ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Махницький О.В., Мирошниченко В.О, Кочеткова І.Б.

Використання відеоаналітики у роботі Національної поліції

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Дніпро – 2020

УДК 34+004 (075) М 36
Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 10 від 18 червня 2020 р.)

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.

Рецензенти:
Сергій СВИРИДЕНКО – начальник УІАП ГУНП в Дніпропетровській області.
Григорій КОРОТЕНКО – доктор технічних наук, професор кафедри геоінформаціних систем Національного технічного університету «Дніпровська політехніка»

У даних методичних рекомендаціях розглянуто приклади використання аналітичних Smart функцій (інтелектуальних детекторів за подією), інтегрованих у обладнання, що використовується при побудові систем «Безпечне місто». Описані переваги використання автоматичних функцій у роботі підрозділів національної поліції при виявленні виникнення нетипових ситуацій та режимів НС. Окрему увагу приділено питанням та сучасним проблемам застосування відеоаналітики у сфері дорожнього руху.

Наряду з технічними питаннями, у методичних рекомендаціях розглядаються також і юридичні аспекти застосування відеофіксуючих пристроїв.

Методичні рекомендації можуть бути корисними для практичних працівників національної поліції, спеціалістам з проектування та обслуговування систем відеоаналітики, а також при підготовці майбутніх правоохоронців.

Автори:

Мирошниченко Володимир Олексійович – к.т.н доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Махницький Олександр Васильович – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Кочеткова Інна Борисівна – викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ЗМІСТ

ВСТУП

В даний час системи відеоспостереження широко застосовуються для забезпечення охорони банків, торговельних центрів, розважальних закладів, промислових підприємств, інших комерційних і некомерційних організацій. Системи відеоспостереження дають змогу здійснювати швидке реагування на небезпечну ситуацію, спостереження за персоналом та відвідувачами, широке застосування та перспективи системи відеореєстрації мають в області контролю за дорожнім рухом тощо.

Відеоаналітіка – це програмний алгоритм, який дозволяє швидко та якісно обробляти відеодані й звільнити оператора від рутинної роботи стеження за безліччю камер для виявлення порушень.

Розвиток інтелектуальної відеоаналітики відбувається за двома основними технологіями – це трекінг та ідентифікація. На основі правил, закладених в алгоритм відеоаналізу, будується весь функціонал системи, який вкрай необхідний для побудови сучасних систем відеоспостереження.

Трекінг – це коли алгоритм обробки відео шукає в кадрі рух, визначає та класифікує об'єкт, що рухається, описує його характеристики (розмір, колір, швидкість).

Ситуаційні детектори – це коли об’єкт спостереження перетинає уявні лінії в кадрі, після чого система видає сигнал тривоги:

- перетин об'єктом прямої лінії в заданому напрямку;
- рух в зоні;
- вихід об'єкта із зони;
- зупинка об'єкта в зоні;
- залишений в зоні предмет.

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

Актуальність. Наразі дана тема має велике значення у потоці різноманітних технологій, які допомагають сприяти працівникам органів внутрішніх справ, а особливо поліції, у розкритті, розслідуванні та попередженні злочинної діяльності. Сучасний світ має змогу за допомогою технологій, моментально отримати потрібну інформацію людині. Важко зараз уявити роботу будь-якої організації чи компанії без використання відеоспостереження. Не є виключенням і сфера правоохоронних структур, в тому числі й поліція.

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

РОЗДІЛ І ПРАКТИЧНЕ ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ У ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

1.1 Відеоаналітика як одне з основних джерел отримання інформації для органів Національної поліції

Сучасні інформаційні технології вражають своїми можливостями та дозволяють як поліпшити життя звичайних пересічних громадян, так і сприяти ефективній роботі працівників Національної поліції. Адже за допомогою сучасних технологій обробки інформації та новітніх технік можливо виконати поставлені завдання з легкістю та швидкістю.

Основними завданнями, які можна та доцільно вирішувати за допомогою відео технологій, є:

– розпізнавання, адже найчастіше розпізнаються обличчя людей і номери автомобілів або вагонів;

– завдання, пов'язані з аналізом поведінки людини, автомобіля або іншого рухомого об'єкту;

– реалізація охоронних функцій на різноманітних об’єктах.

Традиційні камери відеоспостереження, які пристосовані для загального користування, на сьогоднішній день не задовольняють потреб в оперативному реагуванні на можливі позаштатні ситуації у місцях масових скупчень людей та на великих об'єктах транспортної інфраструктури. Для вирішення сучасних завдань потрібні комплексні інтелектуальні системи, в основі яких лежать складні алгоритми відеоаналітики та ідентифікації.

Ідентифікація – це розпізнавання образу за відеозображенням, групування за класами або конкретними шаблонами та порівняння із заздалегідь підготовленою базою еталонних зображень. Найпопулярнішими та найнеобхіднішими з них на сьогоднішній день є розпізнавання обличчя і розпізнавання автомобільних номерів.

У користуванні поліції є обладнання та пристрої для відеоспостереження, які володіють розширеними величезними налаштуваннями для якісної фіксації в денний або темний час зйомки з можливістю застосування посилення деталізації, промальовування картинки (як в HDR режимі) та іншими корисними ефектами, але таких технічних засобів не так багато, як хотілось би.

В режимі онлайн всі камери не використовуються. Але системи розпізнавання номерів працюють, впроваджується подібне і щодо визначення обличчя, як розповідає заступник голови Національної поліції Костянтин Бушуєв [1]. Такі системи успішно працюють в Донецькій області (Маріуполь), в Одесі, Чернігові, у Львові.

«Відеоресурс перебуває на балансі міста, місто обслуговує і встановлює камери. Питання розташування камер узгоджує із Національною поліцією. В Києві більше чотирьох з половиною тисяч камер. Поліція має прямий доступ до відео контенту в режимі онлайн, тобто не треба формувати запит для його отримання», – пояснює Костянтин Бушуєв [1].

Найчастіше у практиці Національної поліції камерами зовнішнього відеоспостереження обладнуються місця масового скупчення людей, і це, як правило, різного роду парки, сквери, площі, прилегла територія ринків і великих торгових центрів, аварійно-небезпечні ділянки доріг. За допомогою відеокамер може здійснюватися як цілодобовий моніторинг в реальному часі, так і ретроспективний пошук у архіві даних. Сигнали з камер відеоспостереження надходять на спеціальні передавачі, призначені для передачі в локальні комп'ютерні центри відеоконтролю. У цих центрах відбувається процес обробки, стиснення і передачі інформації через волоконно-оптичну мережу на Центральний пост відеоспостереження. Такий пост обладнується прямим каналом аудіозв'язку і режимом обміну відео інформацією з відділами поліції, а також комплектом екстреного зв'язку «тривожна кнопка» для виклику оперативної групи в разі вчинення злочину або правопорушення. За допомогою відеоспостереження співробітники поліції відстежують обстановку і самостійно приймають рішення про те, як діяти при виникненні нештатної ситуації. Але в

роботі традиційного відеоспостереження є величезний мінус – занадто багато залежить від людського фактору. Оператори змушені безперервно відстежувати великий потік інформації, ризикуючи пропустити щось важливе, особливо у кінці зміни, коли уважність персоналу знижується.

Статистика розкриття правопорушень, говорить про те, що при використанні систем відеоспостереження, шанс упіймання правопорушника підвищується у декілька разів. Наприклад, за 2018 рік записи з камер відеоспостереження допомогли розкрити понад 2,5 тисячі злочинів у Києві. Правоохоронці часто користуються камерами відеоспостереження для забезпечення правопорядку під час заходів масового скупчення людей, коли охороняється безпека учасників. Також в режимі онлайн поліцейські знаходять покинуті та залишені предмети, сумки, машини, які можуть бути припустимо небезпечними. Як свідчить статистика, це також є хорошим превентивним заходом, який попереджує вчинення злочинів або правоворушень.

Основними завданнями, які вирішують системи відеоспостереження, впроваджені в органах Національної поліції, є питання, пов'язані із забезпеченням безпеки громадян, а також питання контролю автоматизованого процесу використання отриманої інформації, який, як правило, постійно розвивається і стає все більш високотехнологічним.

Широкого застосування в органах Національної поліції знаходять «замкнуті телевізійні системи» (CCTV – Closed Circuit TeleVision), які ще називають охоронними відеосистемами. Основними елементами таких систем є:

– відеокамери;

– комутаційні пристрої;

– пристрої відображення (монітори);

– пристрої документування;

– канали передачі відеосигналу.

Кнопки тривожних сповіщень призначені для непомітної миттєвої подачі сигналу тривоги при загрозі фізичного нападу злочинців на охоронюваний об’єкт та його персонал. Такими кнопками різних конструкцій та модифікацій

обладнуються робочі місця касирів, контролерів кредитно-фінансових установ, керівників підприємств, барменів, тощо. Останнім часом широкого застосування набули радіокеровані кнопки тривожного сповіщення (РКТС), що збільшує мобільність персоналу і краще забезпечує безпеку співробітників. Пристрої резервного живлення встановлюються на об’єктах з метою забезпечення охоронних систем безперебійним електроживленням у випадку масових відключень електроенергії або стихійних лих. Підбір виду, конструкції і потужності таких технічних засобів виконується в індивідуальному порядку залежно від категорійності об’єкта і сумарної потужності споживачів електроенергії [2].

Отже, використання відповідного обладнання та пристроїв для відеоспостереження, які мають розширені технічні характеристики та налаштування для якісної фіксації в денний або темний час зйомки, відеотехнологій обробки отриманої таким чином інформації у роботі Національної поліції має величезне значення у розкритті та попередженні злочинів і у профілактиці правопорушень.

1.2 Використання інформації, отриманої за допомогою відеоспостереження

За допомогою сучасних системи відеоспостереження можливо знаходити у людському потоці підозрілих осіб, покинуті речі, які можуть становити небезпеку для оточуючих, виявляти ознаки скоєння злочинів та правопорушень та слідкувати за діями безпосередньо поліцейських. За допомогою сучасних можливостей відеозйомки впізнання особи стає легшим та простішим. Відомо, що людина володіє індивідуальністю (неповторністю) зовнішнього вигляду і відносною стійкістю ознак. Процес ідентифікації полягає в порівнянні двох (або декількох) сукупностей ознак між собою. Тому для ідентифікації необхідно виділити ці ознаки.

Відповідно до сучасного кримінально-процесуального законодавства матеріали відеозапису можуть виступати в якості доказів у кримінальній справі, будучи додатками протоколів слідчих і судових дій, речовими доказами, а також іншими документами [3].

Більш складним завданням є розпізнавання осіб, коли від системи потрібно, по-перше, виділити особу в натовпі, а потім однозначно визначити (ідентифікувати) конкретну людину [4], порівнявши зображення, отримане з камери, з фотографією в базі даних. Критеріями якості роботи таких систем є точність (частка правильно ідентифікованих і пропущених осіб), швидкість розпізнавання, а також час на пошук і порівняння з особами з бази даних. При описі зовнішності людини криміналістично значущими ознаками особи є: волосяний покрив голови, лоб, брови, очі, повіки, щоки, ніс, губи, зуби, підборіддя, вушні раковини. Однак у конкретному елементі при поглибленому його вивченні можна виділити ще складові частини:

при описі очей - будова очної щілини, виступання очних яблук, вид внутрішніх кутів очей;

при описі носа - перенісся, спинка носа, підстава носа, крила носа.

При цьому кожен елемент зовнішності може характеризуватися такими ознаками: формою, розміром, положенням, кольором. Парні елементи також мають симетрію або асиметрію. Кожна ознака має три значення вираженості (два крайніх і одне середнє). На думку фахівців, загальне число людей, з яких може бути виділено кожну особу за сукупністю цих ознак, дорівнюватиме 950. Відстежити обличчя людини у переповненому залі очікування (на вокзалі) вкрай складно, тому ще одним важливим елементом ідентифікації може бути так званий «динамічний фоторобот» [5]. Виходячи з цього, завдання, які необхідно вирішувати у роботі поліцейських, завжди на порядок складніше, ніж просто відеоспостереження.

Другою великою проблемою при використанні відеотехнологій у роботі Національної поліції є, як правило, погані умови освітлення. Для роботи оглядового відеоспостереження освітленості може бути досить, але, наприклад,

в зоні, де встановлюються системи дистанційного розпізнавання осіб, освітленість повинна бути 300-400 лк. Зручніше за все розпізнати людину в переході, оскільки зазвичай особи рухаються там по певних траєкторіях. Але там, як правило, освітленість приблизно 100 лк, та цього для надійної роботи системи розпізнавання не достатньо [6]. Для роботи відеоаналітичних систем це створює великі проблеми. Доводиться в кожному конкретному випадку шукати нове нестандартне рішення цієї задачі.

Злочинці також стежать за розвитком сучасної техніки та технологій, і використовують в своїх цілях найсучасніші розробки. Завдання відеоаналітики – вчасно їх виявити, запобігти виникненню позаштатної ситуації та далі діяти на випередження.

Як відомо, в роботі по розкриттю злочинів важливе значення має фактор часу. Більшість злочинів розкривається в результаті розшуку злочинців «по гарячих слідах». Тому, чим раніше стане відомо органам поліції про скоєний злочин, чим швидше вони використають отриману інформацію, тим реальніше можливість швидко виявити і затримати злочинця. Це пояснюється тим, що злочинці іноді протягом деякого часу після вчинення злочину знаходяться в місцях, де встановлені камери відеоспостереження, та можуть зберігати на собі сліди злочину і мати предмети, здобуті злочинним шляхом. Використовуючи новітні методи отримання та обробки відеоматеріалу, можна здійснювати безперервний збір та передачу, інтелектуальний аналіз і архівування відеоданих від великого числа камер з можливістю оперативного відображення і доступу до відео архіву з робочих місць операторів. Захищені від вандалів камери рекомендується встановлювати на території міста в найбільш криміногенних місцях, місцях скупчення людей, під'їздах житлових будинків, дорогах, провулках, паркуваннях транспорту і т.д.

Перспективними напрямками застосування інформаційної відеоаналітики може бути запобігання заворушень у місцях масового проходу людей. Так, біометричне впізнання може бути превентивним заходом, який дозволить звести до мінімуму небезпеку виникнення скупченості та несподіваних конфліктів,

наприклад, на вході, оскільки це дасть змогу у рази підвищити пропускну можливість у зоні турнікетів [7].

Слід зазначити, що збільшення кількості камер потребує збільшення ресурсів для обробки інформації, яка надходить з цих камер. Мова йде як про апаратні ресурси системи, так і про людські ресурси, адже для того, щоб виявити позаштатну ситуацію та вірно на неї відреагувати, потрібно втручання людини. Але використання SMART функцій, що вже інтегровані у більшість сучасних камер, може значно зменшити час на виявлення та фіксування позаштатної ситуації.

1.3 Огляд аналітичних Smart функцій

(розглянуто на прикладі обладнання компанії Hikvision, та описано призначення та налаштування кожної функції окремо)

Що таке Smart функції, для чого вони потрібні і чим вони відрізняються від стандартних функцій виявлення? Розглянемо на прикладі стандартного методу налаштування обладнання. Як показує практика, в 80% випадків налаштування, інсталятори використовують простий метод налаштування пристроїв, а саме вибирають режим постійного запису або запис по програмному детектору руху, який підтримують всі самостійні пристрої, щоб уникнути труднощів. При роботі системи, яка налаштована таким методом, є незручності: не зовсім зручно здійснювати пошук або контроль подій, робота з архівом займає багато часу, багато хибних тривог, які викликані сторонніми предметами або об'єктами, нераціональне використання ємності диска. Щоб уникнути всіх цих незручностей, потрібно застосовувати «Smart події».

Smart – це інтелектуальний детектор за подією. Smart детектор застосовується для запису тільки корисних подій за особливими правилами, які розробляє сам користувач. У випадку використання Smart функцій відео архів буде містити тільки корисні та важливі події, які будуть записуватися тільки при появі позаштатної ситуації. Існує десять стандартних Smart правил: *перетин лінії, вторгнення в зону, аудіо детектор, розфокусировка об'єктива, зміна сцени кадру, вхід в зону, вихід із зони, детекція осіб, виявлення залишених предметів, виявлення зниклих об'єктів*.

IVS (*Intelligent Video System*) – це алгоритми роботи Smart подій в системах відео нагляду та охорони. Розглянемо налаштування кожної функції окремо:

Налаштування розкладу.

Обов'язковою і необхідною умовою роботи Smart- функцій (але не всіх) є налаштування розкладу. Без налаштування цього пункту, функція не почне свою роботу. На Рис. 1 показано меню, де за допомогою горизонтальних індикаторів можна встановити тимчасові діапазони роботи для кожного дня індивідуально.

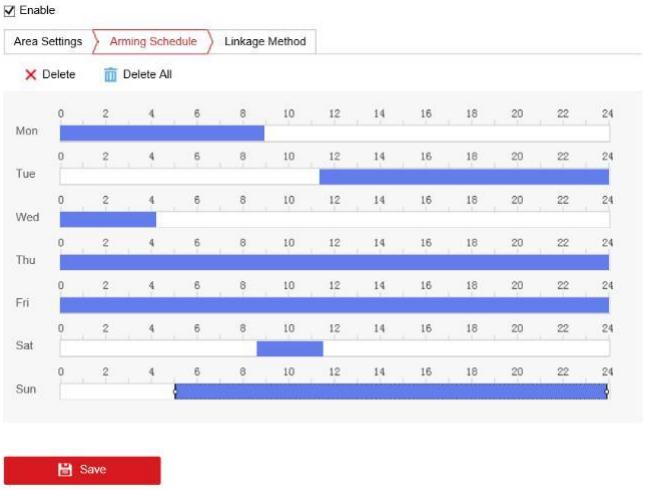


Рис. 1

Налаштування виду тревоги (Рис 2):

- відправка е-мейла (Send Email)

- відправка в центр (Notify Surveillance Center) (наприклад в IVMS)

- відправка на FTP / запис на SD-карту (Upload to FTP / Memory Card)

- відправка сигналу на «тривожний» вихід (реле)

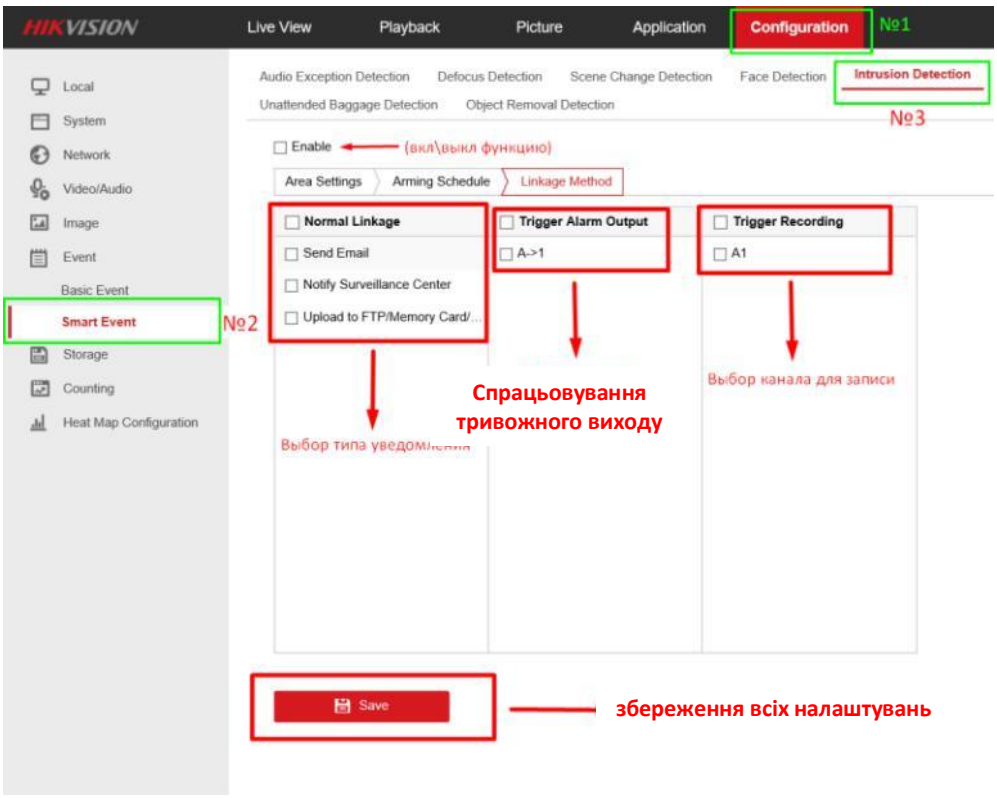


Рис. 2

1.3.1. **Детекція аудіо виключення** (**Audio Exception Detection**)

Функція дозволяє настроїти спрацьовування тривоги на певний зміни шумового фону (підвищення або зниження зовнішнього шуму).

Шлях для включення функції показаний на Рис. 3

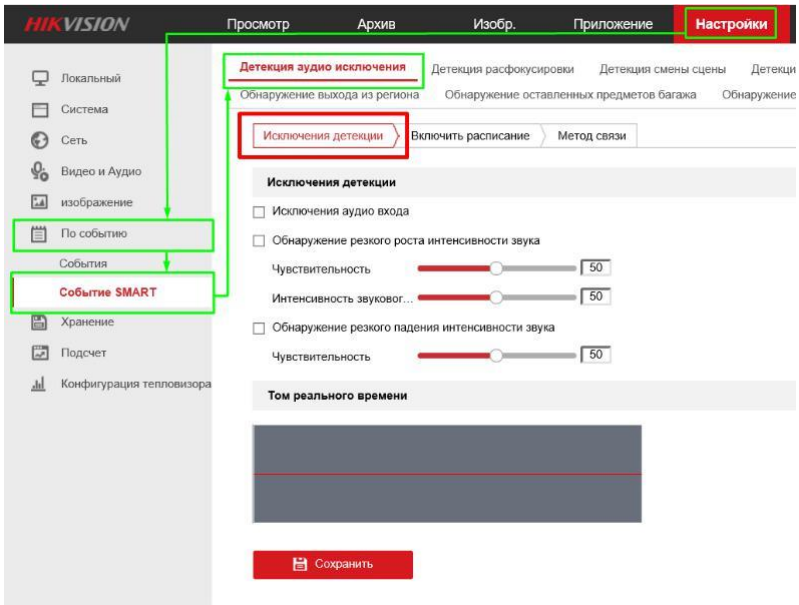


Рис. 3

У розділі «Винятки детекції» є наступні пункти:

Винятки аудіо входу (Audio Loss Detection) – включення / вимикання функції.

Виявлення різкого зростання інтенсивності звуку (Sudden Increase of Sound Intensity Detection) – дозволяє налаштувати мінімальний шумовий поріг, перевищення якого активує запис відео або відправлення повідомлень.

- *Чутливість* (Sensitivity) (від 1 до 100) – налаштування чутливості мікрофона. Чим менше це значення, тим сильніше реакція на зміну звукового фону і частіше спрацьовування в одиницю часу.

- *Інтенсивність звукового порогу* (Sound Intensity Threshold) (від 1 до 100) – налаштування мінімального шумового порогу. Якщо шум перевищує цей поріг - відбудеться спрацювання детектора.

Приклад зміни чутливості і інтенсивності звукового порогу представлений на рисунках нижче. Як можна помітити – на Рис. 4 межа інтенсивності звукового порогу на правій частині вище, ніж на лівій.

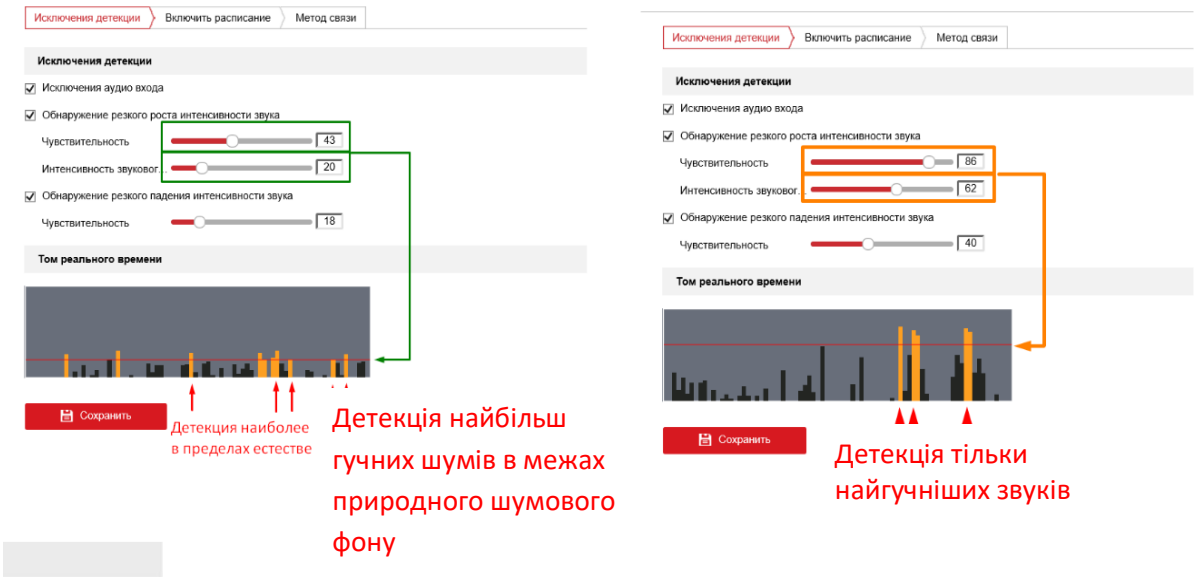


Рис. 4)

- *Виявлення різкого падіння інтенсивності звуку* (Sudden Decrease of Sound Intensity Detection). Функція обернена до попередньої. В умовах постійного шуму можна встановити порогове значення, і якщо шум знизиться нижче цього порога, то цей момент буде розцінений як «спрацювання», активується запис відео або відправка повідомлень.

- *Чутливість* (Sensitivity) (від 1 до 100) – параметр так само можна відрегулювати. Чим менше це значення, тим сильніше реакція на зміну звукового фону і частіше спрацьовування в одиницю часу.

Приклад моделювання ситуації можна бачити на Рис.5

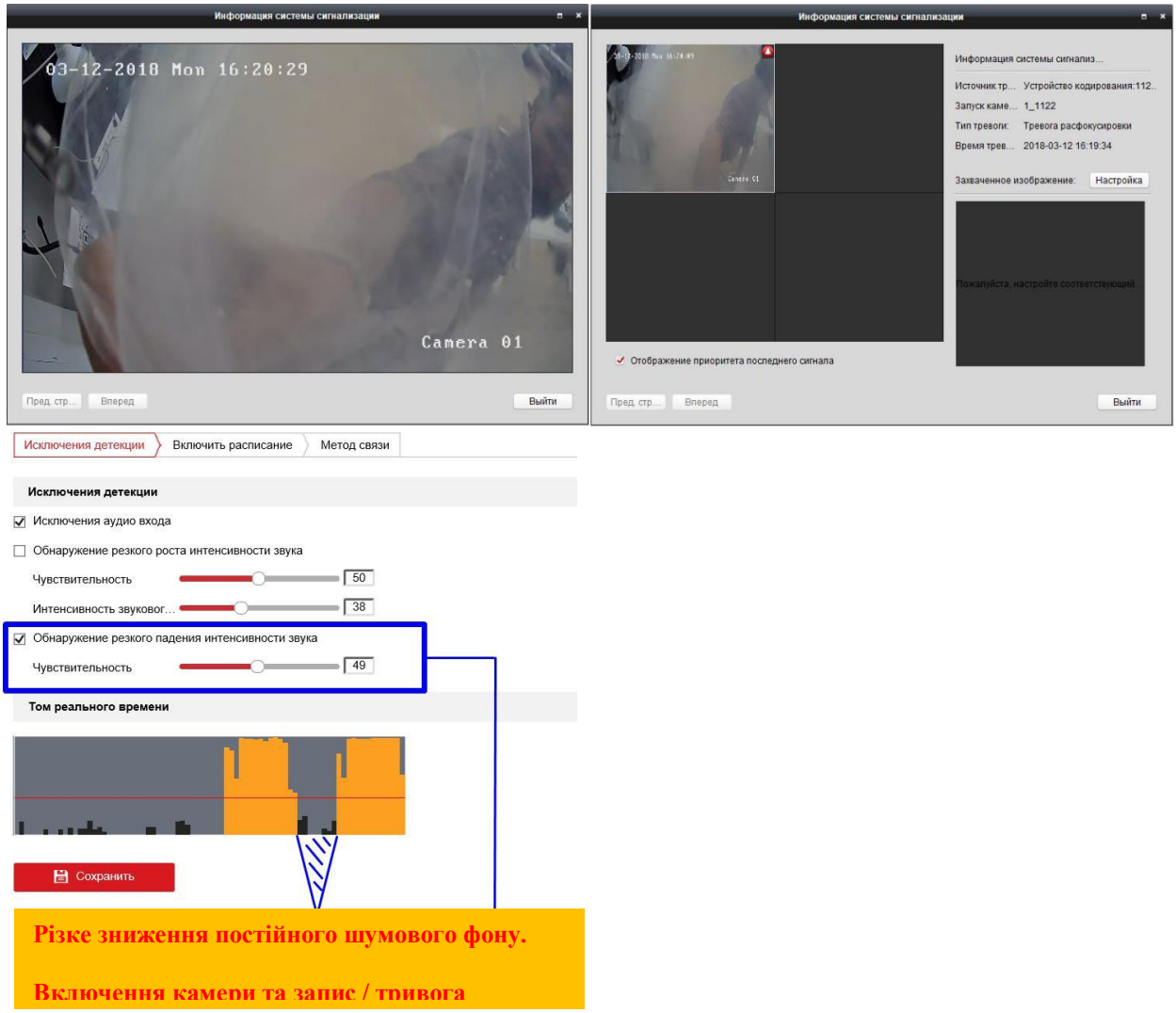


Рис.5

1.3.2. Детекція розфокусування (Configuring Defocus Detection)

Функція дозволяє настроїти спрацьовування тривоги на розфокусування зображення. Наприклад: об'єктив камери заклеїли прозорим скотчем або закрили прозорим поліетиленовим пакетом. У цьому випадку камера здатна відправити повідомлення на е-мейл, включити запис відео або відправити сигнал на alarm-реле. Приклад спрацьовування цієї функції наведено нижче: об'єктив камери навмисно затулили напівпрозорим шматком поліетилену. Камера подала сигнал на систему IVMS, і на моніторі з'явилося повідомлення «Тривога розфокусування» з номером каналу, датою і часом тривоги, було виведено відео в режимі реального часу.

Слід звернути увагу,що ця функція є скоріше допоміжною, ніж основною. Рекомендується використовувати її паралельно з іншими smart-подіями, де в налаштуваннях є можливість запису відео при спрацьовуванні тривоги і можливість настройки розкладу роботи smart-функції.

1.3.3. Детекція зміни сцени (Scene Change Detection)

Функція дозволяє відстежувати зміни положення самої камери. Наприклад, якщо корпус камери був ким-небудь зрушений убік від потрібного напрямку. Слід звернути увагу,що ця функція є скоріше допоміжною, ніж основний. Рекомендується використовувати її паралельно з іншими smart-подіями. Якщо в камері активована функція трекінгу (патрулювання, PTZ), то детекція зміни сцени працювати не буде, щоб не створювати конфлікт в роботі систем). Меню налаштування представлено на Рис.6

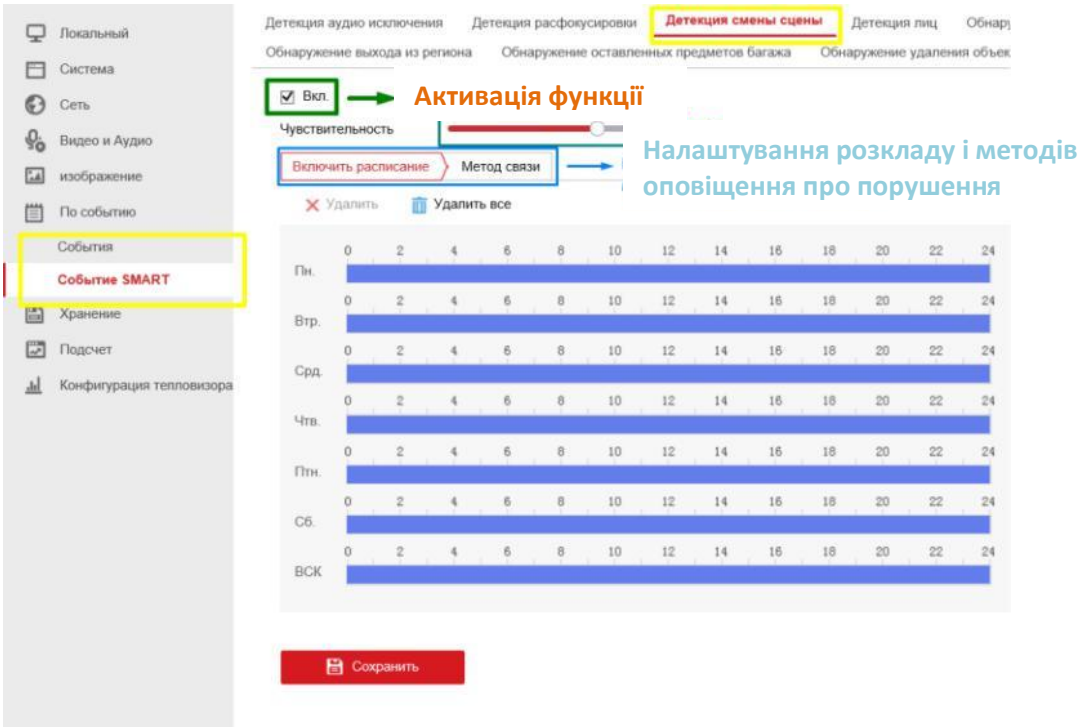


Рис.6

Закладки меню настройки: «Включити розклад» і «Метод зв'язку» не відрізняються від попередніх пунктів. Для більш правильної роботи даної функції, рекомендується додатково встановити час предзапису і післязапису більше 5 секунд. Для цього потрібно пройти шляхом, представленим на Рис.7: Зберігання→ Параметри розкладу→ Розклад запису→ Додаткові налаштування

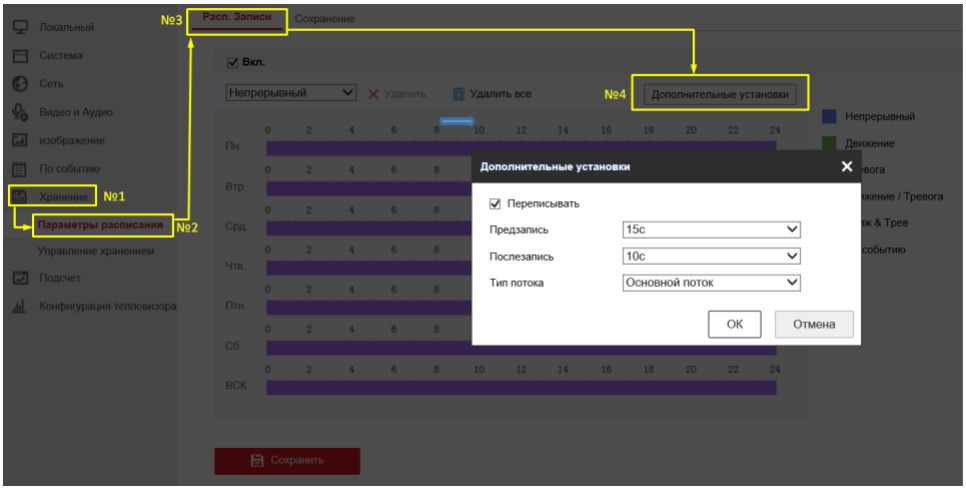


Рис.7

1.3.4. Детекція осіб (Face Detection)

Функція дозволяє виявити обличчя людини в кадрі, і на основі цього активувати запис відео або відправити повідомлення. Наприклад: коли в зону видимості камери входить людина, зберігається фото і відео фіксація цієї події. Ця функція реагує на присутність людського обличчя в кадрі, але не виконує розпізнавання особистості. Меню налаштування представлено на Рис.8.

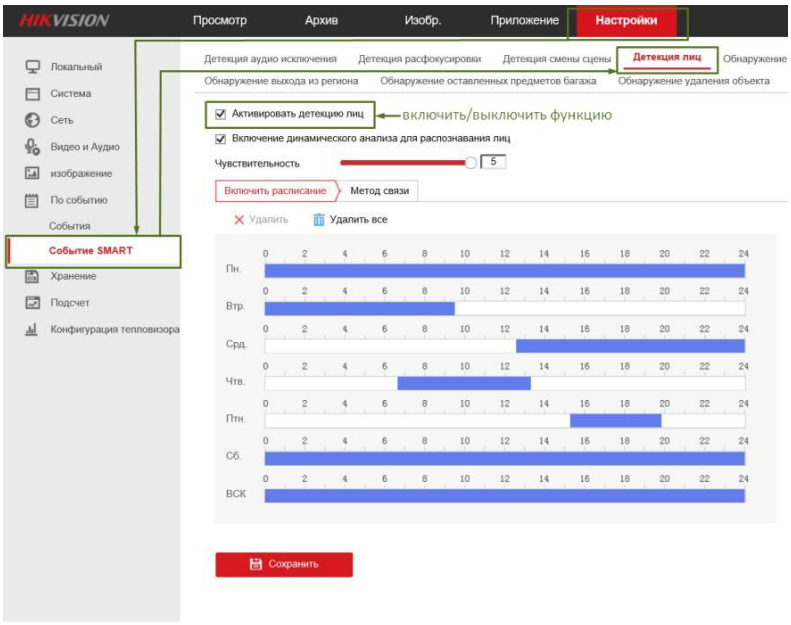


Рис.8

Для того, щоб уникнути помилкових спрацьовувань, треба дотримуватись правил встановлювання камери. Для найбільш коректної роботи функції детекції осіб, рекомендовано встановлювати об'єктив камери під певним кутом до зони детекції, тобто щоб в кадр потрапляло саме обличчя людини, а не верхня частина голови. Приклад спрацювання «детекції особи» в системі Рис 9

Рис 9

При включеному режимі «Динамічний аналіз для розпізнавання осіб» в локальних налаштуваннях Web інтерфейсу, особа підсвічується Зелена рамка в режимі живого відеокадру.

1.3.5. Перетинання лінії (Line Crossing Detection).

Функція «Перетини лінії», дозволяє нам налаштувати запис події перетинання об'єктом умовно намальованої лінії у певному напрямі. При перетину лінії об'єктом спрацьовує тривога і, проводиться: запис і сповіщення в центр спостереження. Як видно на Рис. 10, камера виявила наближення об'єкта до зони (зелений маркер). На Рис. 11 об'єкт перетинає зону (червоний маркер), спрацьовує тривога і виконується запис події.

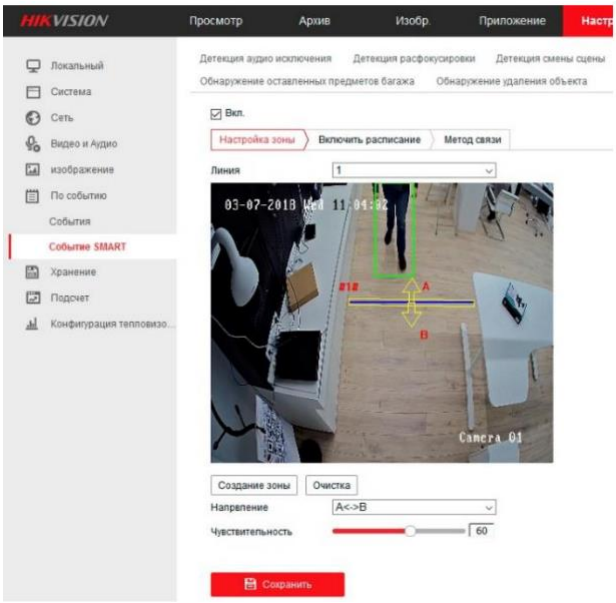
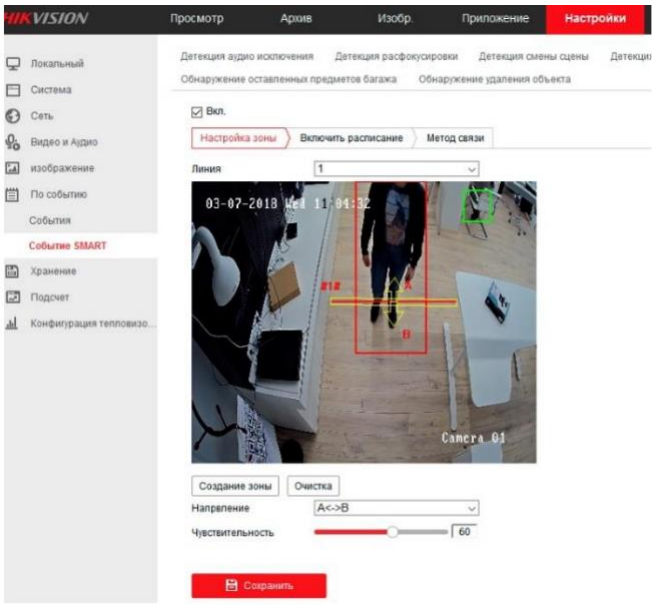


Рис. 10



(Рис. 11)

Налаштування:

- *Чутливість:* значення, за допомогою якого налаштовується спрацьовування детектора. (Макс. чутливість – буде реагувати на всі об'єкти: дрібні та великі; мін. чутливість – буде реагувати тільки на великі об'єкти).

- *Напрямок:* дозволяє налаштувати напрямок перетину. (Зліва направо, справа наліво, або в обидва напрямки)

- *Створити зону:* інструмент для створення умовних ліній. Можна створити від 1 до 4 ліній в залежності від серії пристрою.

- *Очистити:* Видалити всі правила

Закладка розклад: налаштування розкладу роботи детектора «перетин лінії», за замовчуванням активно 24/7. Метод зв'язку: в цьому меню налаштовуються дії, які буде виконувати камера при спрацюванні події. (Відправити Email, оповістити центр спостереження IVMS, включити запис на ftp чи локальну флеш пам'ять, активувати реле тривожного виходу, активувати канал запису).

1.3.6. Детекція вторгнення (Intrusion Detection).

Функція дозволяє встановити віртуальну область на кадрі, яку відстежує камера, і налаштувати спрацьовування тривоги на рух об'єкта при перетині цієї області. Якщо вам потрібно записати події або отримати повідомлення в певній галузі на кадрі, мінімізувати помилкові спрацьовування. Увімкніть «Intrusion Detection», яка буде сповіщати вас тільки при перетині кордону заданої області, форма зони і настройки можуть бути абсолютно індивідуальними.

*Налаштування:*потрібно встановити зону контролю як показано на Рис. 12. Є можливість задати лише певну кількість зон, в залежності від моделі камери.

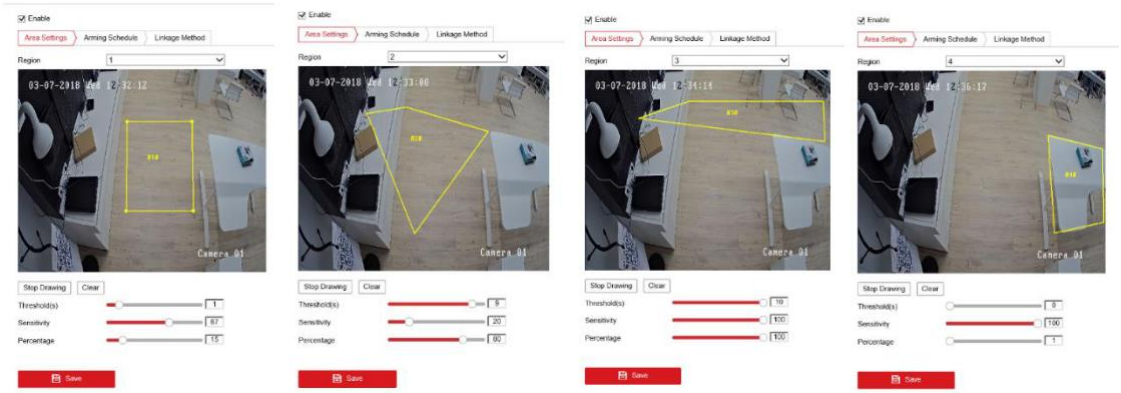


Рис.12

Інтерфейс налаштувань параметрів:

- *Тимчасовий поріг реагування Threshold (s):* установка часу знаходження об'єкта в зоні контролю, після закінчення якого камера зреагує на об'єкт і активує запис і сповіщення (діапазон від 1 до 10 секунд).

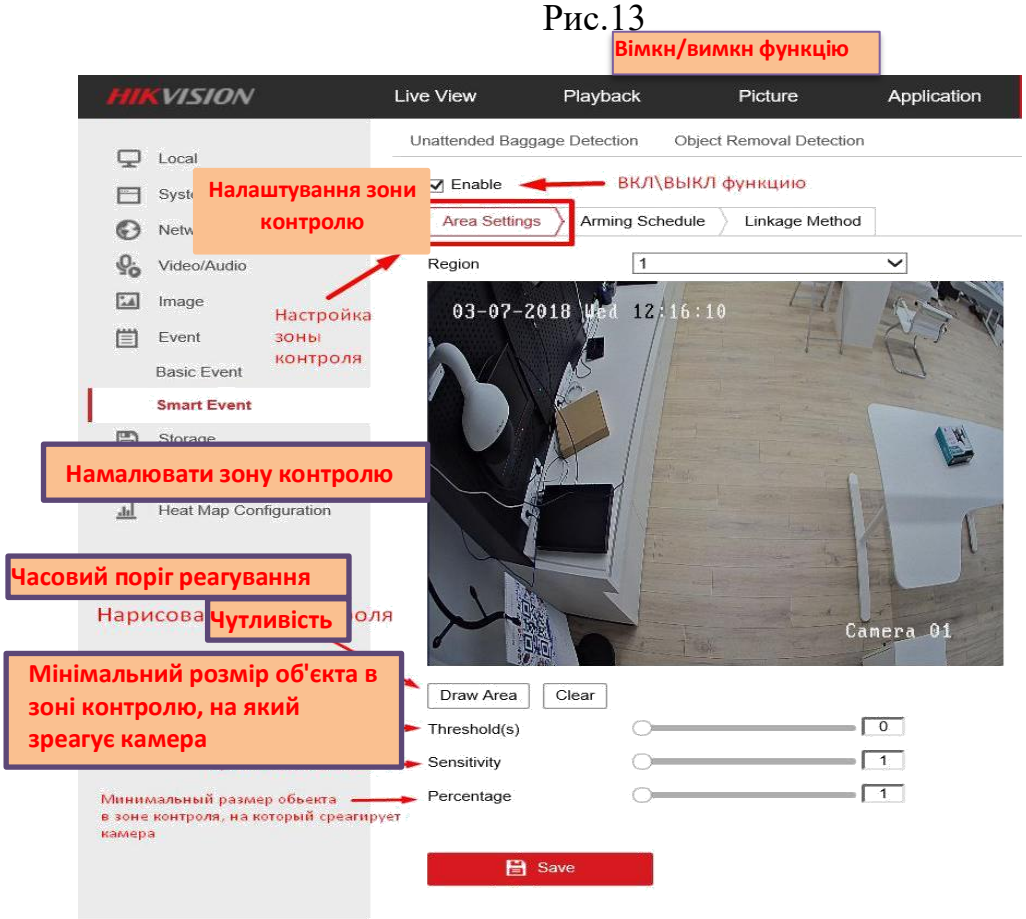
- *Чутливість (Sensitivity):* налаштування швидкості реакції камери. Регулювання реакції камери в залежності від розміру або швидкості об'єкта. Чим менше розмір і швидкість об'єкта, тим більше значення чутливості необхідно встановити. Чим більше розмір і швидкість об'єкта, тим менше значення чутливості необхідно встановити. І навпаки.

- *Мінімальний розмір об'єкта (Percentage):* мінімальний розмір об'єкта, на який зреагує камера в підконтрольній зоні. Іншими словами – поріг чутливості (обсяг зони, яку повинен зайняти об'єкт, щоб сталося спрацювання). Якщо встановлено 1%, то камера зреагує на частину об'єкта, якщо він потрапить в зону контролю. Якщо встановлено 40%, то камера зреагує на появу (наприклад, людини) в зоні контролю, коли людина затулить собою 40% і більше відсотків площі зони контролю. Якщо встановлено 100%, то камера зреагує тільки на повне закриття зони контролю об'єктом.

1.3.7. Виявлення вторгнення в регіон (Region Entrance Detection)

Принцип роботи цього детектора (Рис.13) схожий на функцію, описану в пункті 6.

Рис.13



(«Виявлення вторгнення»), різниця полягає лише в тому, що цей параметр діє тільки на вхід об'єкта в заданий регіон, в той час як детектор «Виявлення вторгнення» реагує на будь-який рух всередині заданої області контролю. Саме з цього для даної функції доступна тільки налаштування чутливості. Налаштування: показано на Рис.14.

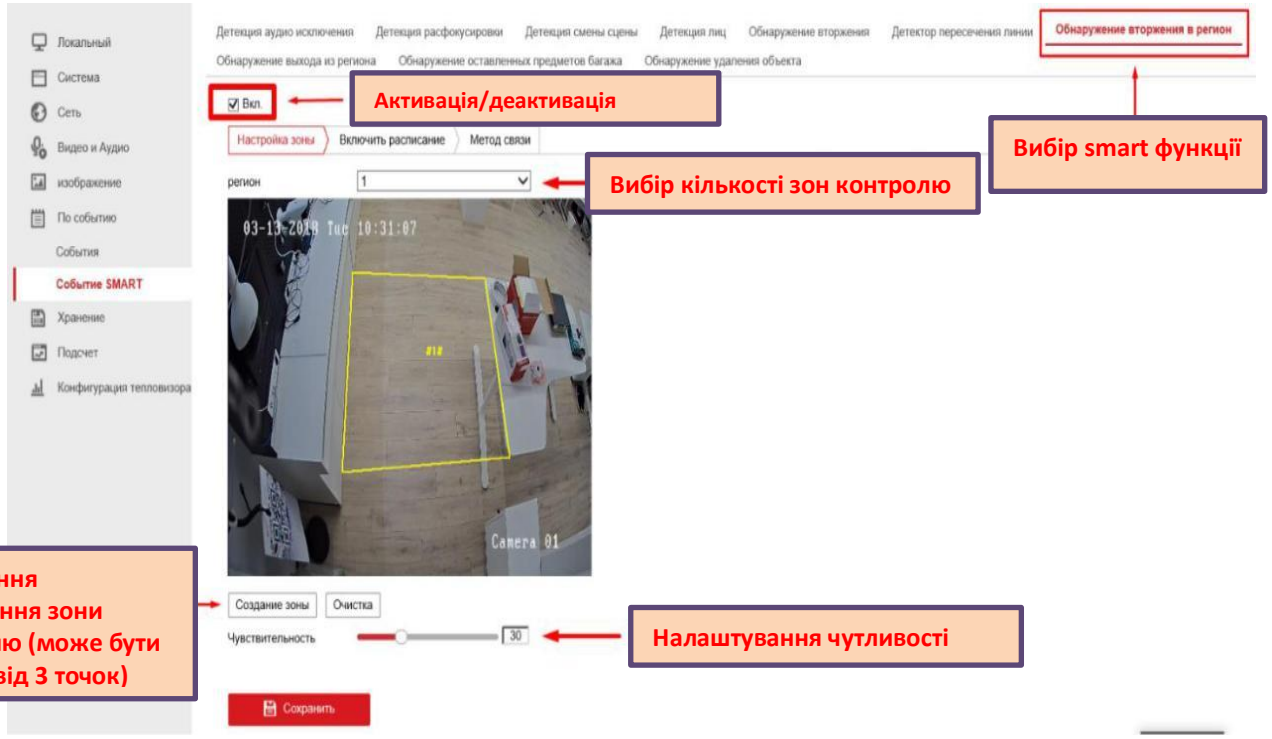


Рис.14

- *Чутливість (Sensitivity):* налаштування швидкості реакції камери, в залежності від розміру або швидкості об'єкта.

Приклад роботи Region Entrance Detection представлений на рис 15.

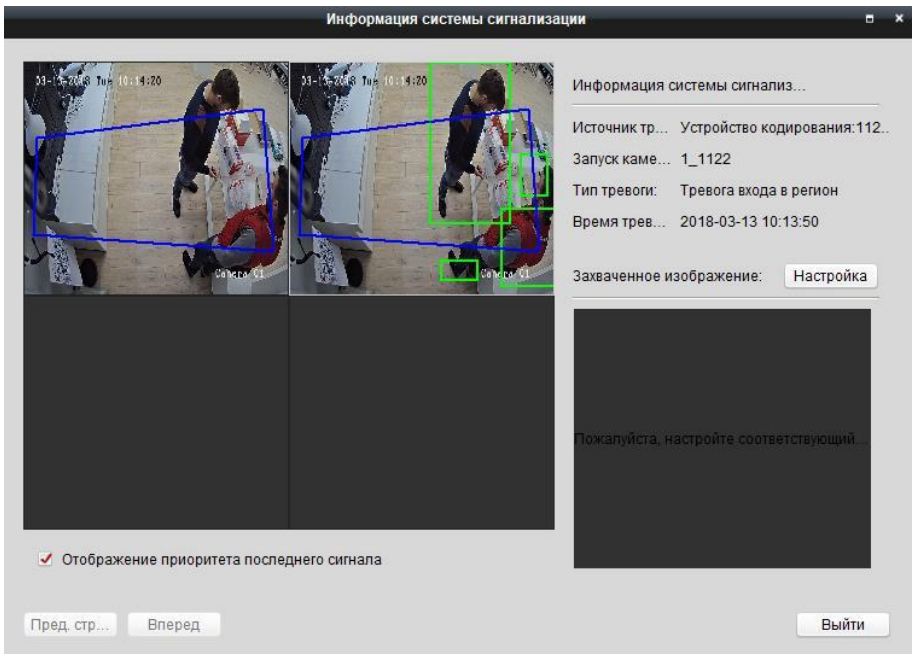


Рис.15

Як видно, система зреагувала на ключові точки руху об'єктів при перетині кордонів зони контролю і вивела на екран зображення в режимі живого перегляду, із зазначенням номера камери, дати, часу і типу тривоги.

1.3.8. Виявлення виходу з регіону (Region Exiting Detection)

Принцип роботи цього детектора схожий на функцію описану в пункті 6 «Виявлення вторгнення», різниця полягає в тому, що цей параметр діє тільки на вихід об'єкта з заданого регіону. По суті - повна протилежність попередньої функції описаної в п. 7, інтерфейс налаштування так само повністю аналогічний п.7. **Наприклад:** Є умовна зона на парковці гіпермаркету, припустимо, зона ряду паркомісць. При виїзді автомобіля з паркомісця спрацює тривога.

1.3.9. Виявлення залишених предметів багажу (Unattended Baggage Detection)

Функція призначена для відстеження залишених предметів в заданій області. При використанні цього детектора камера оповіщає нас і активує запис, якщо в заданій зоні з'явився предмет якого до цього не було, і він знаходиться без руху якесь певний час (за замовчуванням - від 5 секунд). Налаштування: показана на Рис.16.

Чутливість - величина, зворотньо пропорційна розміру об'єкта, який може активувати включення тривоги (чим менше об'єкт, тим більше повинна бути чутливість).

Поріг - допустимий час перебування об'єкта в зоні контролю.

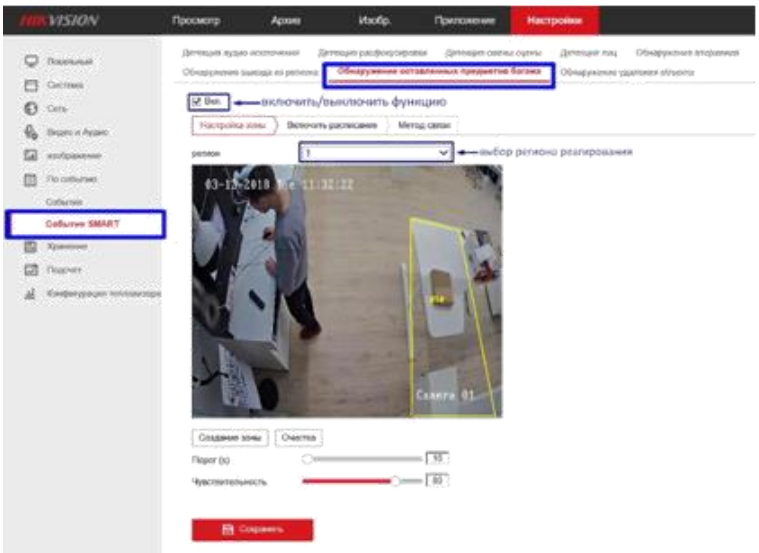


Рис.16

1.3.10. Виявлення видалення об'єкта (Object Removal Detection)

Функція (Рис.17) призначена для відстеження видалення предметів із заданої області. По суті, ця функція є повною протилежністю описаної в п.9 Налаштування повністю аналогічно до п.9

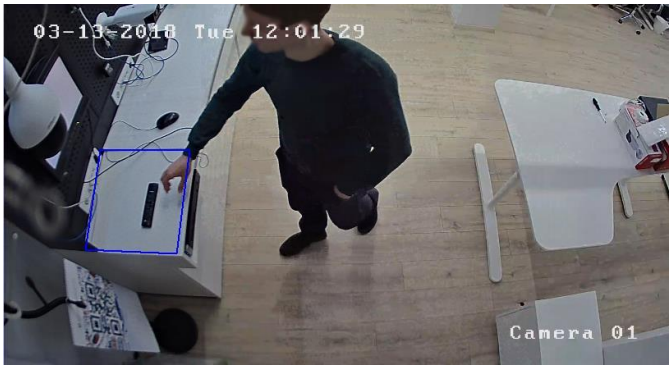
Чутливість - величина, обернено пропорційна розміру об'єкта, який може активувати включення тривоги (чим менше об'єкт, тим більше повинна бути чутливість).

Поріг - допустимий час перебування об'єкта в зоні контролю (від 5с. до 3600с.). Приклад роботи наведений нижче

Рис.17

Крок 1. На столі задана зона контролю і в ній залишений пульт управління (Рис.18).

Крок 2. Відбувається несанкціоноване переміщення об'єкта з підконтрольної зони (Рис.19).



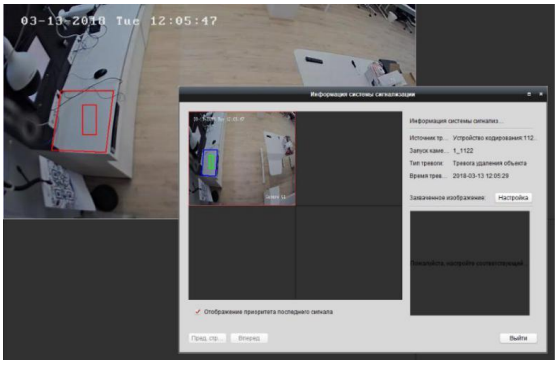


Рис.18 Рис.19

Крок 3. Пульт перенесли на інший стіл, камера відстежила видалення об'єкта з підконтрольної області і включила тривогу.

1.4 Використання аналітичних Smart функцій

В залежності від розташування камери можна активувати тільки необхідні смарт функції. Наведемо декілька прикладів використання.

Функція детекція аудіо виключення може в автоматичному режимі сповістити про постріл чи вибух в місті розташування. Детекція розфокусування сповістить оператора про спробу затулити об’єктив камери стороннім предметом. Детекція зміни сцени сповістить оператора про спробу фізично повернути чи зняти камеру. Функція перетинання лінії має дуже багато варіантів використання. Намальована у напрямку дорожнього руху лінія буде автоматично сповіщати про спробу рухатися у зустрічному напрямку, Намальована на лінії розмежування дорожніх смуг буде автоматично сповіщати про перетин цієї смуги та вести відеозапис порушення. Функція виявлення видалення об'єкта може застосовуватися при спостереженні за об'єктами вуличної інфраструктури (паркомати, урни, банкомати) так і за малими архітектурними формами (пам’ятники, меморіали, таблички тощо).

1.5 Відеоаналітика у сфері дорожнього руху

Відеоаналітика на транспорті застосовується на декількох рівнях. До базових відносять завдання розпізнавання стандартизованих образів, наприклад, номерів транспортних засобів. Слід зазначити, що для експлуатації в реальних умовах важлива не тільки точність розпізнавання номерних знаків, а й надійність функціонування обладнання у важких погодних умовах, антивандальна здатність та забезпечення всіх технічних характеристик у різних режимах роботи. Адже природні чинники не повинні заважати та переривати роботу працівників поліції.

На даний час на українських дорогах здійснюється відеофіксація перевищення швидкості та інших можливих порушень правил дорожнього руху

За даними правоохоронців, з початку використання приладів відеофіксації за перевищення швидкості (жовтень 2018 року) патрульні притягли до відповідальності понад 350 тисяч порушників швидкісного режиму.

Як повідомлялося, з 2022 року автовиробники повинні будуть обладнати машини, які продаються на території ЄС, "чорними ящиками" і системою автоматичного утримання в смузі транспортного засобу [10].

Всі сучасні транспортні комунікації повинні проектуватися з урахуванням обладнання приладами відеоспостереження, однак обладнання тих об'єктів транспортної інфракструктури, які були побудовані за часів, коли відеоспостереження ще не застосовувалося, пов'язане з певними труднощами. Прикладом є звичайні пішохідні переходи. Це оптимальне місце установки інтелектуальних камер розпізнавання осіб, оскільки особу зручніше розпізнати саме тоді, коли людина рухається в направленому потоці по певній траєкторії.

Розпізнавання автомобільних номерів є найпопулярнішою та найнеобхіднішою функцією у сучасних системах відеоспостереження. При правильно побудованій і налагодженій системі можна домогтися розпізнавання автомобільного номеру з ймовірністю до 95%. Але навіть така висока ймовірність говорить про те, що повністю автономну систему відеоспостереження з розпізнаванням номерів побудувати не можна. На ці 5% потрібен оператор, який буде приймати правильні рішення по проїзду автомобіля при наявності двох типів помилок – помилкового доступу і помилкової відмови. Щоб побудувати систему розпізнавання з такою високою точністю, необхідно знати і передбачити велику кількість нюансів.

За інформацією прес-служби KyivSmartCity, на данний час закуплено 20 систем вартістю по 1 млн. грн. за одиницю, з них п'ять змонтовано, а одна навіть сертифікована, інші знаходяться в процесі підготовки до роботи. Як роз'яснив гендиректор КП "Інформатика" Микола Пихтін, кожна система складається з радара-детектора, відеокамери, здатної розпізнавати номер автомобіля і електронного блоку обробки даних.

Якщо водій автомобіля перевищує швидкість, проїжджає на заборонний сигнал світлофора, їде по смузі громадського транспорту, паркується там, де заборонено, це фіксує детектор, камера робить знімок, інформація обробляється і надходить на сервер патрульної поліції. Далі по базі зареєстрованих в Україні автомобілів автоматично визначається власник, його адреса проживання і формується квитанція. Поліцейським залишається її роздрукувати, вкласти в конверт, написати адресу і відправити порушнику для оплати штрафу [11].

1.6 Розширення функцій відеоаналітики у сфері дорожнього руху

Слід зазначити, що використання метаданих з вже встановлених камер зі смарт функціями є новим, але дуже перспективним напрямом. Отже, камера, яка має функцію розпізнавання номерних знаків, робить це в автоматичному режимі, та надсилає дані у такому форматі. Наприклад:

Номер запису	Час події	Дата події	Держ. номер
48541	09:27:35	03.24.2020	АА 3333 АА

Інформація зі стовпців «Час події» та «Дата події» не є службовою таємницею та містить в собі дані про час та сам факт скоєння події, тобто проїзд транспортного засобу у місці розміщення камери. Виходячи з цього, такі дані можна отримати, накопичувати та статистично обробляти. Можна побудувати криву подій (кількість транспортних засобів, що перетинають межу встановлення камери, на хвилину). Отримавши такі дані за певний період часу, можна буде на основі статистичних даних автоматично робити висновки щодо стану автомобільного трафіку: звичайний він, чи потребує уваги оператора.

Оскільки автомобільний трафік залежить від великої кількості не пов’язаних один з одним факторів, то можна вважати, що розглядувані події (перетин транспортним засобом межі встановлення камери) є випадковими, а числову характеристику сукупності таких подій – кількість перетинів за хвилину (чи іншу характерну одиницю часу) – можна наближено описувати за допомогою теорії нормально розподілених випадкових величин [*].

Суттєвим є питання, за яким критерієм можна зробити висновок щодо аномальності стану трафіку. У будь-якому випадку здається доречним базуватися на добре відомому у теорії ймовірностей «правилі трьох сигм» [*], згідно з яким приблизно з ймовірністю 0,9973 значення нормально розподіленої випадкової величини знаходиться у інтервалі $[\bar{x}-3\sigma;\bar{x}+3\sigma]$, де $\bar{x}-$ середнє значення випадкової величини, а σ – середньоквадратичне відхилення випадкової величини від її середнього значення.

Як правило, значення цих параметрів обчислюються за елементами деякої вибірки отриманих результатів досліджень за допомогою формул

$$\bar{x} = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

та

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_n - \bar{x})^2}{n}}.$$

Варіантами є оцінка попадання оцінюваного значення до інтервалів $[\bar{x} - 2\sigma; \bar{x} + 2\sigma]$ (для нормально розподіленої величини ймовірність попадання складає 0,9544) або навіть $[\bar{x} - \sigma; \bar{x} + \sigma]$ (ймовірність дорівнює 0,6826). В цих випадках аномальними будуть вважатися також значення, які менше відрізняються від середнього значення характеристики, ніж у першому варіанті. Такий підхід має як переваги, так і недоліки, адже, з одного боку, існує ймовірність того, що відносно невелика різниця справді відповідає аномальному значенню, але, з іншого боку, може виявитись, що буде вважатися аномальними велика кількість насправді «нормальних» значень.

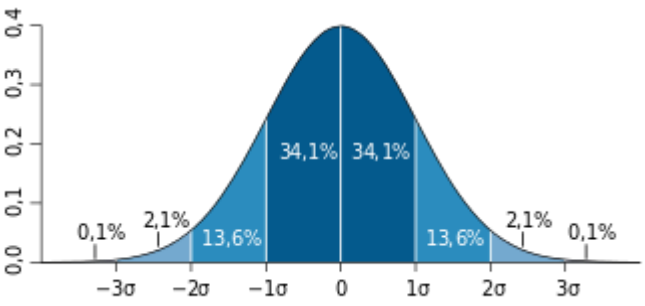


Рис.20

«Правило сигм» добре ілюструється графічно (рис.20): очевидно, що ймовірність попадання у відповідний інтервал (площа замальованої фігури під кривою) є для інтервалів $[\bar{x} - 3\sigma; \bar{x} + 3\sigma]$ та $[\bar{x} - 2\sigma; \bar{x} + 2\sigma]$ великою, а для інтервалу $[\bar{x} - \sigma; \bar{x} + \sigma]$ досить суттєвою.

Слід підкреслити, що критеріальний інтервал може бути й асиметричним, все залежить від того, на яких міркуваннях базується його вибір.

Таким чином, вибір критеріального інтервалу вимагає окремого дослідження, оскільки він повинен базуватися на практичному досвіді спеціалістів з відеоаналітики та порівнянні реальних аномальних значень оцінюваної величини (тобто значень, які відповідають аварійним ситуаціям, ДТП, порушенням дорожнього руху тощо) із запропонованими з теоретичних міркувань варіантами.

Слід зазначити також, що нетривіальним є питання щодо побудови вибірки, за допомогою якої обчислюються параметри $\bar{x}$ та σ . Можна запропонувати оцінювати ці параметри за декількома попередніми значеннями розглядуваної величини. Такий підхід дозволяє брати до уваги особливості трафіку у період часу, що безпосередньо передує моменту спостереження. Залишається відкритим питання щодо обсягу запропонованої вибірки, тобто кількості значень, які слід використовувати у розрахунках. Відповідь на це питання може бути надана тільки після аналізу відповідності отриманих теоретично результатів (оцінок параметрів розподілу для різних обсягів вибірки) реальним значенням, які відповідають «нормальним» та «аномальним» умовам трафіку.

Таким чином, можна відзначити такі проблеми, які доречно розглянути для коректного аналізу результатів спостереження:

– попередній якісний аналіз з метою визначення наявності кореляції між числовою характеристикою трафіку та наявністю/відсутністю його аномалій;
– у випадку позитивної відповіді на зазначене вище питання пошук оптимального обсягу вибірки для визначення оцінок параметрів;
– вибір найбільш доцільного критеріального інтервалу для «нормальних» значень характеристики.

РОЗДІЛ ІІ СУЧАСНІ ПРОБЛЕМИ У ЗАСТОСУВАННІ ВІДЕОАНАЛІТИКИ

2.1 Проблеми використання відеофіксації під час роботи працівників Національної поліції

Як відомо, працівники патрульної поліції оснащені нагрудними камерами (відеореєстраторами), що також є одним із засобів відеоаналітики, наявність яких розглядається ними як засіб захистити себе від упереджених заяв щодо їхньої неправомірної поведінки, фіксації протиправних діянь та ходу виконання службових обов'язків. Проте такий захист вступає у конфлікт із правом на приватність. Ми це спостерігаємо сьогодні, коли записи з цих нагрудних реєстраторів публікуються самою поліцією у мережі YouTube чи передаються у ЗМІ. Інколи вони є фрагментарними, тобто нарізкою із різних кадрів, що відображають упереджену позицію щодо людини, порушуючи презумпцію невинуватості. Крім того, правове регулювання автоматичної зйомки (тобто без згоди на це особи) є непродуманим і таким, що суперечить чинному законодавству. А саме правове регулювання є непрозорим, адже розібратись в цьому питанні шляхом вивчення опублікованої нормативно-правової бази неможливо.

Відомчі акти Національної поліції (№ 100 і № 14/1), що регулюють порядок застосування приладів, зберігання та режим доступу до відеозаписів, не опубліковані, що становить загрозу для дотримання прав людини поліцією. Тому законодавець дає право використовувати превентивний захід відповідно до п. 9 ч. 1 ст. 31 ЗУ «Про Національну поліцію», а саме застосування технічних приладів і технічних засобів, що мають функції фото і відеозйомки. Це і є поліцейський відеореєстратор, хоча тут мова може йти про будь-яку фотокамеру або відеокамеру, яку працівники поліції використовують, наприклад, при охороні мирних зібрань.

Стосовно статті 26 ЗУ «Про Національну поліцію», то вона передбачає формування інформаційних ресурсів поліцією – баз (банків) даних, куди про

затриманих вноситься мультимедійна інформація (фото, відео-, звукозапис) та біометричні дані (дактилокартки, зразки ДНК). Але тут мова йде про затриманих, а не тих, хто підозрюється у скоєнні правопорушення чи в кого перевіряють документи або взагалі опитують [12].

Згідно наказу 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», чітко розписано порядок надання таких відеозаписів третім особам, а саме [13]:

а) необхідність відеофіксації: «використання нагрудних відеокамер (відеореєстраторів) як превентивного поліцейського заходу є важливим елементом функціонування патрульної поліції, покликаним гарантувати чесність, відкритість та антикорупційну спрямованість діяльності патрульної поліції» (п. 1.3 Розділу І Інструкції);

б) випадки застосування такого превентивного заходу: «нагрудна відеокамера (відеореєстратор) повинна активовуватись працівником патрульної поліції та знаходитись у режимі відеозйомки при будь-якому контакті з особами, зокрема, але не виключно:

– при оформленні дорожньо-транспортної пригоди;

– при перевірці документів;

– при поверхневому огляді;

– при загрозі використання фізичної сили, спеціальних засобів або вогнепальної зброї;

– при наданні допомоги особам;

– у випадках, коли усвідомлення особою факту відеофіксації її поведінки може сприяти вирішенню конфліктної ситуації;

в) облік технічних приладів: кожному відеореєстратору присвоюється ідентифікаційний номер та при виході на зміну працівник патрульної поліції оглядає його на справність і розписується про це у відповідному журналі, а при закінченні зміни здає прилад у найкоротший строк;

г) порядок зберігання: патрульному заборонено самостійно показувати інформацію третім особам, змінювати, редагувати, видаляти, копіювати, тощо (п. 3.7 Розділу ІІІ Інструкції). Після здачі технічного приладу уповноважена особа структурного підрозділу інформаційних технологій та зв'язку управління патрульної поліції зберігає відеозапис на сервері – «протягом 6 годин з моменту прийому від працівника здійснюється процедура довготривалого збереження – до 30 діб на сервері за наявності технічної можливості» (п. 4.1, 4.2 Розділу IV Інструкції). При цьому строк може бути подовжено за розпорядженням начальників управлінь поліції у містах (або Департаменту), у випадку отримання скарги від особи на рішення, дії чи бездіяльність працівників патрульної поліції, у інших виключних випадках.

Відтак, сьогодні відеозаписи, отримані з відеореєстраторів і опубліковані без згоди на це особи, котра була об'єктом відеозапису, є порушенням норм Закону України «Про захист персональних даних» [14].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ольга Комарова. Сучасні системи безпеки: чи змінюється служба в поліції? URL: https://www.radiosvoboda.org/a/svoboda-v-detalyakh-chy-zminyuyetsya-sluzhba-v-politsiyi/29654855.html (дата звернення: 17.01.2020).

2. 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.

3. Кримінальний процесуальний кодекс України чинний, поточна редакція — від 28.11.2019, (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88). URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 17.01.2020).

4. 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.

5. 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.

6. Норми освітленості різних приміщень на Україні і в Європі. URL: https://electrosvit.com/index.php?option=com_content&view=article&id=12&Itemid=19&lang=uk (дата звернення: 17.01.2020).

7. 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.

8. Інформаційна газета Liga.net. URL: https://news.liga.net/society/news/avakov-skazal-gde-v-ukraine-samyy-nizkiy-uroven-prestupnosti (дата звернення: 17.01.2020).

9. Патрульна поліція запускає ще 57 новых камер для фиксації руху на дорогах. URL: https://delo.ua/econonomyandpoliticsinukraine/patrulnaja-policija-zapuskaet-esche-57-novyh-kam-360765/ (дата звернення: 17.01.2020).

10. В ЕС обяжут автомобили оборудовать "черными ящиками". URL: https://delo.ua/business/evrosojuz-planiruet-objazatelnuju-ustanovku-v-av-351378/ (дата звернення: 17.01.2020).

11. 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 (дата звернення: 17.01.2020).

12. « Про Національну поліції України». Закон України, поточна редакція —від 28.11.2019, (Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379). URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 17.01.2020).

13. Нагрудна камера (відеореєстратор) патрульного: правове регулювання і порушення права на приватність. URL: http://umdpl.info/police-experts.info/2016/04/14/article-videofixation/ (дата звернення: 17.01.2020).

14. «Про захист персональних даних». Закон України. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 17.01.2020).

15. В Україні працює близько 19 тисяч камер відеоспостереження, але бракує законодавчого регулювання – експерти. URL: http://uacrisis.org/ua/73640-videosurveillance-regulations (дата звернення: 17.01.2020).

16. Hikvision № 1 у світі. URL: https://hikvision.org.ua/uk (дата звернення: 17.01.2020).

17. URL: http://kmr.gov.ua/uk/file/120501/download?token=uZ1tnbccjrZNZhLorW8BG1ICueWlIVbTa-NsHUq76To (дата звернення: 17.01.2020).

18. URL: https://minjust.gov.ua/people/ivan-lishchyna (дата звернення: 17.01.2020).

19. За порядком в Днепре следят 780 камер: результаты работы ситуационного центра. Журавель Максим, Газета «Сьогодні». URL:

https://www.segodnya.ua/regions/dnepr/za-poryadkom-v-dnepre-sledyat-780-kamer-rezultaty-raboty-situacionnogo-centra-1290460.html (дата звернення: 17.01.2020).

20. Город на ладони, или Большой глаз видит все: как ситуационный центр делает Днепр безопасным. Таисия Кузьменко. Наше місто-Головна газета Дніпра. URL: https://nashemisto.dp.ua/2019/05/05/gorod-na-ladoni-ili-bolshoj-glaz-vidit-vse-kak-situacionnyj-centr-delaet-dnepr-bezopasnym/ (дата звернення: 17.01.2020).

21. Найти угнанный автомобиль: как работает Ситуационный центр Днепра? Алена Кузьменко. Останні новини 34 канал. URL: https://34.ua/najti-ugnannyj-avtomobil-kak-rabotaet-situacionnyj-centr-dnepra_n82988 (дата звернення: 17.01.2020).

22. Ситуаційні центри та командні пункти. Проект «Безпечне місто». URL: https://leater.com/ua/services/bezpechne-m-sto.html (дата звернення: 17.01.2020).

23. Безпечне місто. URL: https://www.datagroup.ua/pro-kompaniyu/socialna-vidpovidalnist/bezpechne-misto (дата звернення: 17.01.2020).

24. Вентцель Е.С.,Овчаров Л.А. Прикладные задачи теории вероятностей. – М.: Радио и связь, 1983. – 416 с.

Навчальне видання

Махницький Олександр Васильович
Мирошниченко Володимир Олексійович
Кочеткова Інна Борисівна

ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ У РОБОТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Методичні рекомендації

Підп. до друку 20.10.2020 р. Формат 60х84/16. Гарнітура – Times.
Друк трафаретний (RISO), цифровий. Папір офісний. Ум.-друк. арк. 2,25. Обл.-вид. арк. 2,50
Тираж 100 прим.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49000, м. Дніпро, просп. Гагаріна, 26, т. (056) 756-46-41
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018