДТП призвели до аварії. Наприклад, чи було перевищено швидкість, чи проїхав хтось на заборонений сигнал світлофора, чи не було дотримано правил маневрування тощо.

Відеозаписи аналізуються у поєднанні з іншими доказами, такими як: схема місця ДТП, пояснення учасників та свідків, результати експертиз (технічного стану транспортних засобів, судово-медичної), за наявності дані GPS-трекерів та бортових комп'ютерів автомобілів

У складних випадках для наочної демонстрації подій може бути створена тривимірна модель ДТП або анімація, що базується на аналізі відеозаписів та інших даних.

Результати аналізу відеозаписів є важливим доказом у кримінальному або адміністративному провадженні при визначенні винних у ДТП, для чого запис повинен бути належним чином вилучений та оформлений, а також підставою для призначення судової відео технічної експертизи Відеозаписи та висновки експертів, зроблені на їх основі, можуть бути представлені в суді як докази та допомагають страховим компаніям об'єктивно оцінити обставини ДТП та прийняти рішення щодо страхових виплат.

В ході аналізу дорожньо-транспортних пригод застосовуються:

- відеоаналітика з елементами штучного інтелекту;
- Motion tracking - відстеження руху об’єктів;
- Speed estimation - розрахунок швидкості за відео;
- Video enhancement - покращення якості кадрів;
- 3D-моделювання подій (з використанням спеціалізованих програм: PC-Crash, Virtual CRASH).

4. Алгоритм процесу відео аналітики

Процес відеоаналітики – це складний, але логічно структурований набір дій, спрямованих на автоматизоване вилучення цінних даних, закономірностей та аномалій з відео потоків. Він складається з кількох ключових етапів, кожен з яких відіграє важливу роль у отриманні кінцевого результату.

Етап 1.Збір та обробка відеоданих (Video Acquisition and Pre-processing)

Першим і фундаментальним кроком є отримання відеоданих. Це може відбуватися з різних джерел. Найпоширенішим джерелом є IP-камери, що передають цифровий відео потік по мережі. Аналогові камери - вимагають використання відеокодерів для перетворення аналогового сигналу в цифровий. Відео реєстратори (DVR/NVR) - записують відео з камер і можуть бути джерелом для подальшого аналізу.

Етап 2. Попередня обробка відеоданих, яка включає: а) декодування-розпакування стиснутого відео потоку для подальшого аналізу; б) очищення- усунення шумів, артефактів стиснення та інших спотворень, які можуть погіршити якість аналізу; в) калібрування - налаштування параметрів зображення (яскравість, контрастність, гама) для оптимальної роботи алгоритмів; г) стабілізація - усунення тремтіння камери для більш точного аналізу руху; д) вирівнювання перспективи (за потреби) - корекція спотворень, викликаних кутом огляду камери.

Етап 3. Виявлення об'єктів (Object Detection). На цьому етапі застосовуються алгоритми комп'ютерного зору для ідентифікації та локалізації цікавих об'єктів у кожному кадрі відео. До основних типів об'єктів, які можуть виявлятися, належать:

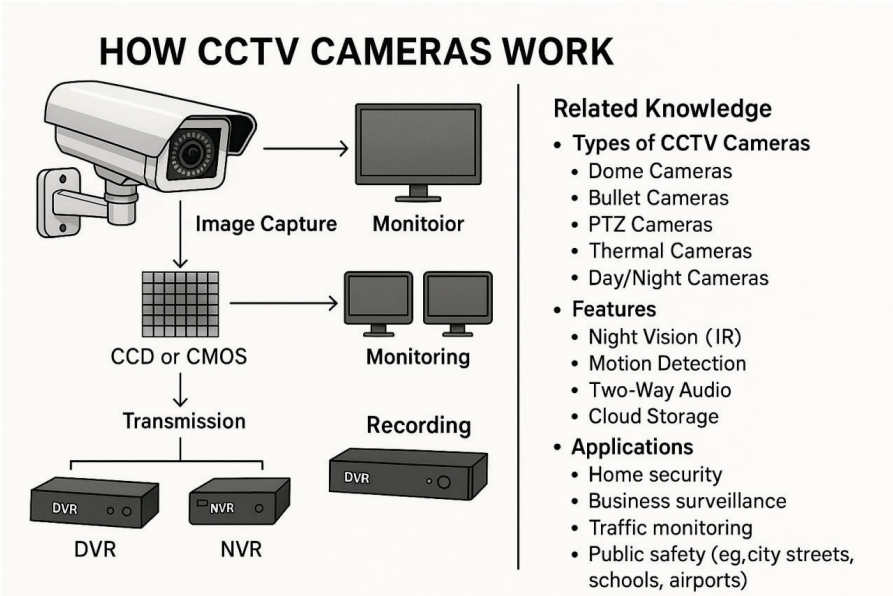
- люди -розпізнавання силуетів, окремих частин тіла, поз;

• транспортні засоби - визначення типу (автомобіль, вантажівка, мотоцикл), розпізнавання номерних знаків;

• тварини - класифікація за видами;

• предмети- виявлення конкретних об'єктів (сумки, коробки, зброя).

Для виявлення об'єктів використовуються різні методи, включаючи класичні алгоритми обробки зображень (наприклад, виявлення країв, виділення кольору) та сучасні нейронні мережі (наприклад, YOLO, Faster R-CNN, SSD), які демонструють високу точність і швидкість.



Етап 4. Відстеження об'єктів (Object Tracking). Після виявлення об'єктів на кожному окремому кадрі наступним кроком є їхнє відстеження в часі. Алгоритми відстеження встановлюють відповідність між об'єктами на послідовних кадрах, формуючи траєкторії їхнього руху. Це дозволяє

аналізувати поведінку об'єктів, їхні швидкості, напрямки руху та взаємодію.

Для відстеження використовуються різні підходи, включаючи: фільтри Калмана (спеціальний алгоритм, який використовує послідовність вимірювань, які містять шум та інші неточності, протягом певного часу для формування оптимальних оцінок невідомих змінних), та інші методи на основі передбачення, тобто прогнозування майбутнього положення об'єкта на основі його попередньої траєкторії; зіставлення візуальних ознак об'єктів між кадрами; використання нейронних мереж для більш надійного відстеження в умовах перешкод, зміни освітлення та часткового перекриття об'єктів.

Етап 5. Аналіз подій та поведінки (Event and Behavior Analysis). На цьому ключовому етапі відбувається інтерпретація зібраних даних про виявлені та відстежені об'єкти. Застосовуються складні алгоритми для виявлення певних подій або нетипової поведінки, які є метою відео аналітики.

Етап 6. Сповіщення та візуалізація (Alerting and Visualization). Останнім етапом є надання користувачеві інформації про виявлені події та результати аналізу в зручному форматі. Це може включати: а) сповіщення в режимі реального часу, тобто відправка повідомлень (текстових, електронних, push-сповіщень) при виявленні заданих подій; б) візуалізація даних - представлення результатів аналізу у вигляді графіків, діаграм, теплових карт, анотованого відео (з виділенням об'єктів та траєкторій); в) збереження та архівування результатів аналізу, для подальшого вивчення та звітності.

5. Впровадження систем відеоспостереження в діяльність Національної поліції України

Впровадження систем відеоспостереження є одним з визначальних факторів, що безпосередньо впливає на зниження рівня злочинності в країні та сприяє створенню безпечних умов для життя громадян. Такі системи мають важливе значення для формування безпечного середовища, профілактики правопорушень та їх ефективного розкриття. Присутність і активне використання відеоспостереження значною мірою сприяє поліпшенню динаміки розкриття злочинів та запобіганню правопорушенням у всіх сферах діяльності.

Національна поліція України активно застосовує різноманітні технології відеоспостереження, серед яких портативні відеореєстратори, системи відеоспостереження, що встановлені на службових транспортних засобах, автомобільні системи, стаціонарні системи, а також відеозапис на безпілотних літальних апаратах (БпЛА). Патрульна поліція використовує нагрудні відеокамери, що фіксують дії поліцейських під час виконання ними службових обов'язків, а також встановлені на транспортних засобах системи відеоспостереження та стаціонарні комплекси.

Основною метою використання відеореєстраторів є забезпечення об'єктивної оцінки дій патрульного під час виконання ним своїх функціональних обов'язків, а також ретельний збір доказів правопорушень, опитування свідків та потерпілих осіб. Відеофіксація подій при оформленні дорожньо-транспортних пригод створює додаткові належні докази, що забезпечують об'єктивний розгляд справ уповноваженими органами. Водночас, відеоконтроль за роботою патрульних сприяє підвищенню їх відповідальності, запобігає випадкам незаконного застосування фізичної сили, спеціальних засобів або

вогнепальної зброї працівниками поліції та захищає від можливих загроз з боку осіб, що можуть застосувати насильство або зброю проти патрульних.

Управління силами та засобами патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби «ЦУНАМІ». До складу цієї системи входить система стаціонарного відеоспостереження, яка забезпечує оперативний візуальний контроль за основними криміногенними місцями, вулицями, майданами, транспортними потоками й об'єктами, що охороняються. Інформація із систем відеоспостереження дозволяє старшому черговому відслідковувати оперативну обстановку та вносити корективи в роботу чергових інспекторів і може використовуватись для вказівок під час переслідування підозрюваних. Записані дані можуть бути використані як докази під час розслідування злочинів.

Під час виконання своїх обов'язків чергові патрульні застосовують системи відеоспостереження, встановлені на службових транспортних засобах. За допомогою таких систем функціонує інформаційна підсистема «Гарпун», призначена для обробки відомостей про транспортні засоби та номерні знаки транспортних засобів, що розшукуються в межах кримінальних і виконавчих проваджень. Крім того, система відслідковує транспортні засоби та номерні знаки транспортних засобів, які розшукуються у справах про адміністративні правопорушення, та для оперативно-розшукової діяльності. Крім засобів відеоспостереження, розташованих на службових транспортних засобах, використовуються прилади, розміщені по зовнішньому периметру доріг і будівель, а також у приватному володінні.

Система «Гарпун» використовує спеціалізоване аналітичне програмне забезпечення, створене для розшуку викрадених транспортних засобів та номерних знаків, виявлення одночасного перебування номерних знаків на різних транспортних засобах, фактів використання знищених номерних знаків, а також для автоматизованого інформування про такі факти чергових диспетчерів патрульної служби.

Однією з основних функцій системи UASC є здійснення процесу розпізнавання та пошуку транспортних засобів, що знаходяться в розшуку. Система ефективно виконує ідентифікацію транспортного засобу за державним номерним знаком, перевіряючи його відповідність реєстраційним даним. Вона здатна не тільки визначати номерні знаки автомобілів, а й ідентифікувати тип, марку та колір транспортного засобу. З використанням цих характеристик система може визначити, чи перебуває автомобіль у розшуку, а також провести перевірку його реєстраційних документів. Крім того, система має можливість ідентифікації осіб, що перебувають на передньому сидінні транспортного засобу.

Система також забезпечує моніторинг і виявлення скупчень людей, фіксуючи можливу неадекватну поведінку, а також розпізнає аномальні або заборонені маневри транспортних засобів. Вона здатна фіксувати порушення заборонених зон, виявляти перетин візуальних ліній та реагувати на рух людей у заданому напрямі. У контексті дорожнього руху система ідентифікує різноманітні події, включаючи щільність потоку, утворення заторів, а також масове скупчення транспортних засобів. Вона може виявляти людей у зоні спостереження та ідентифікувати залишення чи зникнення предметів.

Система «Безпечне місто» має потенціал відігравати важливу роль у профілактиці дорожньо-транспортних

пригод, у процесі розслідування правопорушень, а також у підтримці громадського порядку на вулицях. Вона сприятиме ефективному розвантаженню транспортних магістралей і стане значущим стримуючим фактором для потенційних правопорушників. [12]

У структурі апарату НП України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації та контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України.

Стрімкий розвиток безпілотних літальних апаратів (БпЛА) призвів до появи специфічних злочинів, пов'язаних із використанням цієї техніки, від вторгнення у приватне життя громадян до використання дронів, оснащених вибуховими пристроями та вогнепальною зброєю. Створення УПВП було викликано такими новими, нетрадиційними вимогами до безпеки громадян. Розвиток і використання нових сил і засобів такого типу повинні забезпечувати виконання завдань, покладених на НП України, зокрема протидії злочинності, підтримання публічної безпеки і порядку, сприяння в ліквідації надзвичайних ситуацій, захисту держав ного кордону.

Підрозділи поліції застосовують БпЛА для:

– висотного спостереження під час проведення масових святкувань, політичних демонстрацій, спортивних заходів, а також під час припинення масових заворушень;

– висотного спостереження в разі загрози нападу на стратегічні об'єкти та об'єкти, які перебувають під охороною;

– виявлення злочинів та адміністративних правопорушень;

організації відеодокументування;

– забезпечення зв’язку й управління наземними нарядами поліції;

– організації взаємодії підрозділів поліції з іншими силовими структурами;

– забезпечення та контролю безпеки дорожнього руху;

– проведення спостереження під час здійснення оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань;

– пошуку підозрюваних, які намагаються сховатись;

– пошуку зниклих людей.

Ручна обробка потоків інформації з відеокамер залишилась у минулому. Людина не може впоратися з аналізом великої кількості відеоматеріалу. Той, хто першим зможе максимально використовувати можливості інтелектуальної відеоаналітики, інакше кажучи, штучного інтелекту, отримає конкурентні переваги та повною мірою зможе забезпечити безпеку громадянського суспільства. Із точки зору застосування і розвитку штучного інтелекту у сфері безпеки необхідно розробити стратегію розвитку систем безпеки в Україні. Самі силові структури не в змозі розробити, впровадити й експлуатувати такі системи, у них на це немає ні фінансових, ні інтелектуальних ресурсів.

Виходячи зі світового досвіду, основні тенденції розвитку систем безпеки з відеоспостереженням є такими:

1) масове впровадження штучного інтелекту в усі системи безпеки, біометричне розпізнавання осіб, пошук поведінкових аномалій у рухах людини, розвиток розумних систем керування дорожнім рухом, автоматичний пошук підозрюваних, автотранспорту в розшуку тощо;

2) сертифікація інтелектуальних систем відеоспостереження із заданими показниками точності розпізнавання, визначення координат об'єкта тощо;

3) запровадження нейронних мереж для забезпечення високих показників точності;

4) упровадження систем безпеки в усіх місцях масового скупчення людей і на транспорті.

Згідно з п.4 розділу II наказу № 1026 під час здійснення повноважень поліцейськими портативний відеореєстратор закріплюється на його форменому одязі на грудях (ближче до плечового суглоба) так, щоб не створювати перешкод діям поліцейського. У випадках, пов'язаних з необхідністю якісної фіксації подій, поліцейські можуть тримати портативний відеореєстратор у руках. Дозволяється закріплення портативного відеореєстратора на екіпіруванні (шоломі) або зброї, якщо їх конструкцією передбачені відповідні кріплення.

Включення портативного відеореєстратора відбувається з моменту початку виконання службових обов'язків та/або спеціальної поліцейської операції, а відеозйомка ведеться безперервно до її завершення, крім випадків, пов'язаних з виникненням у поліцейського особистого приватного становища (відвідування вбиральні, перерви для приймання їжі тощо). У процесі включення портативного відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу.

Відеореєстратор може бути встановлений усередині салону службового транспортного засобу та/або зовні для максимальної фіксації навколишньої обстановки та/або внутрішньої частини салону в спосіб, що не заважає огляду водія.

Включення відеореєстратора здійснюється з моменту початку виконання службових обов'язків або спеціальної

поліцейської операції, а відеозапис ведеться безперервно до її завершення, при цьому в процесі включення відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу. Залежно від наявних режимів відеореєстратора та освітлення відеозапис здійснюється у відповідному режимі денної або нічної зйомки.

Обов'язки працівника поліції, пов'язані із застосуванням технічних приладів і технічних засобів фото- і кінозйомки, відеозапис

Під час виконання своїх повноважень поліцейським забороняються:

1) самовільне видалення відеозаписів з носіїв відеозапису, заміна цих носіїв, зміна їх системної дати та часу;

2) примусове виключення відеореєстраторів, у тому числі на вимогу сторонніх осіб;

3) перешкоджання здійсненню фото- і кінозйомки, відеозапису;

4) використання носіїв відеозапису у випадках, не пов'язаних із здійсненням ними повноважень поліції;

5) копіювання, передання інформації з відповідних носіїв стороннім особам.

Порядок застосування портативних відеореєстраторів та карт пам'яті до них, їх облік, зберігання та видача відеозаписів

Наказом керівника органу, підрозділу поліції призначається відповідальна особа з числа працівників органу, підрозділу поліції, на яку покладається відповідальність за: зберігання, видачу та приймання портативних відеореєстраторів; зберігання, видачу та приймання карт пам'яті; зміну дати та часу на портативних відеореєстраторах; облік, зберігання та видачу інформації, отриманої з портативних відеореєстраторів.

Портативні відеореєстратори та карти пам'яті зберігаються в приміщеннях органів, підрозділів поліції та видаються поліцейському під підпис у журналі обліку видачі, повернення портативного відеореєстратора та карт пам'яті, копіювання цифрової інформації, який зберігається в органі, підрозділі поліції.

Під час здійснення повноважень поліцейськими портативний відеореєстратор закріплюється на його форменому одязі на грудях (ближче до плечового суглоба) так, щоб не створювати перешкод діям поліцейського. У випадках, пов'язаних з необхідністю якісної фіксації подій, поліцейські можуть тримати портативний відеореєстратор у руках. Дозволяється закріплення портативного відеореєстратора на екіпіруванні (шоломі) або зброї, якщо їх конструкцією передбачені відповідні кріплення.

Включення портативного відеореєстратора відбувається з моменту початку виконання службових обов'язків та/або спеціальної поліцейської операції, а відеозйомка ведеться безперервно до її завершення, крім випадків, пов'язаних з виникненням у поліцейського особистого приватного становища (відвідування вбиральні, перерви для приймання їжі тощо). У процесі включення портативного відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу.

Порядок застосування відеореєстраторів, встановлених на службових транспортних засобах

Відеореєстратор може бути встановлений усередині салону службового транспортного засобу та/або зовні для максимальної фіксації навколишньої обстановки та/або внутрішньої частини салону в спосіб, що не заважає огляду водія.

Включення відеореєстратора здійснюється з моменту початку виконання службових обов'язків або спеціальної

поліцейської операції, а відеозапис ведеться безперервно до її завершення, при цьому в процесі включення відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу. Залежно від наявних режимів відеореєстратора та освітлення відеозапис здійснюється у відповідному режимі денної або нічної зйомки.

Застосування стаціонарних систем

Стаціонарні системи органів, підрозділів поліції працюють у цілодобовому режимі. Копіювання та видача інформації із стаціонарної системи проводяться відповідальною особою на підставі письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов'язки, про що робиться відмітка в Журналі обліку копіювання та видачі відеозаписів зі стаціонарної системи технічних приладів і технічних засобів фото- і кінозйомки, відеозапису.

Під час ведення відеоспостереження з використанням стаціонарних систем у громадських місцях, окремих службових приміщеннях органів і підрозділів поліції, у тому числі спеціальних приміщеннях, призначених для утримання затриманих та взятих під варту осіб, на видному місці встановлюється попереджувальний знак про проведення відеоспостереження.

Порядок застосування засобів фото- та відеозапису на БпЛА

Польоти БпЛА здійснюються відповідно до законодавства у галузі державної авіації України. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису залежно від технічних характеристик повітряного судна.

Кількість відеокамер та порядок їх використання на БпЛА (умови польотів, погодні умови, час доби тощо) визначаються згідно з керівництвом з льотної експлуатації БпЛА та/або згідно з інструкцією виробника.

Підготовка та розробка польотного завдання, у якому визначається початок та кінець роботи систем фото- і відеозапису, розміщених на БпЛА, здійснюються у порядку, визначеному законодавством, із дотриманням відповідних вимог, польотне завдання затверджує керівник органу підрозділу поліції.

Після виконання польотного завдання інформація з карти пам'яті або флеш-карти БпЛА експортується (переноситься) на носій інформації (карту пам'яті або флеш-карту) працівника поліції, який ставив завдання, про що робиться відмітка в польотному завданні.

У структурі апарату Національної поліції України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації та контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України. Стрімкий розвиток безпілотних літальних апаратів (БпЛА) призвів до появи специфічних злочинів, пов'язаних із використанням цієї техніки, від вторгнення у приватне життя громадян до використання дронів, оснащених вибуховими пристроями та вогнепальною зброєю. Створення УПВП було викликано такими новими, нетрадиційними вимогами до безпеки громадян. Розвиток і використання нових сил і засобів такого типу повинні забезпечувати виконання завдань, покладених на НП України, зокрема протидії злочинності, підтримання публічної безпеки і порядку, сприяння в ліквідації надзвичайних ситуацій, захисту держав ного кордону.

Підрозділи поліції застосовують БпЛА для:

– висотного спостереження під час проведення масових святкувань, політичних де монстрацій, спортивних заходів, а також під час припинення масових заворушень;

– висотного спостереження в разі загрози нападу на стратегічні об'єкти та об'єкти, які перебувають під охороною;

– виявлення злочинів та адміністративних правопорушень;

організації відео документування;

– забезпечення зв'язку й управління наземними нарядами поліції;

– організації взаємодії підрозділів поліції з іншими силовими структурами;

– забезпечення та контролю безпеки дорожнього руху;

– проведення спостереження під час здійснення оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань;

– пошуку підозрюваних, які намагаються сховатись;

– пошуку зниклих людей.

Порядок застосування засобів фото- та відеозапису на БпЛА

1. Польоти БпЛА здійснюються відповідно до законодавства у галузі державної авіації України.

2. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису залежно від технічних характеристик повітряного судна.

3. Кількість відеокамер та порядок їх використання на БпЛА (умови польотів, погодні умови, час доби тощо) визначаються згідно з керівництвом з льотної експлуатації БпЛА та/або згідно з інструкцією виробника.

4. Підготовка та розробка польотного завдання, у якому визначається початок та кінець роботи систем фото- і відеозапису, розміщених на БпЛА, здійснюються у порядку, визначеному законодавством, із дотриманням відповідних вимог, польотне завдання затверджує керівник органу підрозділу поліції.

5. Після виконання польотного завдання інформація з карти пам'яті або флеш-карти БпЛА експортується (переноситься) на носій інформації (карту пам'яті або флеш-карту) працівника поліції, який ставив завдання, про що робиться відмітка в польотному завданні.

Загальний порядок зберігання та видачі відеозаписів

Вивантаження відеозаписів з карт пам'яті портативних відеореєстраторів та відеореєстраторів, установлених на службових транспортних засобах, БпЛА, на сервер зберігання відеозаписів здійснюється шляхом приєднання карти пам'яті до спеціального обладнання в автоматичному режимі за допомогою спеціального програмного забезпечення або в інший спосіб, визначений виробником до такого сервера.

Відеозаписи автомобільних та стаціонарних систем зберігаються на сервері у визначений виробником спосіб.

Строк зберігання відеозаписів становить:

1) з портативних та відеореєстраторів, установлених у службових транспортних засобах, БпЛА,- 30 діб;

2) з автомобільної або стаціонарної системи залежно від технічних характеристик - не менше 30 діб;

3) у стаціонарних системах, які використовуються під час відбору кандидатів на службу до поліції,- 60 діб;

4) під час проведення поліцейськими навчальних занять та навчальних зборів зі службової підготовки - встановлюється керівником навчань.

Строк зберігання відеозаписів за рішенням керівника органу, підрозділу поліції може бути збільшено у разі використання їх у процесі здійснення оперативно-розшукової діяльності, у рамках розслідування кримінального провадження та/або в провадженнях у справах про адміністративні правопорушення, у разі фіксації надзвичайних подій за участю особового складу поліції, інших подій, якщо вони можуть бути використані в процесі службової діяльності органів, підрозділів поліції, під час проведення службових розслідувань.

Контроль за використанням технічних приладів і технічних засобів, що мають функцію фото- і кінозйомки, відеозапису, здійснює відповідальна особа, за інформацією, отриманою з їх допомогою,- безпосередньо керівник органу, підрозділу поліції.

Дозвіл на копіювання та видачу відеозаписів надається відповідальній особі виключно за рішенням керівника цього органу, підрозділу поліції.

Копіювання та видача відеозапису проводяться відповідальною особою на підставі відповідного письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов'язки.

У разі копіювання та видачі відеозапису робиться відмітка в Журналі обліку копіювання та видачі відеозаписів зі стаціонарної системи або в Журналі обліку.

Відеозаписи або копії з них можуть бути надані за вмотивованими запитами органів державної влади, органів досудового розслідування, прокуратури, слідчого судді та суду, поліцейського та інших осіб у порядку, передбаченому законодавством України.

Передавання відеозаписів, отриманих з портативних та відеореєстраторів, установлених на службових транспортних засобах, БпЛА, автомобільних та стаціонарних систем для використання засобами масової

інформації, а також поширення в мережі Інтернет, здійснюється з дозволу керівника органу, підрозділу поліції з дотриманням Закону України «Про захист персональних даних». Таке передавання здійснюється виключно з метою забезпечення безпеки та захисту інтересів громадян, суспільства і держави, а також з метою захисту гідності та честі працівника поліції.

Відеозаписи працівникам органу, підрозділу поліції видаються в тому вигляді, в якому вони були збережені на док-станції,- без коригування. Перегляд, аналіз відеозапису здійснюються працівником поліції, якому він виданий для виконання покладених на нього завдань в межах його повноважень.

Ручна обробка потоків інформації з відеокамер залишилась у минулому. Людина не може впоратися з аналізом великої кількості відеоматеріалу. Той, хто першим зможе максимально використовувати можливості інтелектуальної відеоаналітики, інакше кажучи, штучного інтелекту, отримає конкурентні переваги та повною мірою зможе забезпечити безпеку громадянського суспільства. Із точки зору застосування і розвитку штучного інтелекту у сфері безпеки необхідно розробити стратегію розвитку систем безпеки в Україні. Самі силові структури не в змозі розробити, впровадити й експлуатувати такі системи, у них на це немає ні фінансових, ні інтелектуальних ресурсів.

Виходячи зі світового досвіду, основні тенденції розвитку систем безпеки з відеоспостереженням є такими:

1) масове впровадження штучного інтелекту в усі системи безпеки, біометричне розпізнавання осіб, пошук поведінкових аномалій у рухах людини, розвиток розумних систем керування дорожнім рухом, автоматичний пошук підозрюваних, автотранспорту в розшуку тощо;

2) сертифікація інтелектуальних систем відеоспостереження із заданими показниками точності розпізнавання, визначення координат об’єкта тощо;

3) запровадження нейронних мереж для забезпечення високих показників точності;

4) упровадження систем безпеки в усіх місцях масового скупчення людей і на транспорті.

Якісна робота відеоаналітики потребує якісного зображення.

Найбільшого застосування отримали відеокамери на основі ПЗЗ-матриць. У більшості випадків використовуються короткофокусні об'єктиви типу фікс-фокус, що не потребують фокусування, та автоматичне керування експозицією. Основні виробники матриць - Sony, Sharp, Panasonic, Samsung, LG, Hynix. Їх використання дозволило створити помірні за ціною та досить високоякісні вироби широкого застосування. Зазвичай різниця між камерами, заснованими на матрицях різних виробників, проявляється у складних умовах освітлення. У лінійці кожного виробника присутні як дешеві та стандартні за параметрами матриці, так і матриці підвищеної роздільної здатності та/або підвищеної чутливості.

За типом вихідного сигналу відеокамери поділяють на аналогові та цифрові. Більшість цифрових камер передають сигнал стандартної комп'ютерної мережі типу Ethernet — звані IP-камеры.

За способом передачі даних відеокамери поділяються на дротові та бездротові. Останні мають у своєму складі передавальний пристрій та антену. Бездротовими в тому числі є цифрові IP-камери, що передають зображення по радіоканалу мережі Wi-Fi - так звані Wi-Fi відеокамери.

Особливістю систем IP-відеоспостереження є передача відеопотоку в цифровому форматі через мережу

Ethernet, що використовує міжмережевий протокол або IP, звідси і назва. Система IP-відеоспостереження складається з мережевих пристроїв, кожен з яких має в мережі свою IP-адресу та унікальну MAC-адресу.

Першим та головним компонентом будь-якої системи IP-відеоспостереження є IP-камера. Настільки головним, що сама IP-камера може бути повноцінною системою IP-відеоспостереження. IP-камера може знімати відео, записувати його на вбудовану SD-карту, може надсилати повідомлення про події, що відбуваються в кадрі, дозволяє переглядати відео онлайн на екрані монітора або смартфона, може виконувати аналіз відео (відеоаналітика), наприклад, розпізнавати автомобільні номери.

Засоби відеоаналітики дозволяють виявляти залишені або, навпаки, віднесені предмети, фіксувати траєкторію руху об'єкта і навіть відстежувати його переміщення від камери до іншої.

При побудові систем IP-відеоспостереження окрім основного завдання вибору тактики охорони з урахуванням особливостей IP-відеоспостереження, необхідно вирішувати безліч супутніх завдань, які потребують спеціальних знань, і значно впливають на підсумковий результат.

Серед таких завдань можна відзначити вибір активного обладнання, побудову локальної мережі, розрахунок сховища відео, вибір серверного обладнання.

Тип відеокамер, роздільна здатність та функціонал вибирається виходячи з конкретного завдання. Сучасні камери мають багатий функціонал і набір можливостей. Основні та найбільш значущі параметри:

• роздільна здатність камери;

• передача даних, тип стиснення, багатопотокова передача відео;

• чутливість до роботи у темний час доби.

Відеокамера являє собою пристрій, що перетворює світловий потік стандартний відеосигнал, який в подальшому транслюється на пристрої обробки сигналу (монітори, записуючі пристрої і т. д.).

Щоб отримати якісне зображення з відеокамери, важливим є кожен елемент, що входить до складу пристрою. Важливу роль у генерації відеопотоку з чітким деталізованим малюнком грає об'єктив. Від якості лінз, їх припасування та складання, а також сумісності з характеристиками світлочутливої матриці залежить ефективність роботи обладнання. Тому при виборі об'єктиву камер відеоспостереження важливо правильно визначити, яка оптика потрібна в конкретній ситуації. Для цього потрібно знати її основні характеристики, специфіку та сферу застосування.

Види об'єктивів камер відеоспостереження

За конструкцією розрізняють 4 типи оптики:

• фіксований (монофокальний). Мають одне незмінне значення фокусної відстані. Не потребують налаштування, не можуть змінювати кут огляду камери.

• варіофокальні. Дозволяють вручну регулювати фокусну відстань у межах, заданих конструктивно. Таку оптику можна підлаштовувати під об'єкт або швидко переконфігурувати виконання нового завдання. Універсальний варіант підбору об'єктива для камери відеоспостереження.

• трансфокаторний. Обладнаний двигуном для зміни фокусної відстані в автоматичному режимі. Використовується в обладнанні PTZ, дозволяє змінювати кут огляду, масштабувати зону спостереження. Як правило, оптика обладнана системою автофокусування під час зумування об'єктів.

• fish-eye. Панорамна оптика, що дає кут огляду 360°. У зв'язку зі специфікою передачі зображення вимагає використання розгортки картинки на площину. Відео, отримане з камери, є незручним для перегляду в необробленому вигляді.

Основні характеристики різних типів об'єктивів камер відеоспостереження

Кожна оптична система, встановлена у відеокамерах, має низку характеристик, які впливають на специфіку її роботи.

Так до основних параметрів ми можемо віднести фокусну відстань та кут огляду.

Як підібрати об'єктив для камери відеоспостереження за кутом огляду?

• вузькокутні (3-30°). Використовують контролю невеликого сектора: коридорів, сходів, території під вікнами;

• середньокутові (30-70°). Застосовують у системах відеоспостереження на дитячих чи спортивних майданчиках, парковках, невеликих офісних чи складських приміщеннях;

• ширококутні (до 95°). Ставлять на спостереження великими залами, вхідними конструкціями, дворами приватних будинків;

• панорамні (360°). Використовуються при спостереженні за приміщенням або вуличною територією. Не залишають «мертвих» зон.

Камери нічного бачення та тепловізори

ІЧ-відеокамера, або камера нічного бачення, має вбудоване інфрачервоне підсвічування. Працює таке обладнання за рахунок фіксації відбитого інфрачервоного випромінювання, яке невидиме для людського ока, проте достатнього для того, щоб зробити якісний кадр.

Тепловізор також працює в інфрачервоному діапазоні, але зображення, що отримується з приладу, відчутно відрізняється від зображення з камери відеоспостереження. Устаткування відображає температурне поле об'єкта, що випромінюється. Розпізнати фігуру людини буде нескладно, але зрозуміти хто саме на картинці неможливо.

Більшість тепловізорів здатні змінювати температуру та надавати кольорове зображення, де кожному кольору відповідає певна температура.

Окрім відповідного освітлення (якому на периметрах почасти не приділяється багато уваги), відсутності оптичних завад в зоні відеонагляду (предметів, конструкцій, що заважають прямій видимості), важливим є й показник розподільчої здатності, що зазвичай вимірюється в пікселях на метр. Найкращі алгоритми здатні надійно виявляти і класифікувати об’єкти у відеоряді при щільності точок 120-130 піксель/м. При цьому, деякі виробники для спрощення прямо вказують дистанцію від точки фізичного розташування камери, на якій гарантовано надійне функціонування системи.

Концепція безпеки периметру об’єктів критичної інфраструктури зазвичай передбачає побудову глибокоешелонованої системи детекції, що включає кілька

охоронних рубежів із застосуванням різних фізичних принципів. Почасти, однак, замовнику необхідно контролювати зовнішню територію, що безпосередньо прилягає до периметру, однак не є його власністю (а відтак немає можливості побудувати повноцінну огорожу). "

В таких випадках оптимальним рішенням може стати впровадження технічних засобів нульового, або попереджувального рубежу, основу якого складає відеоплатформа з аналітикою. Глибока інтеграція охоронної централі або комплексної системи управління безпекою з підсистемою відеонагляду дозволяє розпізнавати аналітичні метадані в якості стандартних детекторів, підключених на віртуальні зони. В той же час, потік з тих же камер продовжує використовуватись як відеопідтвердження отримуваних оператором тривог

Типи камер

Фіксовані камери є стаціонарними та фокусуються на певній ділянці, забезпечуючи постійне й незмінне зображення.

PTZ-камери (панорамування, нахил і зум) розширюють можливості системи безпеки завдяки можливості рухатися й масштабуватися, щоб забезпечити широке охоплення та сфокусований моніторинг певних ділянок. Ці камери можуть панорамувати, нахиляти й масштабувати, ефективно охоплюючи великі площі та збільшуючи масштаб зображення в разі необхідності. Зони спостереження можна змінювати відповідно до запитів у реальному часі та мінливих пріоритетів, щоб отримати гнучкий і оперативний моніторинг. Віддалене керування і можливість автоматизованого патрулювання PTZ-камер забезпечують адаптивне і комплексне спостереження, пристосоване до мінливих потреб.

Купольні камери часто використовуються всередині приміщень і захищені від несанкціонованого доступу.

Довгі циліндричні камери (булет) ідеально підходять для спостереження на великих відстанях і зазвичай використовуються на вулиці.

Під час зйомки відео потік інформації розбивається на послідовність із двох кадрів. Кадр – отримане з камери зображення зі своєю роздільною здатністю та форматом. Усередині такого потоку система аналітики може використовувати стиснення кадрів зниження обсягу і прискорення передачі. Однак при демонстрації результату на екран відображається зображення в початковому, не стислому вигляді.

Спочатку система зменшує отриманий кадр для швидкої обробки. При цьому частина інформації буде втрачена, проте система відеоаналітики працює в основному з великими об'єктами, і вони не пропадуть під час стиснення кадру. В основному при стиску пропадає все зайве, особливо шуми та світло.

Далі система порівнює наступні кадри з обробленим кадром і приймає рішення в залежності від завдання, яке поставлено перед системою відеоаналітики.

Водночас системи відеоспостереження, встановлені в межах муніципальних програм “Безпечне місто”, працюють за дещо іншим принципом. Більшість камер “Безпечного міста” є оглядовими та позбавлені додаткових функцій. Такі камери в цілодобовому режимі транслюють відео до інформаційних центрів, де відбувається запис та зберігання трансляції. Зазвичай інформаційні центри створюються на базі комунальних підприємств або на певних об’єктах, що потребують підвищеного рівня охорони, а територіальні підрозділи поліції забезпечують постійний доступ до камер і збережених записів. У такому разі поліцейські можуть отримати інформацію щодо

обставин порушення або особи порушника лише постфактум. Малоймовірно, що поліцейський у прямому ефірі певної муніципальної відеокамери побачить, наприклад, крадіжку з вітрини вуличного магазину.

До пристроїв обробки відеосигналів та відеозапису відносять: відеоквадратори, відеомультиплексори, відеодетектори руху, пристрої запису відеосигналу DVR та IVR.

Пристрої обробки відеосигналів - прилади, за допомогою яких відбувається обробка відеозображень, що одержуються від декількох камер відеоспостереження, аналіз отриманих зображень та їх передача на монітор ПК. Виходячи з типу використовуваних відеокамер, УВВ бувають чорно-білими або кольоровими.

Пристрої запису відео - прилади, призначені для запису, зберігання та відтворення зображень, що надходять від камер і мультиплексорів систем відеоспостереження.

Відеомонітори – пристрої, призначені для цілодобового відображення подій, що відбуваються на об'єкті, що охороняється.

Відеоквадратори - це цифрові пристрої, що забезпечують виведення зображень від чотирьох відеокамер на один монітор, екран якого в цьому випадку ділиться на 4 частини (квадранти). Квадратори високої роздільної здатності дозволяють працювати на одному моніторі з 8 камерами. Вони формують дві групи по 4 камери та дають можливість по черзі виводити їх на екран. Розрізняють відеоквадратори «реального часу», що забезпечують одночасну зміну зображень у всіх 4 квадрантах, та відеоквадратори послідовного типу, що забезпечують швидкість зміни зображень у кожному квадранті з частотою в 4 рази нижчою за номінальну частоту полів

Більшість квадраторів можуть працювати як світильники послідовної дії, тобто підключати будь-яку з камер, що працюють, до монітора. Квадратори повинні

мати додаткові (за кількістю камер) тривожні входи для підключення засобів сигналізації та забезпечувати виведення відеосигналу на повний екран під час спрацьовування у її зоні спостереження засобів сигналізації.

Квадратор можна використовувати і для запису на відеомагнітофон, але при цьому на магнітофон записуються всі чотири камери (квадрована картинка).

Відеомультиплексор - це один із пристроїв системи відеоспостереження, що дозволяє сигнал, що надходить з камер відеоспостереження, направити відразу на кілька каналів, що виходять - на монітор для перегляду і на запис (наприклад, на відеомагнітофон). Крім того, говорячи про демонстрацію сигналу з відеокамер на моніторі, слід зазначити, що відеомультиплексор дозволяє відобразити на одному екрані зображення відразу з декількох відеокамер. Наприклад, 16-канальний мультиплексор дозволить зобразити на моніторі зображення з 16 (або менше) камер. Взагалі слово мультиплексація означає об'єднання декількох каналів даних в один.

Так само відеомультиплексор дозволяє здійснювати запис з декількох відеокамер на один носій. При відтворенні це виглядає так, що спочатку показується зображення з однієї камери, потім з іншої, і так далі.

У разі настання тривожної ситуації («тривожний вхід») відеомультиплексор може працювати у наступних режимах (тут ми розглядаємо варіант, коли мультиплексор продовжив працювати у стандартному режимі).

• Ексклюзивний. На моніторі відображається лише сигнал із камери, що спостерігає за місцем виникнення тривожної ситуації.

• Пріоритетний. Картинки починають змінюватися не в звичайному порядку, а в такому: сигнал із місця

виникнення тривожної ситуації, сигнал із наступної відеокамери, знову з тривожного входу тощо.

• Режим індивідуального налаштування. Оператор сам може настроїти порядок демонстрації зображень у разі виникнення тривожної ситуації. Також він може самостійно перемикати відображення сигналів із відеокамер.

Відеодетектор руху являє собою апаратно-програмний засіб, що входить до складу системи охоронного спостереження і забезпечує автоматичне виявлення об'єктів, що рухаються в потоковому відео. На практиці такі технічні засоби повинні не тільки детектувати об'єкти, що рухаються, але і забезпечувати їх безперервний супровід (трасування) в поле зору однієї або навіть декількох камер. Ця функція необхідна зниження частоти помилкових і особливо повторних спрацьовувань, і навіть візуалізації траєкторії руху на екрані оператора. Відеодетектори багаторазово підвищують продуктивність роботи співробітників безпеки. Метадані, що генеруються детектором, можуть використовуватися як індекс для оперативного пошуку подій у відеоархіві. У цьому випадку у оператора відпадає необхідність у виснажливому перегляді багатоденного відеозапису.

Хороший детектор може значно підвищити ефективність використання сховищ даних та каналів зв'язку за рахунок зменшення надмірності відеоматеріалів. У системах охорони периметра економія дискового простору та мережевого трафіку збільшується в десятки – тисячі разів залежно від жвавості контрольованих ділянок

Відеодетектори можуть бути реалізовані як на сервері системи безпеки або інтегровані безпосередньо в камеру. В останньому випадку виробник камери використовує сигнальний процесор (DSP) або мікросхему замовлення (ASIC) для обробки потокового відео в

реальному масштабі часу. Багато сучасних IP-камери мають вбудований детектор руху.

Відеореєстратор (DVR) – пристрій для перегляду, запису та зберігання відеоінформації, отриманої з камер відеоспостереження . В даний час, запис на відеореєстратор є найпопулярнішим методом отримання відеоінформації кінцевим користувачем. Відеореєстратор має у своєму складі АЦП, який обробляє аналоговий відеосигнал, що надходить з камер, і перетворює на цифровий відеосигнал, який з різним типом компресії, за допомогою процесора, записується на носій інформації, як правило, жорсткий диск. Також, залежно від функціональної оснащеності, відеореєстратор може записувати аудіосигнал, що надходить із відеокамер; відеореєстратор може здійснювати управління PTZ - камерами, вести запис з руху та багато іншого. За допомогою мережного відеореєстратора (NVR) стало можливим, віддалено отримувати відеоінформацію з камер, як в режимі запису, так і Online через локальну мережу або через Інтернет.

IVR – це відеореєстратор для Інтернету, який може працювати на слабких каналах Інтернету та навіть без постійного Інтернету.

Принцип «коротких даних» ефективніший, ніж нескінченні відеопотоки. Короткі ролики повністю передають сенс довгих сюжетів, показують всі прикмети осіб, що беруть участь, швидко доходять до потрібних людей і легко проглядаються всі разом і відразу - без тривалого програвання кожного відеоканалу.

Відеоаналітика з глибоким навчанням, що базується на нейронних мережах

Відеоаналітика – технологія, що використовує методи комп'ютерного зору для автоматизованого

отримання різних даних на підставі аналізу послідовності зображень, що надходять із відеокамер у режимі реального часу або з архівних записів. Відеоаналітика є програмним забезпеченням (ПЗ) для роботи з відеоконтентом. В основі програмного забезпечення лежить комплекс алгоритмів машинного зору, що дозволяють вести відеомоніторинг та проводити аналіз даних без прямої участі людини. Алгоритми відеоаналітики можуть бути інтегровані в різні бізнес-системи, які найчастіше використовуються у відеоспостереженні та інших сферах безпеки.

Нейронна мережа (також штучна нейронна мережа, ІНС) - математична модель, і навіть її програмне чи апаратне втілення, побудована за принципом організації та функціонування біологічних нейронних мереж - мереж нервових клітин живого організму. Це поняття виникло щодо процесів, які у мозку, і за спробі змоделювати ці процеси.

Глибоке навчання вважається останнім етапом розвитку штучного інтелекту. Застосовується в різних галузях промисловості, щоб допомогти комп'ютерам краще розуміти та оцінювати різні ситуації.

Концепція машинного навчання

Машинне навчання (Machine Learning) - великий підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, здатних навчатися. Розрізняють два типи навчання. Навчання за прецедентами, або індуктивне навчання, ґрунтується на виявленні загальних закономірностей за приватними емпіричними даними. Дедуктивне навчання передбачає формалізацію знань експертів та його перенесення на комп'ютер як бази знань. Дедуктивне навчання прийнято відносити до галузі експертних систем, тому терміни машинне навчання та навчання за прецедентами можна вважати синонімами.

Машинне навчання знаходиться на стику математичної статистики, методів оптимізації та класичних математичних дисциплін, але має також і власну специфіку, пов'язану з проблемами обчислювальної ефективності та перенавчання. Багато методів індуктивного навчання розроблялися як альтернатива класичним статистичним підходам. Багато методів тісно пов'язані з вилученням інформації та інтелектуальним аналізом даних (Data Mining).

Найбільш теоретичні розділи машинного навчання поєднані в окремий напрямок, теорію обчислювального навчання (Computational Learning Theory, COLT).

Машинне навчання - як математична, а й практична, інженерна дисципліна. Чиста теорія, як правило, не призводить відразу до методів та алгоритмів, які застосовуються на практиці. Щоб змусити їх добре працювати, доводиться винаходити додаткові евристики, що компенсують невідповідність зроблених теоретично умов реальних завдань. Майже жодне дослідження в машинному навчанні не обходиться без експерименту на модельних або реальних даних, що підтверджує практичну працездатність методу.

Системи із глибоким навчанням

Глибоке навчання – технологія глибокого навчання, яка застосовується у IP камерах Hikvision DeepinView та NVR серії DeepinMind.

Розробники технології ґрунтувалися на особливостях людського мозку – побудові його нейромереж, процесів навчання та пам'яті, намагаючись використати принципи їхньої роботи та моделюючи структуру мільярдів взаємопов'язаних нейронів. В результаті цього, «глибоке навчання» є поетапним процесом, схожим на процес навчання людини.

У разі впровадження системи відеомоніторингу стану безпеки сучасні технології відеоспостереження, інтегровані з аналітичними алгоритмами та штучним інтелектом, здатні в режимі реального часу:

- розпізнавати загрози та допомагати правоохоронцям запобігати злочинам;

-сприяти ефективному розслідуванню правопорушень;

-зменшувати людський чинник у питаннях безпеки, що мінімізує корупційні ризики;

-покращувати координацію між правоохоронними структурами;

-слугувати елементом швидкого реагування на надзвичайні ситуації.

6. Безпека відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України

Враховуючи, що відеоспостереження та відеоаналітика стали невід'ємною частиною сучасної інфраструктури безпеки, починаючи від моніторингу громадських місць і закінчуючи забезпеченням безпеки на приватних об'єктах, розширення використання цих технологій також створює нові та складні загрози безпеці, які вимагають ретельного аналізу та впровадження ефективних заходів захисту. Слід виокремити основні загрози стосовно забезпечення безпечної роботи із зазначеними системами.

1. *Загрози конфіденційності даних*

Камери відеоспостереження збирають величезні обсяги візуальної інформації, яка часто містить особисті дані. Це може бути зовнішність людей, їхня поведінка, номерні знаки автомобілів, а в деяких випадках навіть чутлива інформація, така як медичні або біометричні дані, якщо система використовує розширені функції розпізнавання. Якщо системи відеоспостереження не мають належного захисту, сторонні особи можуть отримати доступ до записів, що призведе до витоку конфіденційної інформації. Це може бути результатом слабких паролів, незахищених мережевих підключень або вразливостей програмного забезпечення.

Навіть якщо доступ санкціонований, існує ризик використання зібраних даних не за призначенням. Наприклад, відеозаписи можуть бути використані для стеження за окремими особами, збору маркетингових даних без згоди або навіть для злочинних цілей, таких як шантаж.

Технології відеоаналітики, зокрема розпізнавання обличь та аналіз поведінки, можуть значно зменшити або повністю усунути анонімність осіб, які потрапляють в поле

зору камер, що викликає виникнення проблем з забезпечення конфіденційності, приватного життя та свобод громадян.

Дотримання вимоги стосовно цілісності отриманих відеоданих є критично важливою для їхнього використання як доказу в ході судового розгляду або для розслідування інцидентів. Зловмисники можуть змінювати, видаляти або вставляти фейкові кадри у відеозаписи, в тому числі і з використанням штучного інтелекту, щоб змінити хід подій або приховати злочин. Це може бути зроблено за допомогою спеціалізованого програмного забезпечення для редагування відео. Тому, будь-яке втручання або спотворення даних може зробити їх непридатними для використання.

Крім того, несправність обладнання, програмні помилки або спеціально створені шкідливі програми можуть призвести до спотворення або пошкодження відеозаписів, що робить їх непридатними для аналізу. За допомогою цих програм зловмисники можуть видалити важливі відеозаписи для приховування своїх дій або для того, щоб перешкодити розслідуванню.

2. Загрози доступності систем

Доступність систем відеоспостереження та відеоаналітики є досить важливою для ефективного моніторингу та швидкого реагування на інциденти. Системи відеоспостереження, особливо ті, що підключені до Інтернету, можуть бути об'єктом DDoS-атак, які перевантажують мережу або сервери, роблячи систему недоступною. Несправність камер, записуючих пристроїв, серверів або мережевого обладнання може призвести до тимчасової або постійної недоступності системи.

Перебої в електропостачанні можуть вивести з ладу всю систему відеоспостереження, якщо немає резервних джерел живлення, а програмні в програмному забезпеченні

або збої в роботі операційної системи можуть призвести до нестабільної роботи або повного відключення системи.

Окрім зазначених загроз окремо слід виділити загрози*, пов'язані з відеоаналітикою.*

Системи відеоаналітики, що використовують штучний інтелект та машинне навчання для обробки відеоданих, також піддаються специфічним загрозам серед яких можливо зазначити:

- "Отруєння" даних навчання - відбувається, коли зловмисники впливають на моделі навчання, щоб отримати певний результат або створити упереджену інформаційну модель вставляючи спотворені або неправдиві дані, що приносить користь зловмиснику. Це може призвести до того, що система буде робити неправильні висновки або ідентифікувати неіснуючі загрози.

- Обхід алгоритмів розпізнавання за допомогою спеціальних методів або навіть макіяжу та одягу, зловмисники можуть обійти алгоритми розпізнавання обличь або поведінки, залишаючись непоміченими системою.

- Неправильно налаштовані або недостатньо точні алгоритми відеоаналітики можуть генерувати велику кількість помилкових спрацьовувань, що призводить до втрати часу операторів та зниження ефективності системи.

3. Загрози з боку внутрішніх зловмисників

Також не варто недооцінювати загрози, що виходять від внутрішніх зловмисників, тобто співробітників, які мають доступ до систем відеоспостереження. Враховуючи, що вони мають доступ до відеозаписів або налаштувань системи, тому можуть використовувати свої права для несанкціонованого перегляду, копіювання, видалення або маніпуляцій з даними.

Навіть без злого наміру, співробітники можуть припуститися помилок, які призведуть до порушення

безпеки, наприклад, залишити відкритим доступ до системи або випадково видалити важливі файли, а співробітники які не задоволені відношенням до них з боку керівництва, або звільнені можуть спробувати саботувати систему відеоспостереження, пошкодивши обладнання або знищивши дані.

Таким чином, для мінімізації зазначених загроз необхідно впровадити комплексний підхід до безпеки, який включає технічні, організаційні та правові заходи.

По-перше, посилення захисту даних, які полягають у використанні шифрування для передачі та зберігання відеоданих, та застосування надійних механізми автентифікації та авторизації, регулярне резервне копіювання.

По- друге, впровадження контролю цифрових підписів для відеозаписів, фіксація всіх дій входу у систему у відповідних системних журналах.

По - третє, регулярне оновлення програмного забезпечення та прошивок камер, моніторинг мережевого трафіку та системних журналів які допомагають відстежувати і аналізувати мережеву активність, щоб виявляти проблеми, оптимізувати мережу та забезпечувати її безпеку. Вони можуть бути як програмним забезпеченням, так і спеціальними пристроями. Ці журнали використовуються для отримання інформації про мережеву активність, наприклад, про обсяг трафіку, IP-адреси, протоколи та інші важливі дані.

По-четверте, для розробки політики безпеки чітко визначити права доступу, правил використання даних, процедур реагування на інциденти.

Враховуючи викладене можливо зробити висновок, ігнорування загроз безпеки в системах відеоспостереження та відеоаналітики може призвести до серйозних наслідків, включаючи фінансові збитки, репутаційні ризики, судові

позови та порушення приватного життя. Тому інвестування в надійні заходи безпеки є не просто бажаним, а критично важливим аспектом розгортання та експлуатації цих технологій.

Перелік використаних джерел

1. Білоус Р. В. Кримінальний аналіз в діяльності правоохоронних органів України. Удосконалення механізму правового регулювання суспільних відносин з урахуванням зарубіжного досвіду : зб. матеріалів Міжнар. наук.-практ. конф. (Київ, 1 черв. 2020 р.) / відп. ред. О. Ю. Бусол. Київ : Ліра-К, 2020. С. 20–22.
2. В Україні працює близько 19 тисяч камер відеоспостереження, але бракує законодавчого регулювання – експерти. URL: http://uacrisis.org/ua/73640-videosurveillance-regulations (дата звернення: 12.04.2025).
3. Використання відеоаналітики у роботі Національної поліції. Методичні рекомендації. Мирошниченко В.О, Кочеткова. І.Б. Махницький О.В. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2020 34 с.
4. Відеоаналітика URL: https://uk.wikipedia.org/wiki/Відеоаналітика (дата звернення: 17.04.2025).
5. Дамьяновскі Владо Роль відеоспостереження в розслідуванні серйозних інцидентів 19 серпня 2017 URL:https://worldvision.com.ua
6. Дмитро Черноусов Досвід застосування безпілотних літальних апаратів підрозділами міністерства внутрішніх справ у сучасних умовах ведення війни. *Збірник наукових праць Національної академії прикордонної служби України*. Том 97 № 4 (2024)
7. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду: метод. матеріали для працівників підрозділів поліції МВС України / В. А. Коршенко, М. В. Мордвинцев, Ю. В.

Гнусов та ін. Харків : Харків. нац. ун-т внутр. справ, 2020. 44 с.
8. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. Львів: ЛьвДУВС, 2015. 492 с.
9. Інформаційна газета Liga.net. URL: https://news.liga.net/society/news/ avakov-skazal-gde-v-ukraine-samyy-nizkiy-uroven-prestupnosti (дата звернення: 17.04.2025).
10. Комарова О. Сучасні системи безпеки: чи змінюється служба в поліції? URL:https://www.radiosvoboda.org (дата звернення: 17.04.2025).
11. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) URL: https://zakon.rada.gov.ua (дата звернення: 17.04.2025).
12. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) URL: https://zakon.rada.gov.ua (дата звернення: 17.04.2025).
13. Коршенко, В. А., Чумак, В. В., Мордвинцев, М. В. і 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 №77(2), с. 86-92
14. Кримінальний кодекс України від 05.04.2001 № 2341-14. URL: http://zakon.rada.gov.ua/laws (дата звернення: 17.04.2025).
15. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI URL: https://zakon.rada.gov.ua
16. Мирошниченко В.О. «Динамічний фоторобот» людини та перспективи його використання. *Протидія*

організованій злочинній діяльності: матеріали всеукраїнської наук.-практ. інтернет-конф. м. Одеса, 31 бер. 2017 р. Одеса, 2017. с.103-105.
17. Мирошниченко В.О. Аналіз біометричних систем ідентифікації особи в умовах діяльності правоохоронних органів / *Науковий вісник Дніпроп. держ. ун- ту внутр. справ.* 2007. Вип. 1(32). С. 314-321.
18. Нагрудна камера (відеореєстратор) патрульного: правове регулювання і порушення права на приватність. URL: http://umdpl.info/police- experts.info
19. Наказ Департаменту патрульної поліції НПУ від 03.02.2016 року № 100, яким затверджено «Інструкцію про порядок зберігання, видачі, приймання, використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції та доступ до відеозаписів з них», URL: https://zakon.rada.gov.ua (дата звернення: 17.04.2025).
20. Ольга Комарова. Сучасні системи безпеки: чи змінюється служба в поліції? URL:https://www.radiosvoboda.org
21. Патрульна поліція запускає ще 57 нових камер для фіксації руху на дорогах. URL: https://delo.ua
22. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних система: Постанова КМУ від 8 лютого 2021 року № 92. URL: https://zakon.rada.gov.ua
23. Про єдину інформаційну систему Міністерства внутрішніх справ: Постанова Кабінету Міністрів України № 1024 від 14 листопада 2018 р. URL:https://zakon.rada.gov.ua
24. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03.08.2017. № 676. URL:https://zakon.rada.gov.ua

25. Інструкція з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ МВС України від 27.04.2020 № 357. URL:https://zakon.rada.gov.ua
26. Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України: Наказ Адміністрації Державної прикордонної служби України 30.09.2008. № 810 URL: https://zakon.rada.gov.ua
27. Русило М.О., Мирошниченко В.О. Використання сучасних технологій відеоаналітики в органах Національної поліції. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса: ОДУВС, 2019. 108 с.
28. Ситуаційні центри та командні пункти. Проект «Безпечне місто». URL: https://leater.com/ua/services/bezpechne-m-sto.html (дата звернення: 17.04.2025).
29. Спеціальна техніка Національної поліції України: навч. посіб. з дисц. «Тактико-спеціальна підготовка» / Ю. В. Гнусов, В. А. Світличний, Ю. М. Онищенко. Харк. нац. ун-т внутр. справ, факультет № 4, каф. кібербезпеки. Х.: ХНУВС, 2017. 175 с.
30. У Києві вводять автофіксацію порушень ПДР: де встановлять перші камери. URL: https://www.segodnya.ua/ua/economics/avto/v-kieve-vvodyat-avtomaticheskuyu-fiksaciyu-i-shtrafy-za-narusheniya-pdd-gde-ustanovyat-pervye- kamery-1362444.html

Науково-методичне видання

Калугін *Володимир Юрійович*
Форос *Ганна Володимирівна*

ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ ТА ВІДЕОСПОСТЕРЕЖЕННЯ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

НАУКОВО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Підп. до друку 19.06.2025. Формат 60х84/16.
Друк цифровий. Папір офсетний. Гарнітура Times.
Ум.-друк. арк. 4,42. Обл.-вид. арк.3,024.
Наклад 30 прим.
Надруковано з готового оригінал-макета.
Поліграфічне відділення
Одеського державного університету внутрішніх справ
м. Одеса, вул. Успенська,1,
Свідоцтво суб'єкта видавничої справи ДП № 3507 від 25.06.2009
e-mail rvv@oduvs.edu.ua