



**МІНІСТЕРСТВО
ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ
ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО
ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

**АНАЛІЗ ПОБУДОВИ
ЦЕНТРАЛІЗОВАНИХ СИСТЕМ
ВІДЕОСПОСТЕРЕЖЕННЯ ТА
ВІДЕОАНАЛІТИКИ В ЧАСТИНІ
ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОГО
(ГРОМАДСЬКОГО) ПОРЯДКУ
(МІЖНАРОДНИЙ ДОСВІД
СТВОРЕННЯ ТАКИХ СИСТЕМ,
ЗАДІЯНІ ТЕХНОЛОГІЇ ТА
ВИРОБНИКИ)**

Навчальний посібник

**Одеса
2025**

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

**НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ
СЛУЖБИ УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО**

**АНАЛІЗ ПОБУДОВИ ЦЕНТРАЛІЗОВАНИХ СИСТЕМ
ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОАНАЛІТИКИ В ЧАСТИНІ
ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОГО (ГРОМАДСЬКОГО) ПОРЯДКУ
(МІЖНАРОДНИЙ ДОСВІД СТВОРЕННЯ ТАКИХ СИСТЕМ,
ЗАДІЯНІ ТЕХНОЛОГІЇ ТА ВИРОБНИКИ)**

Навчальний посібник

Одеса 2025

*Рекомендовано до друку Вченою радою
Одеського державного університету внутрішніх справ
(протокол № 15 від 25 листопада 2025 року)*

Рецензенти:

Балтовський Олексій Анатолійович – професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, доктор юридичних наук, доцент

Клименко Вячеслав Анатолійович – заступник начальника Управління кримінального аналізу Головного управління Національної поліції в Одеській області, підполковник поліції

А 64 Аналіз побудови централізованих систем відеоспостереження та відеоаналітики в частині забезпечення публічного (громадського) порядку (міжнародний досвід створення таких систем, задіяні технології та виробники : навч. посіб. / А. О. Бабарика та ін. — Одеса : Одеський державний університет внутрішніх справ, 2025 —148 с.

Навчальний посібник присвячений аналізу побудови централізованих систем відеоспостереження та відеоаналітики в частині забезпечення публічного (громадського) порядку, дослідження міжнародного досвіду при створенні таких систем та задіяних технологій. Приділена увага висвітленню поняття публічного порядку та місця і ролі Національної поліції України та Державної прикордонної служби України у його забезпеченні. Проаналізовано сучасний стан побудови систем відеоспостереження, технологічну базу та архітектуру сучасних систем інтелектуального відеоспостереження, а також досліджено системи відеоспостереження та відеоаналітики, що використовуються Національною поліцією України та Державною прикордонною службою України.

Навчальний посібник може бути корисним для слідчих, представників оперативних підрозділів Національної поліції України, слухачів закладів вищої освіти зі специфічними умовами навчання, а також усім, хто цікавиться тематикою забезпечення публічного порядку за допомогою систем відеоспостереження та відеоаналітики.

ISBN 978-617-7633-34-X

УДК 351.741:351.86:004
© Барарика А. О. та ін.?2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ.....	5
ВСТУП.....	6
I. ПОНЯТТЯ ПУБЛІЧНОГО ПОРЯДКУ ТА МІСЦЕ ОРГАНІВ І ПІДРОЗДІЛІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ У СФЕРІ ЙОГО ЗАБЕЗПЕЧЕННЯ.....	7
1.1. Публічний порядок та його роль у функціонуванні та розвитку сучасного суспільства.....	7
1.2. Забезпечення публічного порядку органами і підрозділами Національної поліції України.....	14
1.3. Забезпечення публічного порядку органами і підрозділами Державної прикордонної служби України.....	27
<i>Контрольні питання до розділу I.....</i>	<i>37</i>
II. АНАЛІЗ СУЧАСНОГО СТАНУ ПОБУДОВИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЯМИ ВІДЕОАНАЛІТИКИ: ІСТОРИЧНИЙ АСПЕКТ.....	38
2.1. Витоки розвитку систем відеоспостереження (1930 – 1950-ті роки).....	40
2.2. Розвиток аналогових CCTV-систем (1960 – 1970-ті роки).....	41
2.3. Перехід до цифрових технологій (1980 – 1990-ті роки).....	43
2.4. IP-відеоспостереження (2000-ні роки).....	45
2.5. Інтелектуальні системи (2010-ті – сьогодення).....	46
2.6. Тенденції майбутнього розвитку систем відеоспостереження.....	47
<i>Контрольні питання до розділу II.....</i>	<i>50</i>
III. ТЕХНОЛОГІЧНА БАЗА ТА АРХІТЕКТУРА СУЧАСНИХ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО ВІДЕОСПОСТЕРЕЖЕННЯ.....	51
3.1. Технологічна база сучасних систем відеоспостереження.....	51
3.2. Архітектура сучасних систем відеоспостереження.....	55
3.3. Класифікація систем відеоспостереження.....	64
<i>Контрольні питання до розділу III.....</i>	<i>69</i>

IV. СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОАНАЛІТИКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ТА ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ.....70

4.1. Системи відеоспостереження та відеоаналітики Національної поліції України.....70

4.2. Системи відеоспостереження та відеоаналітики Державної прикордонної служби України.....81

4.2.1. Система відеоспостереження Державної прикордонної служби України «ЗІР ПРО».....81

4.2.2. Інтелектуальна система відеоспостереження та відеоаналітики для Державної прикордонної служби України INCORESOF VEZHA.....101

Контрольні питання до розділу IV.....132

V. МІЖНАРОДНИЙ ДОСВІД ПОБУДОВИ ЦЕНТРАЛІЗОВАНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОАНАЛІТИКИ.....134

5.1. Модель «Тотального контролю»: китайський досвід централізованого державного нагляду.....134

5.2. Модель «Публічно-приватного партнерства» (на прикладі Великої Британії та США).....136

5.3. Модель «Збалансованого підходу та захисту даних» (на прикладі країн ЄС та Скандинавії).....137

5.4. Інноваційні моделі (на прикладі Сінгапуру та ОАЕ).....140

Контрольні питання до розділу V.....142

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....143

АВТОРСЬКИЙ КОЛЕКТИВ (за алфавітом).....146

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

MBC	– Міністерство внутрішніх справ
НПУ	– Національна поліція України
ДПСУ	– Державна прикордонна служба України
ДСНС	– Державна служба України з надзвичайних ситуацій
ДМС	– Державна міграційна служба
НГУ	– Національна гвардія України
БПЛА	– безпілотний літальний апарат
CBC	– системи відеоспостереження
ICB	– інтегрована система відеоспостереження
AI	– Artificial Intelligence (штучний інтелект)
ANPR	– Automatic Number Plate Recognition (автоматичне розпізнавання номерних знаків)
CCTV	– Closed-circuit television (система замкнутого телебачення)
CNN	– Convolutional Neural Networks (згорткові нейронні мережі)
DVR	– Digital Video Recorder (цифровий відеореєстратор)
FLIR	– Forward-Looking InfraRed (інфрачервона система переднього огляду);
GNSS	– Global Navigation Satellite System (це глобальна навігаційна супутникова система)
GPS	– Global Positioning System (глобальна навігаційна супутникова система)
iFogSim	– відкритий пакет програм для імітаційного моделювання обчислювальних середовищ
IoT	– Інтернет речей
NVR	– Network Video Recorder (мережевий відеореєстратор)
ONVIF	– Open Network Video Interface Forum (Відкритий форум мережевого відеоінтерфейсу)
PTZ-камера	– роботизована камера відеоспостереження

ВСТУП

У сучасних умовах у сфері забезпечення публічного (громадського) порядку, у тому числі, поблизу державного кордону України дедалі більшого значення набувають інтелектуальні системи відеоспостереження, що дозволяють підвищувати ефективність контролю та реагування на різноманітні загрози. За останні десятиліття системи відеоспостереження пройшли значний еволюційний розвиток – від простих аналогових пристроїв до потужних цифрових комплексів із функціями відеоаналітики, що дають змогу не лише фіксувати події, але й автоматично аналізувати ситуацію в режимі реального часу.

Збільшення обсягів відеоданих та складність їх обробки поставили нові виклики щодо побудови архітектури інтелектуальних систем, які з урахуванням територіальної розподіленості об'єктів, можуть ефективно працювати на основі сучасних технологій хмарних та туманних обчислень. У цьому контексті особливо актуальним є розробка гнучких, масштабованих та модульних рішень, які враховують функціональні потреби правоохоронних органів держави, зокрема, Національної поліції України та Державної прикордонної служби України під час забезпечення публічного (громадського) порядку.

Використання інтелектуальних систем відеоспостереження в НПУ та ДПСУ забезпечує автоматизацію ключових завдань контролю території, ідентифікації осіб, аналізу транспортних засобів, а також ефективний моніторинг з багатьох камер у просторі. Застосування технологій відеоаналітики дозволяє зменшити вплив людського фактору, підвищити точність виявлення тривожних ситуацій та своєчасність їхнього реагування.

У навчальному посібнику авторами здійснено аналіз побудови централізованих систем відеоспостереження та відеоаналітики, що використовується під час забезпечення публічного (громадського) порядку не тільки в Україні, але й у світі в цілому.

I. ПОНЯТТЯ ПУБЛІЧНОГО ПОРЯДКУ ТА МІСЦЕ ОРГАНІВ І ПІДРОЗДІЛІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ У СФЕРІ ЙОГО ЗАБЕЗПЕЧЕННЯ

1.1. Публічний порядок та його роль у функціонуванні та розвитку сучасного суспільства

У науковій літературі часто дискутується співвідношення термінів «публічний порядок» і «громадський порядок». Деякі науковці ототожнюють їх, інші вважають, що поняття «публічний порядок» є більш базовим і широким за змістом, охоплюючи не тільки поточну поведінку громадян у публічних місцях, але й загальнодержавні правові та моральні засади.

Відповідно до статті 2 Закону України «Про Національну поліцію» завданнями поліції є надання поліцейських послуг у сферах:

- 1) забезпечення публічної безпеки і порядку;
- 2) охорони прав і свобод людини, а також інтересів суспільства і держави;
- 3) протидії злочинності;
- 4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги¹.

Публічний порядок – це сукупність суспільних відносин, що врегульовані правовими та моральними нормами, які забезпечують громадську безпеку, спокій, захист прав і свобод громадян, а також нормальні умови для діяльності державних та громадських організацій.

Публічний порядок – це публічно-правові відносини імперативного характеру, які визначають основи суспільного ладу держави, її правові засади, принципи моралі та інші соціальні норми. Це оціночне та широке поняття, яке використовується в законодавстві, зокрема в міжнародному приватному праві, і не має єдиного офіційно закріпленого визначення.

Публічний порядок охоплює фундаментальні принципи, на яких ґрунтується державний і суспільний лад, забезпечуючи нормальні умови для життя громадян, здійснення їхніх прав (наприклад права власності) та належного функціонування органів влади, юридичних осіб та громадських формувань.

Згідно з роз'ясненнями, викладеними в пункті 12 Постанови Пленуму Верховного Суду України «Про практику розгляду судами клопотань про визнання й виконання рішень іноземних судів та арбітражів і про скасування рішень, постановлених у порядку міжнародного комерційного арбітражу на території України» від 24.12.1999, під публічним порядком належить розуміти правопорядок держави, визначальні принципи та засади, які

¹ Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>.

становлять основу сформованого в ній ладу (стосуються її незалежності, цілісності, самостійності й недоторканності, основних конституційних прав, свобод, гарантій тощо)¹.

У статті 1 Закону України «Про Національну гвардію України» визначено, що Національна гвардія України є військовим формуванням з правоохоронними функціями, що входить до системи Міністерства внутрішніх справ України і призначено для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від кримінальних та інших протиправних посягань, охорони громадської безпеки і порядку та забезпечення громадської безпеки, а також у взаємодії з правоохоронними органами – із забезпечення державної безпеки і захисту державного кордону, припинення терористичної діяльності, діяльності незаконних воєнізованих або збройних формувань (груп), терористичних організацій, організованих груп та злочинних організацій².

Наказом Міністерства внутрішніх справ України 10.08.2016 № 773 визначається механізм організації взаємодії Національної гвардії України (НГУ) та Національної поліції України у сфері забезпечення (охорони) публічної (громадської) безпеки і порядку. Цей Порядок діє у мирний час, за винятком періоду надзвичайного стану³.

Взаємодія між НГУ та Національною поліцією України здійснюється в межах, визначених законодавством, шляхом:

спільного патрулювання нарядами вулиць, площ, парків, скверів, вокзалів, аеропортів, морських та річкових портів, інших публічних (громадських) місць;

забезпечення (охорони) публічної (громадської) безпеки і порядку під час проведення зборів, мітингів, вуличних походів, демонстрацій, інших масових та спортивних заходів, а також під час заходів у публічних (громадських) місцях за участю осіб, щодо яких здійснюється державна охорона;

проведення спільних заходів з метою стабілізації оперативної обстановки в разі її загострення в межах території однієї чи декількох адміністративно-територіальних одиниць.

У положеннях статті 228 Цивільного кодексу України викладено, правові наслідки вчинення правочину, який порушує публічний порядок, вчинений з метою, що суперечить інтересам держави і суспільства.

Правочин вважається таким, що порушує публічний порядок, якщо він був спрямований на порушення конституційних прав і свобод людини і

¹ Про практику розгляду судами клопотань про визнання й виконання рішень іноземних судів та арбітражів і про скасування рішень, постановлених у порядку міжнародного комерційного арбітражу на території України: Постанова Пленуму Верховного Суду України від 24.12.1999. URL: <https://zakon.rada.gov.ua/laws/show/v0012700-99#Text>.

² Про Національну гвардію України: Закон України від 13.03.2014 № 876-VII. URL: <https://zakon.rada.gov.ua/laws/show/876-18#Text>.

³ Про затвердження Порядку організації взаємодії Національної гвардії України та Національної поліції України під час забезпечення (охорони) публічної (громадської) безпеки і порядку: наказ МВС України від 10.08.2016 № 773. URL: <https://zakon.rada.gov.ua/laws/show/z1223-16#Text>.

громадянина, знищення, пошкодження майна фізичної або юридичної особи, держави, Автономної Республіки Крим, територіальної громади, незаконне заволодіння ним.

Правочин, який порушує публічний порядок, є нікчемним.

У разі недодержання вимоги щодо відповідності правочину інтересам держави і суспільства, його моральним засадам такий правочин може бути визнаний недійсним¹.

Відповідно до частини 1 статті 1 Закону України «Про особливості забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольних матчів» надається таке визначення термінів:

громадська безпека – стан захищеності життєво важливих інтересів суспільства, сконцентрованих у його матеріальних і духовних цінностях, від джерел небезпеки природного або штучного характеру під час підготовки та проведення футбольних матчів, за якого забезпечується запобігання загрозам заподіяння шкоди такими джерелами небезпеки;

громадський порядок – сукупність суспільних відносин, що забезпечують нормальні умови життєдіяльності людини, діяльності підприємств, установ і організацій під час підготовки та проведення футбольних матчів шляхом встановлення, дотримання і реалізації правових та етичних норм;

спеціальні суб'єкти забезпечення громадського порядку та громадської безпеки – Національна поліція та центральний орган виконавчої влади, що реалізує державну політику у сфері цивільного захисту, в особі їх органів або підрозділів, які у встановленому законодавством порядку та у межах своєї компетенції відповідають за забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольного матчу;

стратегія безпеки спортивної споруди – документація, розроблена оператором спортивної споруди за участю органів Національної поліції та державного пожежного нагляду, що передбачає порядок організації та проведення футбольних матчів на даній спортивній споруді, у тому числі підтримання громадського порядку та громадської безпеки, пожежної безпеки, надання невідкладної допомоги, евакуації².

Механізм проведення МВС України огляду громадської безпеки та цивільного захисту визначено у постанові Кабінету Міністрів України від 22 травня 2019 р. № 507 «Про затвердження Порядку проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ»³.

¹ Цивільний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.

² Про особливості забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольних матчів: Закон України від 08.07.2011 № 3673-VI. URL: <https://zakon.rada.gov.ua/laws/show/3673-17#Text>.

³ Про затвердження Порядку проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ: постанова Кабінету Міністрів України від 22 травня 2019 р. № 507. URL: <https://zakon.rada.gov.ua/laws/show/507-2019-%D0%BF#Text>.

Наведені в цьому Порядку терміни вживаються в такому значенні:

громадська безпека і порядок – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз;

єдиний перелік спроможностей МВС із забезпечення громадської безпеки та цивільного захисту із забезпечення громадської безпеки та цивільного захисту – сукупність наявних, необхідних і перспективних спроможностей МВС, Національної поліції, ДСНС, ДМС та Національної гвардії, які використовуються для забезпечення громадської безпеки та цивільного захисту, з описом їх характеристик та вимог до них;

надлишкові спроможності – спроможності, застосування яких не спрямоване на виконання жодного із завдань, а також ті, застосування яких у подальшому є неможливим або недоцільним;

наявні спроможності – спроможності, що є в розпорядженні відповідного органу для виконання завдань;

необхідні спроможності – спроможності, що повинні бути в розпорядженні відповідного органу у визначений час та місці для виконання завдань у певних умовах середовища з метою досягнення необхідного результату (ефекту);

огляд громадської безпеки – процедура оцінювання стану захищеності життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина від протиправних посягань і готовності МВС, Національної поліції, ДСНС, ДМС та Національної гвардії до забезпечення громадської безпеки;

огляд цивільного захисту – процедура оцінювання стану готовності єдиної державної системи цивільного захисту, її функціональних і територіальних підсистем, сил цивільного захисту до реагування на можливі надзвичайні ситуації та стану захисту населення і територій від таких ситуацій;

перспективні спроможності – спроможності, що повинні бути в розпорядженні відповідного органу у визначений час та місці для виконання ним завдань за призначенням відповідно до імовірних сценаріїв виникнення та розвитку ситуацій;

спроможність – здатність МВС, Національної поліції, ДСНС, ДМС та Національної гвардії виконувати завдання за призначенням за певних умов з використанням наявних ресурсів відповідно до визначених сценаріїв дій у межах повноважень та способів, що передбачені Конституцією та законами України.

Огляд громадської безпеки та цивільного захисту проводиться з метою оцінювання сучасних і перспективних загроз життєво важливим для держави, суспільства та особи інтересам, правам і свободам людини і громадянина, розроблення ефективної моделі протидії злочинності та іншим протиправним

посяганням, а також запобігання та ліквідації надзвичайних ситуацій; для практичного виконання завдань щодо набуття Україною членства в ЄС, вжиття комплексу невідкладних заходів, спрямованих на подолання наслідків повномасштабного збройного вторгнення, оцінки стану і готовності МВС, Національної поліції, ДСНС, ДМС та Національної гвардії (далі – органи системи МВС) до виконання визначених законами повноважень, стану їх кадрового, фінансового, матеріально-технічного та інших видів забезпечення, а також наявних спроможностей щодо ефективного реагування на виклики і загрози у сфері громадської безпеки та цивільного захисту.

За результатами огляду громадської безпеки та цивільного захисту формуються перспективні моделі організації діяльності органів системи МВС з урахуванням реальних і потенційних загроз у визначених законом сферах їх діяльності та фінансово-економічних можливостей держави; розробляється Стратегія громадської безпеки та цивільного захисту України, що є основою для розроблення інших галузевих стратегій і концепцій, державних цільових програм у сферах громадської безпеки, цивільного захисту та міграційної політики, а також для розроблення оперативних планів та планів застосування сил і засобів у кризових ситуаціях; розробляються стратегічні та програмні документи; актуалізуються нормативно-правові акти з питань формування та реалізації державної політики у визначених законом сферах у мирний час та під час дії правових режимів надзвичайного та воєнного стану.

Завданнями огляду громадської безпеки та цивільного захисту є:

- 1) прогнозування (аналіз) майбутнього безпекового середовища;
- 2) оцінка здатності спроможностей органів системи МВС щодо виконання завдань за призначенням та імовірними сценаріями виникнення та розвитку кризових ситуацій на довгострокову перспективу, зокрема з урахуванням загроз воєнного характеру, а також оцінка результатів виконання поставлених завдань за попередній період;
- 3) визначення переліку необхідних спроможностей органів системи МВС, які відповідатимуть потребам сил безпеки та сил оборони з урахуванням ресурсних можливостей держави;
- 4) визначення переліку надлишкових спроможностей органів системи МВС;
- 5) уточнення завдань органів системи МВС за імовірними сценаріями виникнення та розвитку безпекової ситуації, зокрема з урахуванням загроз воєнного характеру;
- 6) планування спроможностей органів системи МВС;
- 7) актуалізація та вдосконалення законодавства з метою правового регулювання діяльності органів системи МВС в умовах нових викликів у безпековому середовищі;
- 8) формування потреби в ресурсному забезпеченні на розвиток спроможностей органів системи МВС;
- 9) аналіз ризиків у діяльності органів системи МВС;

10) оцінка стану досягнення цілей і завдань діючих програм і планів, спрямованих на досягнення спроможностей органів системи МВС.

Стратегія громадської безпеки та цивільного захисту України визначає загрози національній безпеці у сферах громадської безпеки та цивільного захисту та шляхи досягнення цілей і реалізації пріоритетів державної політики у цих сферах, зокрема:

1) готовність сил та засобів виконувати завдання за призначенням, інфраструктуру, напрями розвитку, інші показники, необхідні для планування діяльності Міністерства внутрішніх справ України, Національної гвардії України, Національної поліції України, Державної міграційної служби України, Державної служби України з надзвичайних ситуацій;

2) потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів;

3) державні програми, галузеві стратегії та програми, які мають бути спрямовані на реалізацію Стратегії громадської безпеки та цивільного захисту України, їхні цілі, відповідальних за розроблення документів, моніторинг їх виконання та оцінки¹.

У статті 24 Конституції України визначено, що громадяни мають рівні конституційні права і свободи та є рівними перед законом. Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками².

Але, слід звернути увагу, що у виключних випадках можливе обмеження певних прав людини. Так, відповідно до статті 29 Конституції України кожна людина має право на свободу та особисту недоторканність. Ніхто не може бути заарештований або триматися під вартою інакше як за вмотивованим рішенням суду і тільки на підставах та в порядку, встановлених законом. У разі нагальної необхідності запобігти злочинові чи його перепинити уповноважені на те законом органи можуть застосувати тримання особи під вартою як тимчасовий запобіжний захід, обґрунтованість якого протягом сімдесяти двох годин має бути перевірена судом. Затримана особа негайно звільняється, якщо протягом сімдесяти двох годин з моменту затримання їй не вручено вмотивованого рішення суду про тримання під вартою.

У статті 30 Конституції України зазначено, що кожному гарантується недоторканність житла. Не допускається проникнення до житла чи до іншого володіння особи, проведення в них огляду чи обшуку інакше як за вмотивованим рішенням суду. У невідкладних випадках, пов'язаних із врятуванням життя людей та майна чи з безпосереднім переслідуванням осіб, які підозрюються у вчиненні злочину, можливий інший, встановлений

¹ Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

² Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

законом, порядок проникнення до житла чи до іншого володіння особи, проведення в них огляду і обшуку.

Стаття 34 Конституції України визначає, що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 35 – кожен має право на свободу світогляду і віросповідання. Це право включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноособово чи колективно релігійні культи і ритуальні обряди, вести релігійну діяльність. Здійснення цього права може бути обмежене законом лише в інтересах охорони громадського порядку, здоров'я і моральності населення або захисту прав і свобод інших людей.

Стаття 36 – громадяни України мають право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів, за винятком обмежень, встановлених законом в інтересах національної безпеки та громадського порядку, охорони здоров'я населення або захисту прав і свобод інших людей.

Стаття 39 – громадяни мають право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації, про проведення яких завчасно сповіщаються органи виконавчої влади чи органи місцевого самоврядування. Обмеження щодо реалізації цього права може встановлюватися судом відповідно до закону і лише в інтересах національної безпеки та громадського порядку – з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення або захисту прав і свобод інших людей.

1.2. Забезпечення публічного порядку органами і підрозділами Національної поліції України

Підтримання публічного порядку є однією з фундаментальних функцій демократичної держави, що прямо пов'язана із реалізацією прав і свобод людини, стабільністю суспільства та довірою до влади. Національна поліція України як центральний суб'єкт охорони публічного порядку забезпечує безпеку громадян у повсякденному житті та під час масових подій, реагує на правопорушення, здійснює превентивну діяльність.

Правову основу забезпечення публічного порядку органами Національної поліції становлять: Конституція України, яка гарантує права людини та визначає обов'язок держави забезпечувати безпеку громадян; Кодекс України про адміністративні правопорушення; Закон України «Про Національну поліцію», що закріплює повноваження поліції у сфері превенції та охорони порядку; відомчі накази МВС, міжнародні стандарти правоохоронної діяльності. Ці акти формують нормативну систему, що визначає межі, процедури та гарантії діяльності поліції у сфері забезпечення публічного порядку.

Основними завданнями Національної поліції у забезпеченні публічного порядку є:

- охорона прав і свобод людини та громадянина;
- забезпечення безпеки в громадських місцях;
- профілактика правопорушень, у тому числі превентивні поліцейські заходи;
- нагляд за дотриманням правил у сфері дорожнього руху, благоустрою, тиші, охорони масових заходів;
- оперативне реагування на повідомлення про правопорушення;
- забезпечення публічної безпеки та порядку під час масових заходів;
- взаємодія з органами місцевого самоврядування, громадськими формуваннями.

Ключову роль у забезпеченні публічного порядку в системі органів Національної поліції відіграють: **патрульна поліція та підрозділи реагування патрульної поліції, відділи превентивної комунікації (поліція діалогу), служба дільничних офіцерів поліції та поліцейських офіцерів громад, підрозділи ювенальної превенції, служба освітньої безпеки, поліція особливого призначення, підрозділи поліції охорони та інші підрозділи Національної поліції, орієнтовані на забезпечення окремих аспектів публічного порядку.**

Патрульна поліція та підрозділи реагування патрульної поліції відіграють ключову роль у підтриманні публічної безпеки та порядку, оскільки саме вони забезпечують постійну, безперервну та найбільш видиму присутність поліції у публічному просторі. Їх діяльність спрямована на оперативне реагування на правопорушення, попередження небезпечних

ситуацій та формування безпечного середовища у громадах. Першочерговим завданням патрульної поліції є здійснення цілодобового патрулювання вулиць, площ, парків, місць масового перебування людей, що забезпечує постійний контроль за криміногенною ситуацією та дає змогу своєчасно виявляти й припиняти адміністративні й кримінальні правопорушення. Публічна присутність патрулів має превентивний ефект, знижує рівень правопорушень та підвищує відчуття безпеки серед населення. Патрульна поліція забезпечує негайний виїзд на повідомлення громадян, що надходять через лінію «102», та інші канали. Їх завдання полягає у швидкому з'ясуванні обставин події, відновленні публічного порядку, локалізації загроз та наданні допомоги потерпілим. Оперативність реагування є визначальною умовою мінімізації негативних наслідків правопорушень і кризових ситуацій. Важливою складовою діяльності є регулювання дорожнього руху, здійснення контролю за безпекою дорожнього руху, попередження ДТП та реагування на аварійні ситуації. Це напряду пов'язано з підтриманням публічного порядку, оскільки аварійність і транспортні порушення мають високий ризик загрози життю та здоров'ю громадян.

Патрульна поліція також бере участь у забезпеченні порядку під час масових заходів, спортивних і культурних подій, виборів, урочистостей та інших подій, що передбачають масове скупчення людей. Її завдання полягає у запобіганні конфліктним ситуаціям, недопущенні провокацій, контролі потоків людей і реагуванні на будь-які інциденти, що загрожують публічній безпеці. Крім того, значну роль відіграє взаємодія з населенням: спілкування з громадянами, прийом звернень, участь у превентивних програмах, здійснення роз'яснювальної роботи щодо правил поведінки у публічному просторі, особистої та колективної безпеки. Такий підхід формує довіру до поліції та сприяє розвитку партнерських відносин між поліцією й громадою.

Узагальнюючи, патрульна поліція та підрозділи реагування патрульної поліції виступають основною силою оперативного забезпечення публічного порядку, забезпечуючи постійний моніторинг, швидке реагування, превенцію правопорушень, захист громадян та стабільність у публічному просторі. Їх діяльність є фундаментом повсякденної безпеки та базовою умовою належного функціонування суспільства.

Відділи превентивної комунікації («поліція діалогу»), є одним із сучасних інструментів Національної поліції України, спрямованих на превентивне забезпечення публічного порядку шляхом налагодження комунікації між поліцейськими та учасниками масових заходів, локальних конфліктних ситуацій або потенційно ризикових подій. Їхня діяльність ґрунтується на принципах партнерства, відкритості та зниження соціальної напруги. Ключова роль поліції діалогу полягає у запобіганні конфліктам та мінімізації ризику застосування сили. На відміну від силових або тактичних підрозділів, поліцейські діалогу працюють у «першій лінії комунікації», завдяки чому забезпечують оперативне інформування громадян про правила поведінки, умови проведення заходів та допустимі межі дій. Це дозволяє упереджувати правопорушення ще до їхнього виникнення.

Основні напрями їх внеску у забезпечення публічного порядку такі:

1. Превентивна комунікація з учасниками заходів. Поліцейські діалогу у доступній формі пояснюють вимоги законодавства, правила безпеки, обмеження та необхідні заходи. Чітке інформування знижує рівень непорозумінь та агресії, сприяючи добровільному дотриманню правопорядку.

2. Зниження конфліктності та посередництво. Підрозділи діалогу виступають посередниками між громадянами та іншими підрозділами поліції, що дозволяє деескалувати напружені ситуації й уникати силових сценаріїв. Їх цілеспрямована робота з емоціями та поведінкою натовпу істотно зменшує ризик масових заворушень.

3. Моніторинг настроїв та оцінка ризиків. Постійний контакт з учасниками заходів дає змогу оперативно оцінювати рівень соціальної напруги, виокремлювати потенційні загрози та своєчасно інформувати керівництво поліції, що посилює ефективність реагування.

4. Формування довіри до поліції. Присутність спеціально підготовлених комунікаторів підвищує сприйняття поліції як партнерської та сервісно орієнтованої інституції. Це зміцнює громадську безпеку, оскільки довіра громадян сприяє готовності співпрацювати, виконувати вимоги та повідомляти про правопорушення.

5. Підтримка дій інших підрозділів поліції. Поліція діалогу створює умови, за яких інші підрозділи – патрульні, поліція особливого призначення, охорона – виконують свої функції у менш конфліктному середовищі, що підвищує ефективність всього механізму забезпечення публічного порядку.

Таким чином, поліція діалогу відіграє системоутворюючу роль у сучасній моделі публічної безпеки, забезпечуючи превентивний, ненасильницький та комунікативний підхід до охорони громадського порядку. Її діяльність сприяє не лише збереженню стабільності під час масових заходів, а й формуванню нової культури взаємодії поліції з населенням, заснованої на партнерстві та довірі.

Дільничні офіцери поліції (ДОП) та поліцейські офіцери громад (ПОГ) відіграють ключову роль у щоденному забезпеченні публічного порядку та безпеки на території громади. Їх діяльність поєднує профілактику правопорушень, оперативне реагування, взаємодію з населенням та різними органами влади та регламентується Інструкцією щодо організації діяльності дільничних офіцерів поліції та поліцейських офіцерів громад, затвердженої Міністерством внутрішніх справ України від 28.07.2017 № 650¹.

Одним із ключових напрямів їх роботи є превентивна діяльність, яка спрямована на виявлення криміногенних чинників у середовищі громади, здійснення індивідуальної профілактики щодо осіб групи ризику та формування безпечного соціального середовища. Завдяки систематичним профілактичним бесідам, роботі з сім'ями, що перебувають у складних

¹ Про затвердження Інструкції з організації діяльності дільничних офіцерів поліції та поліцейських офіцерів громад : наказ МВС України від 28.07.2017 № 650. URL: <https://zakon.rada.gov.ua/laws/show/z1041-17#Text>.

життєвих обставинах, а також ідентифікації причин та умов, які сприяють правопорушенням, ДОП та ПОГ створюють підґрунтя для запобігання протиправній поведінці ще до її виникнення.

Важливе значення у підтриманні публічного порядку має ведення профілактичного обліку осіб, схильних до правопорушень. Контроль за дотриманням ними встановлених законодавством чи судом обмежень, оцінка ризиків їх повторної протиправної поведінки та здійснення індивідуальної профілактики сприяють зменшенню рівня рецидивної злочинності та стабілізації оперативної ситуації на території обслуговування. Значна частина роботи ДОП та ПОГ пов'язана також із забезпеченням оперативного реагування на заяви та повідомлення громадян про правопорушення або події. Виїзд на місце події, фіксація обставин, складання адміністративних матеріалів, участь у дізнанні щодо кримінальних проступків – усе це дозволяє негайно відновити правопорядок у ситуаціях, що створюють загрозу безпеці населення.

Не менш важливою сферою їхньої діяльності є забезпечення публічної безпеки під час масових заходів – зібрань, святкових подій, демонстрацій. У таких умовах дільничні та офіцери громади здійснюють профілактику конфліктів, моніторинг поведінки учасників заходу, недопущення порушень громадського порядку, що має безпосередній вплив на загальний стан безпеки у громаді. Особливе місце у їх повноваженнях посідає контроль за дотриманням правил обігу зброї та предметів дозвільної системи, що пов'язано з мінімізацією ризиків незаконного використання небезпечних предметів у публічному просторі. Перевірка належних умов зберігання зброї, реагування на порушення та ініціювання анулювання дозволів у разі загрози безпеці формують важливий запобіжний механізм для охорони громадського порядку.

У межах роботи з дітьми та особами, що перебувають у складних життєвих обставинах, ДОП і ПОГ здійснюють превентивні заходи, спрямовані на недопущення залучення дітей до кримінальної поведінки та їх захист від можливих загроз. Це включає взаємодію зі службами у справах дітей, закладами освіти та соціального захисту. Такі заходи сприяють формуванню безпечного середовища для неповнолітніх і водночас позитивно впливають на загальний стан публічного порядку в громаді.

Водночас важливою складовою діяльності дільничних офіцерів та офіцерів громади є партнерство з населенням та місцевою владою. У межах моделі «поліція громади» вони організовують зустрічі з жителями дільниці, звітують про стан правопорядку, визначають актуальні ризики, залучають громадян до профілактичних ініціатив і формувань з охорони громадського порядку. Така взаємодія виявляється ефективним інструментом зміцнення довіри до поліції та підвищення рівня соціального контролю за ситуацією у громаді.

Забезпечення публічного порядку неможливе без належної координації діяльності правоохоронних, соціальних та адміністративних структур. Саме тому ДОП і ПОГ активно співпрацюють з органами місцевого

самоврядування, соціальними службами, навчальними закладами, Державною прикордонною службою та іншими підрозділами Національної поліції. Така міжвідомча взаємодія забезпечує комплексний підхід до підтримання безпеки, дозволяє оперативно реагувати на зміни криміногенної ситуації, а також сприяє реалізації спільних програм і профілактичних заходів.

З метою підвищення ефективності роботи у сфері забезпечення публічного порядку офіцери громади та дільничні поліцейські здійснюють постійний моніторинг території обслуговування, ведуть контрольно-наглядові справи, аналізують криміногенну обстановку, визначають проблемні місця та групи ризику. На основі отриманих даних складаються плани превентивних заходів, що дозволяє планувати діяльність поліції на науково обґрунтованих засадах.

Окреме значення має забезпечення доступності поліцейських послуг для громадян. Організація прийому мешканців у поліцейських станціях або приміщеннях органів місцевого самоврядування, належна реєстрація звернень, а також можливість оперативного зв'язку з поліцейськими через засоби комунікації підвищують рівень довіри населення та формують відчуття захищеності, що є однією з ознак ефективної діяльності поліції у сфері підтримання публічного порядку.

Ювенальна превенція є підрозділом Національної поліції України, який забезпечує публічну безпеку і правопорядок через комплексний захист прав та інтересів дітей у публічному просторі та в середовищі їх життєдіяльності шляхом виконання завдань, зазначених в Інструкції про організацію роботи підрозділів ювенальної превенції Національної поліції України, затверджена наказом МВС України від 19.12.2017 № 1044¹.

Підрозділи ювенальної превенції Національної поліції України відіграють важливу роль у підтриманні публічного порядку, оскільки їхня діяльність спрямована на профілактику правопорушень у дитячому середовищі, захист прав дітей та усунення факторів, що створюють ризики для безпеки громади, адже профілактика правопорушень серед дітей безпосередньо впливає на загальний рівень правопорядку. Виявлення причин девіантної поведінки та системне проведення профілактичних заходів у школах і за місцем проживання зменшує ймовірність учинення кримінальних та адміністративних правопорушень неповнолітніми.

Поліцейське піклування та запобігання дитячій бездоглядності є важливими для запобігання появі ситуацій, що можуть призвести до вчинення дітьми небезпечних або асоціальних дій у публічному просторі. Своєчасне виявлення дітей без нагляду та їхня передача до безпечного середовища знижує ризики порушення порядку. Значний внесок у забезпечення публічної безпеки має реагування на випадки домашнього насильства щодо дітей або з боку дітей. Усунення загроз життю і здоров'ю

¹ Про затвердження Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України : наказ МВС України від 19.12.2017 № 1044. URL: <https://zakon.rada.gov.ua/laws/show/z0686-18#Text>

неповнолітніх, застосування термінових заборонних приписів, а також робота з дітьми-кривдниками сприяють стабілізації ситуації у сім'ях, що є важливою складовою загального правопорядку.

Важливим елементом є також контроль за дотриманням законодавчих обмежень у публічному просторі (заборона продажу алкоголю, тютюну неповнолітнім, перебування дітей у нічний час у розважальних закладах). Ці заходи прямо спрямовані на запобігання ризикованій поведінці неповнолітніх та підтримання публічного порядку. Особливої уваги заслуговує участь ювенальних поліцейських у забезпеченні реалізації права дитини на освіту, адже систематичне відвідування навчання, контроль за бродяжництвом і прогулами, взаємодія зі службами у справах дітей сприяють зменшенню соціальних ризиків і підвищенню рівня безпеки у громадах. Крім того, розшук безвісти зниклих дітей є важливим напрямом роботи, оскільки ситуації зникнення дітей створюють серйозні загрози для публічної безпеки та потребують швидкого й координованого реагування. Нарешті, міжвідомча взаємодія з іншими підрозділами поліції, органами влади, закладами освіти та соціальними службами забезпечує комплексний підхід до профілактики правопорушень серед дітей, що підсилює загальну спроможність держави підтримувати стабільний публічний порядок.

Служба освітньої безпеки Національної поліції України є новоствореним спеціалізованим підрозділом, створеним з метою забезпечення публічного порядку та безпеки в закладах загальної середньої освіти. Її поява зумовлена потребою у формуванні стійкого безпечного освітнього середовища, здатного ефективно реагувати на сучасні виклики, пов'язані як з воєнними ризиками, так і з внутрішніми загрозами у дитячому середовищі. Служба освітньої безпеки реалізує державну політику у сфері захисту прав та законних інтересів учасників освітнього процесу, здійснює превентивну діяльність, контролює стан безпеки в закладах освіти та виконує спеціально визначені функції, спрямовані на підтримання належного рівня публічного порядку у шкільному просторі. Її діяльність передбачає постійну присутність поліцейського в закладах освіти, оперативне реагування на правопорушення й надзвичайні події, а також тісну взаємодію з педагогами, батьками, органами влади та іншими суб'єктами забезпечення безпеки¹.

Діяльність **поліції охорони** у системі Національної поліції України має важливе значення для забезпечення публічного порядку та безпеки, особливо в частині запобігання посяганням на об'єкти критичної інфраструктури, державне майно та життя і здоров'я громадян. Основний зміст роботи підрозділів поліції охорони полягає не лише у фізичному захисті майна чи осіб на договірних засадах, а й у виконанні функцій, що прямо впливають на рівень публічної безпеки в державі. Під час здійснення охоронної діяльності виконують завдання з:

¹ Про затвердження Інструкції з організації роботи підрозділів Національної поліції України із забезпечення безпечного освітнього середовища в закладах загальної середньої освіти : наказ МВС України від 01.10.2024 № 663. URL: <https://zakon.rada.gov.ua/laws/show/z1590-24#Text>

1) охорони об'єктів (майна) усіх форм власності шляхом контролю за станом майнової безпеки об'єкта охорони, використання пунктів централізованого спостереження та оперативного реагування нарядів поліції охорони на повідомлення про спрацювання технічних засобів охорони чи інші повідомлення про правопорушення;

2) охорони валютних та інших цінностей, вантажів під час їх перевезення транспортними засобами, інкасації;

3) охорони фізичних осіб шляхом запобігання загрозам особистій безпеці фізичної особи, яка охороняється;

4) інші повноваження відповідно до законодавства України та нормативно-правових актів МВС¹.

Таким чином, передусім поліція охорони здійснює контроль за станом майнової безпеки об'єктів різних форм власності. Використання систем централізованого спостереження та оперативне реагування на сигнали тривоги забезпечують можливість швидкого припинення правопорушень, мінімізації наслідків злочинних дій та недопущення порушення публічного порядку на прилеглих територіях. Важливим напрямом є охорона перевезення валютних цінностей, вантажів, документів суворого обліку. Такі заходи спрямовані на запобігання розбійним нападам, крадіжкам, посяганням на стратегічно важливі ресурси, що становлять підвищену суспільну небезпеку. Окреме місце у забезпеченні публічної безпеки займає охорона фізичних осіб, під час якої поліція охорони виконує превентивні заходи щодо виявлення і нейтралізації загроз життю та здоров'ю людей. Це сприяє не лише захисту конкретної особи, а й загальній стабільності в громадських місцях, оскільки попереджає потенційні резонансні правопорушення.

Особливо значущою є діяльність підрозділів поліції охорони на об'єктах, що мають критичне значення для держави. До таких об'єктів належать, зокрема, об'єкти стратегічного значення в енергетичній, нафтогазовій та транспортній сферах; органи державної влади та місцевого самоврядування; сховища небезпечних речовин; об'єкти зберігання та виготовлення зброї, боєприпасів, вибухових матеріалів; архівні та музейні фонди; об'єкти інформаційної інфраструктури держави; пунктів проведення ЗНО та інші установи, діяльність яких має суспільно важливий характер, тощо².

Охорона таких об'єктів спрямована на запобігання диверсіям, терактам, крадіжкам, пошкодженню критично важливого майна та порушенню безпеки населення. Це є елементом національної безпеки та прямо впливає на загальний стан публічного порядку. Форми охорони – фізична охорона та/або використання технічних засобів – визначаються з урахуванням особливостей кожного об'єкта, ступеня ризику та умов його

¹ Про організацію службової діяльності поліції охорони з питань забезпечення фізичної охорони об'єктів: Наказ МВС України від 07.07.2017 № 577. Дата оновлення: 27.11.2018. URL: <https://zakon.rada.gov.ua/laws/show/z0989-17#n21>

² Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах: Постанова Кабінету міністрів України від 21 листопада 2018 р. № 975. URL: <https://zakon.rada.gov.ua/laws/show/975-2018-%D0%BF#n15>

розташування. У випадках підвищеної загрози поліція охорони може посилювати охорону навіть на об'єктах, де вже працюють відомчі чи спеціалізовані підрозділи, що сприяє комплексному забезпеченню безпеки¹. Таким чином, діяльність поліції охорони становить важливу складову системи забезпечення публічного порядку та безпеки. Її робота спрямована на запобігання правопорушенням, охорону стратегічних об'єктів, захист громадян, а також на підвищення стійкості держави до внутрішніх і зовнішніх загроз.

Діяльність підрозділів **поліції особливого призначення** є одним з ключових елементів системи забезпечення публічної безпеки та порядку в Україні, особливо в умовах підвищених ризиків, суспільної напруги та воєнного стану. Виконуючи спеціальні завдання, визначені наказом МВС України від 04.12.2017 року № 987², ці підрозділи не лише реагують на правопорушення, а й формують превентивний захисний механізм держави, спрямований на стабілізацію ситуації в суспільстві.

Діяльність із запобігання, виявлення та припинення адміністративних і кримінальних правопорушень безпосередньо сприяє підтриманню публічного порядку. Підрозділи особливого призначення залучаються у ситуаціях, коли існує підвищений рівень загроз, що потребує швидкого, професійного та силового реагування. Їхня присутність і оперативність знижує ймовірність ескалації правопорушень, припиняє небезпечні дії та забезпечує контроль над складною оперативною обстановкою. Вагому роль підрозділи особливого призначення відіграють у забезпеченні безпеки під час масових заходів: зборів, мітингів, демонстрацій тощо. Саме від них залежить недопущення провокацій, конфліктів, тисняви та інших загроз життю і здоров'ю громадян. Чітка організація охорони публічного порядку під час масових заходів є запорукою реалізації конституційних прав громадян на мирні зібрання, водночас гарантує загальний громадський спокій. Забезпечення безпеки осіб, які перебувають під державним захистом, та охорона адміністративних і державних будівель мають суттєве значення для стабільності в державі. Охорона таких об'єктів запобігає посяганням на органи влади, порушенням їх діяльності, диверсіям або терактам, що можуть мати широкі негативні наслідки для суспільної безпеки. Підрозділи особливого призначення також беруть активну участь у антитерористичних операціях, що безпосередньо впливає на рівень безпеки держави і громадян. Їхня діяльність спрямована на нейтралізацію терористичних загроз, недопущення терактів і мінімізацію наслідків можливих нападів. Таким чином формується один із ключових бар'єрів у системі національної безпеки.

Особливої ваги їх робота набуває в умовах воєнного стану, коли підрозділи особливого призначення залучаються до оборони держави, виконання завдань територіальної оборони та забезпечення заходів правового

¹ Про затвердження Порядку забезпечення охорони об'єктів органами поліції охорони на договірних засадах: Наказ МВС України від 14.12.2022 № 816. URL: <https://zakon.rada.gov.ua/laws/show/z0126-23#Text>

² Про затвердження Положення про підрозділи поліції особливого призначення: Наказ МВС України від 04.12.2017 № 987. URL: <https://zakon.rada.gov.ua/laws/show/z1565-17#Text>

режиму воєнного стану. У цей період їх діяльність спрямована на підтримання публічного порядку на територіях, які зазнають обстрілів, диверсій або перебувають у безпосередній близькості до бойових дій. Забезпечення контролю, підтримання безпеки, припинення мародерства, реагування на загрози – усе це створює умови для функціонування критичної інфраструктури, евакуації населення та стабільної роботи органів державної влади.

Таким чином, підрозділи поліції особливого призначення забезпечують публічний порядок і безпеку шляхом виконання комплексу завдань, спрямованих на стабілізацію ситуації в громаді, захист громадян і протидію загрозам підвищеного рівня. Їх діяльність є невід’ємною складовою загальної системи безпеки держави в мирний та воєнний час.

В умовах воєнного стану Національна поліція України є одним із ключових суб’єктів забезпечення публічного порядку. Забезпечення публічного порядку Національною поліцією в умовах воєнного стану має низку сутнісних особливостей, що якісно відрізняються від діяльності у мирний час. По-перше, змінюється правовий режим здійснення поліцейських повноважень: значна частина заходів реалізується в умовах дії спеціальних обмежень прав і свобод людини, запроваджених на підставі Закону України «Про правовий режим воєнного стану», що зумовлює посилення ролі поліції як інструмента реалізації режимних приписів. По-друге, пріоритетного значення набувають превентивні, стабілізаційні та охоронні функції, спрямовані на нейтралізацію загроз національній безпеці, протидію диверсійним і терористичним проявам, охорону об’єктів критичної інфраструктури та забезпечення виконання таких заходів, як комендантська година, спеціальний порядок пересування осіб і транспорту. По-третє, службова діяльність поліції характеризується підвищеним рівнем ризику, необхідністю оперативного реагування в умовах динамічної та небезпечної обстановки, що потребує розширеного застосування спеціальних засобів, сучасних технічних систем нагляду й документування.

Діяльність Національної поліції в таких умовах спирається на комплекс нормативно-правових актів, які визначають особливий порядок функціонування органів публічної влади в період збройної агресії та встановлюють баланс між вимогами безпеки й гарантіями прав людини. Конституція України проголошує людину, її життя і здоров’я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю, а утвердження і забезпечення прав і свобод людини – головним обов’язком держави. Основний Закон гарантує кожному невід’ємні права, зокрема право на життя, особисту недоторканність і свободу, повагу до гідності, рівність перед законом, право на судовий захист тощо. Водночас під час воєнного стану допускається тимчасове обмеження окремих прав і свобод, але лише в межах, прямо визначених Конституцією України, із дотриманням критеріїв необхідності, законності та пропорційності. Частина прав, перелік яких міститься в статті 64 Конституції України, не підлягає обмеженню, що є

базовою передумовою для правомірної діяльності поліції навіть у надзвичайних умовах¹.

Одним із центральних нормативно-правових актів, який визначає правові засади функціонування органів державної влади в умовах воєнного стану, є Закон України «Про правовий режим воєнного стану». Стаття 8 цього Закону встановлює перелік заходів, які можуть бути запроваджені на територіях, де введено воєнний стан². Хоча сама стаття не містить прямого переліку повноважень Національної поліції, більшість передбачених заходів реалізуються саме за її участю, оскільки поліція відповідає за підтримання публічної безпеки, охорону публічного порядку, контроль за виконанням правових обмежень і превенцію правопорушень.

Частина перша статті 8 Закону України «Про правовий режим воєнного стану» передбачає, що військове командування разом із військовими адміністраціями можуть самостійно або із залученням органів виконавчої влади, до яких належить і Національна поліція, здійснювати визначені законом заходи³. Це означає, що поліція виступає основним інструментом практичної реалізації режиму воєнного стану в частині забезпечення публічного порядку: контролює дотримання обмежень, організовує охорону важливих об'єктів, супроводжує евакуаційні заходи, проводить превентивні та примусові дії у межах своєї компетенції.

Серед заходів, що безпосередньо стосуються забезпечення публічної безпеки, слід виокремити встановлення (посилення) охорони об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення. Так, підрозділи поліції залучаються до патрулювання прилеглих територій, охорони стратегічно важливих споруд, запровадження пропускового режиму, а також до протидії диверсійним чи терористичним загрозам. Важливою є й участь поліції у реалізації таких заходів, як запровадження комендантської години, обмеження свободи пересування, перевірка документів, огляд особистих речей, транспортних засобів і, у спеціально визначених законом випадках, житла громадян. Усі ці інструменти прямо впливають на стан публічного порядку та безпеки, але їх застосування повинно бути чітко врегульоване законом і не перетворюватися на свавільне втручання у приватне життя.

Окремий блок повноважень Національної поліції пов'язаний з обмеженням масових заходів. Воєнний стан не означає автоматичну тотальну заборону мирних зібрань, однак їх проведення істотно деталізується і ставиться в залежність від безпекової ситуації. Показовим є затверджений протоколом оперативного штабу Ради оборони Київської області № 145 від 07.07.2022 року порядок проведення масових заходів у регіоні: допускається лише виняткове проведення таких заходів за умови письмового погодження з

¹ Конституція України від 28 червня 1996 р. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

² Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. URL : <https://zakon.rada.gov.ua/laws/show/389-19#Text>

³ Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. URL : <https://zakon.rada.gov.ua/laws/show/389-19#Text>

виконавчими органами місцевого самоврядування. Ці органи зобов'язані завчасно повідомити Національну поліцію та інші компетентні суб'єкти¹, а поліція у свою чергу забезпечує належний публічний порядок під час заходу. За відсутності погодження поліція залучається до недопущення та припинення несанкціонованих зібрань, мітингів чи демонстрацій, щоб запобігти можливим загрозам безпеці та масовим порушенням правопорядку.

Стаття 8 Закону України «Про правовий режим воєнного стану» також покладає на поліцію низку завдань, безпосередньо спрямованих на захист життя і безпеки людей. Йдеться, зокрема, про участь у евакуації цивільного населення, евакуації затриманих осіб з ізоляторів тимчасового тримання, підозрюваних та обвинувачених, щодо яких обрано запобіжний захід у вигляді тримання під вартою, а також етапування засуджених із установ, розташованих поблизу районів ведення бойових дій, до більш безпечних регіонів. Паралельно поліція здійснює контроль за дотриманням заборон на переміщення осіб, виконанням рішень про заборону діяльності політичних партій або громадських об'єднань, сприяє підтриманню інформаційної безпеки². Всі ці функції мають виразний оборонний і безпековий характер, але також істотно впливають на реалізацію прав людини, що потребує від працівників поліції високого рівня професійної та правової відповідальності.

Важливою складовою діяльності Національної поліції щодо забезпечення публічного порядку в умовах воєнного стану є здійснення превентивних заходів. Йдеться про попередження кримінальних та адміністративних правопорушень, підтримання публічного порядку на вулицях і в громадських місцях, виявлення та нейтралізацію потенційних загроз у регіонах, де оперативна обстановка є нестабільною. Поліцейські мають діяти в умовах зростання соціальної напруги, мобілізаційних процесів, обмежень транспортної та інформаційної інфраструктури, що потребує від них не лише юридичної підготовки, а й психологічної стійкості, здатності працювати в умовах постійного ризику. При цьому стандартом діяльності мають залишатися норми міжнародного гуманітарного права та універсальні стандарти у сфері захисту прав людини, з дотриманням балансу між інтересами національної безпеки та гарантіями фундаментальних прав і свобод.

Розширення повноважень поліції в умовах воєнного стану, зокрема у частині застосування сили, використання зброї, здійснення оперативних дій у зоні бойових дій, має безпосередній вплив на забезпечення публічного порядку. Швидке реагування на загрози, у тому числі можливість повідомляти керівництво про застосування зброї або спецзасобів у спрощеній формі, обумовлене реаліями фронтової ситуації, дає змогу ефективніше захищати населення. Водночас задля недопущення зловживань

¹ Порядок проведення масових заходів на території Київської області в умовах правового режиму воєнного стану. URL : <https://koda.gov.ua/wp-content/uploads/2022/07/poryadok-provedennya-masovyh-zahodiv-na-terytorii-kyivskoї-oblas.pdf>

² Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. URL : <https://zakon.rada.gov.ua/laws/show/389-19#Text>

запроваджуються додаткові механізми контролю, зокрема обов'язкова електронна фіксація доступу до інформаційних ресурсів, розширення переліку персональних та біометричних даних, що збираються у встановленому законом порядку. Це дозволяє поєднати оперативність поліцейських дій із підзвітністю та прозорістю.

Запровадження сучасних технічних засобів у діяльність Національної поліції України в умовах воєнного стану набуває ключового значення, оскільки саме технологічні інструменти забезпечують підвищення ефективності підтримання публічної безпеки та правопорядку в умовах зростання військових і кримінальних загроз. Використання систем автоматичного відеоспостереження, аналітичного програмного забезпечення, безпілотних літальних апаратів та спеціалізованих комплексів фіксації наслідків обстрілів дозволяє поліції оперативніше реагувати на правопорушення, виявляти небезпечні ситуації та забезпечувати достовірну доказову базу.

Правові підстави застосування таких засобів містяться у статті 40 Закону України «Про Національну поліцію», яка надає поліцейським право використовувати технічні прилади та спеціальне програмне забезпечення для виконання службових завдань. Закон також передбачає можливість їх розміщення на форменому одязі, транспортних засобах, безпілотниках і навіть на об'єктах без спеціального маркування, що є виправданим в умовах воєнного конфлікту та підвищеного ризику диверсійної активності¹.

Технічні засоби виконують подвійне призначення. По-перше, вони мають превентивну функцію – сприяють стримуванню правопорушників, підвищенню рівня безпеки населення та своєчасному виявленню загроз. По-друге, вони забезпечують процесуальну функцію – фіксують події та обставини, що можуть бути використані як докази у кримінальних, адміністративних провадженнях чи справах про воєнні злочини.

Упровадження таких технологій є елементом адаптації системи забезпечення публічної безпеки до реалій гібридної війни. Вони підвищують можливості поліції у сфері оперативно-розшукової діяльності, одночасно створюючи правові та технічні гарантії захисту прав людини через об'єктивну фіксацію подій. Таким чином, технічна модернізація не лише посилює інституційну спроможність поліції діяти в умовах воєнного стану, а й сприяє зміцненню правових механізмів забезпечення безпеки та справедливості.

Окремим важливим напрямом діяльності Національної поліції в умовах воєнного стану є участь у заходах з оперативного розмінування вибухонебезпечних предметів, що залишилися після бойових дій або були навмисно встановлені з диверсійною чи кримінальною метою. Значення цього напрямку важко переоцінити, адже саме вибухонебезпечні предмети

¹ Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. URL : <https://zakon.rada.gov.ua/laws/show/580-19#Text>

становлять одну з найсерйозніших загроз життю та здоров'ю цивільного населення, а також стабільності та безпеці на звільнених територіях.

Діяльність підрозділів поліції у сфері розмінування охоплює комплекс завдань. По-перше, це оперативне реагування на повідомлення громадян щодо виявлення мін, снарядів, розтяжок, саморобних вибухових пристроїв та інших небезпечних об'єктів. У таких випадках поліцейські забезпечують охорону місця події, організовують евакуацію людей, перекривають доступ до небезпечних ділянок і координують роботу зі спеціалізованими вибухотехнічними підрозділами ДСНС та Збройних Сил України. По-друге, Національна поліція виконує важливу функцію виявлення вибухонебезпечних предметів у ході превентивних і стабілізаційних заходів. Під час патрулювання деокупованих територій, перевірки покинутих будівель, об'єктів критичної інфраструктури, транспортних вузлів або місць масового перебування людей поліція здійснює первинний огляд території з метою виявлення потенційних загроз та недопущення надзвичайних подій. По-третє, поліція бере участь у документуванні фактів встановлення вибухових пристроїв як способу вчинення кримінальних правопорушень або воєнних злочинів. Мова йде про фіксацію обставин, фото- та відеодокументування, вилучення залишків вибухових засобів, встановлення маршруту проникнення, а також взаємодію зі слідчими підрозділами для проведення досудового розслідування. Це особливо важливо для належної правової оцінки дій осіб, причетних до замінування територій, що може кваліфікуватися як терористична діяльність, диверсія чи порушення законів і звичаїв війни. По-четверте, участь поліції у розмінуванні має значний соціальний вимір. Поліцейські забезпечують інформування населення про небезпеку вибухонебезпечних предметів, проводять роз'яснювальну роботу, беруть участь у заходах із мінної безпеки, особливо в місцях компактного проживання дітей, літніх людей, внутрішньо переміщених осіб. Такі заходи суттєво знижують ризики нещасних випадків і формують належний рівень безпекової культури в суспільстві.

Участь поліції в оперативному розмінуванні є важливим компонентом забезпечення публічної безпеки, оскільки мінна небезпека тривалий час зберігає свій руйнівний потенціал і здатна спричиняти масові жертви та дестабілізувати життєдіяльність територій. У цьому контексті діяльність поліції спрямована не лише на ліквідацію конкретних загроз, але й на створення умов для відновлення нормального функціонування громад, повернення населення до деокупованих територій та відбудови інфраструктури.

Таким чином, діяльність Національної поліції України в умовах воєнного стану спрямована на комплексне забезпечення публічного порядку та безпеки населення. Поліція одночасно виступає інструментом реалізації державної політики безпеки та гарантом дотримання прав людини. Саме поєднання цих двох вимірів – безпекового та правозахисного – визначає специфіку її функціонування в умовах збройного конфлікту та формує

підґрунтя для відновлення довіри громадян до державних інституцій на звільнених територіях.

1.3. Забезпечення публічного порядку органами і підрозділами Державної прикордонної служби України

Забезпечення публічного порядку органами й підрозділами Державної прикордонної служби України (ДПСУ) є одним з ключових напрямів її діяльності, яка виступає невід'ємним елементом загальної системи національної безпеки та правоохоронної діяльності держави. Особливість забезпечення публічного порядку в зоні державного кордону полягає в тому, що ця територія є простором підвищеного ризику, де національні інтереси перетинаються з міжнародним правовим режимом, економічними процесами, транскордонною злочинністю, міграційними потоками, а також з актуальними загрозами державному суверенітету й територіальній цілісності. Відтак діяльність ДПСУ щодо охорони кордону та гарантування публічного порядку має комплексний, правоохоронний і превентивний характер.

Правову основу діяльності ДПСУ у сфері забезпечення публічного порядку становить Конституція України, яка у статті 17 визначає, що захист суверенітету та територіальної цілісності України є найважливішим обов'язком держави, а оборона держави та захист її кордонів належать до загальнодержавних пріоритетів. Стаття 92 Конституції України встановлює, що виключно закони України визначають організацію та діяльність органів і підрозділів, відповідальних за охорону громадської безпеки та правопорядку, а також засади застосування сили та зброї.¹ Відповідно до цих положень, законодавець визначив правовий статус ДПСУ як правоохоронного органу спеціального призначення.

Закон України «Про Державну прикордонну службу України» від 03 квітня 2003 року № 661-IV визначає завдання, принципи діяльності, повноваження, порядок організації та функціонування служби.

У статті 1 зазначено, що ДПСУ є правоохоронним органом спеціального призначення, на який покладаються забезпечення недоторканності державного кордону та охорона суверенних прав України в її виключній (морській) економічній зоні. Стаття 2 визначає, що діяльність ДПСУ спрямовується на забезпечення державної, національної, громадської та публічної безпеки. Стаття 19 цього Закону закріплює право особового складу застосовувати заходи фізичного впливу, спеціальні засоби та вогнепальну зброю для припинення правопорушень, захисту життя та здоров'я людей, в умовах необхідної оборони або крайньої необхідності. Даний нормативно-правовий порядок прямо створює правові передумови для

¹ Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <http://zakon.rada.gov.ua/laws/show/254к/96-ВР>

участі ДПСУ у підтриманні публічного порядку та забезпеченні безпеки у прикордонній сфері.¹

Важливою правовою передумовою діяльності ДПСУ щодо забезпечення публічного порядку є Закон України «Про державний кордон України», який визначає поняття державного кордону, режим державного кордону, прикордонний режим та режим у пунктах пропуску через державний кордон. У статті 20 Закону закріплено, що забезпечення режиму державного кордону покладається на органи ДПСУ, а стаття 23 встановлює право прикордонників затримувати осіб, які порушують прикордонні правила, і притягувати їх до відповідальності відповідно до закону. Додатково Закон надає право застосовувати підрозділи охорони кордону спільно з іншими органами, зокрема з Національною поліцією та Службою безпеки України, для забезпечення громадського порядку у прикордонних районах під час ускладнення оперативної обстановки.

Діяльність ДПСУ у сфері забезпечення публічного порядку має комплексний характер і передбачає реалізацію як правозастосовних, так і превентивних функцій.

До основних завдань прикордонних органів у забезпеченні публічного порядку належать:

- контроль за дотриманням режиму державного кордону;
- охорона прикордонного режиму;
- забезпечення режиму в пунктах пропуску через державний кордон;
- здійснення прикордонного контролю осіб, транспортних засобів і вантажів;
- запобігання та припинення незаконної міграції, торгівлі людьми, контрабанди, зокрема зброї, наркотичних засобів, культурних цінностей; затримання порушників;
- застосування заходів адміністративного та кримінального процесуального впливу; попередження масових порушень порядку; участь у забезпеченні оборони держави під час воєнного стану.

Специфіка діяльності ДПСУ щодо забезпечення публічного порядку найбільш очевидна у пунктах пропуску через державний кордон, які є місцями масового скупчення населення і транспортних потоків, де виникають конфліктні ситуації, пов'язані з пропускними процедурами, затримками або протиправними діями громадян. Саме у цих умовах прикордонники здійснюють комплекс профілактичних та режимних заходів, контролюють виконання правил переміщення осіб, а також регулюють поведінку громадян з метою недопущення порушень публічного порядку.

У пункті пропуску ДПСУ виконує і функції, пов'язані з протидією міжнародній злочинності. Оперативно-розшукова діяльність прикордонників, згідно зі статтею 12 Закону України «Про оперативно-розшукову діяльність»,

¹ Про державну прикордонну службу України: Закон України від 03.04.2003 № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15#Text>

включає виявлення осіб, які перебувають у розшуку, встановлення каналів незаконного переміщення товарів та зброї, участь у ліквідації злочинних груп.¹

Як слушно зазначає А. М. Притула, оперативно-розшукові відділи органів охорони державного кордону ДПСУ, будучи оперативними підрозділами, уповноваженими здійснювати оперативно-розшукову діяльність відповідно до Закону України «Про оперативно-розшукову діяльність» та Кримінального процесуального кодексу України, спрямовують свою діяльність на пошук і фіксацію фактичних даних про протиправні діяння, що посягають на безпеку громадян, суспільства і держави, тобто виконують функцію важливого інструменту забезпечення публічної безпеки в прикордонному просторі.²

У вітчизняній доктрині оперативно-розшукову діяльність, що здійснюється оперативними підрозділами ДПСУ, розглядають як один із ключових засобів запобігання тяжким та особливо тяжким злочинам у сфері громадської та державної безпеки, оскільки її завданням є своєчасне виявлення, припинення та документування протиправних діянь, небезпечних для публічної безпеки.³

Застосування прикордонниками заходів примусу і спеціальних засобів є регламентованим правом і здійснюється в порядку, визначеному Законом «Про Національну поліцію», на підставі статей 43–46, які застосовуються до ДПСУ як нормативні аналоги, за умови відсутності власних процедур.⁴

Нормативне регулювання порядку застосування сили підрозділами Державної прикордонної служби України є необхідною передумовою їх належного функціонування, оскільки прикордонні формування дедалі частіше діють в умовах, наближених до режиму спеціальних поліцейських операцій. При цьому законність діяльності ДПСУ прямо залежить від дотримання вимог адекватності та пропорційності застосування сили, адже саме ці критерії забезпечують реальну повагу до прав і свобод людини та мінімізують ризики їх необґрунтованого обмеження.⁵

Важливим напрямом забезпечення публічного порядку є взаємодія ДПСУ з іншими органами державної влади та суб'єктами сектору безпеки й оборони. У цьому контексті показовими є завдання, які виконує Національна поліція України у прифронтових та прикордонних регіонах. Як слушно зазначає О. В. Крижановська, поряд з основними функціями щодо охорони публічного порядку, протидії правопорушенням та забезпечення безпеки

¹ Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

² Притула А.М. Оперативно-розшукові відділи Державної прикордонної служби України : сутність та призначення. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 21. С. 95.

³ Кириченко О. В., Хмеленко В. В. Принципи оперативно-розшукового запобігання злочинам. Монографія / О. В. Кириченко, В. В. Хмеленко. Київ: Центр учбової літератури, 2020. С. 53.

⁴ Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: <http://zakon3.rada.gov.ua/laws/show/580-19>

⁵ Трофименко О.В., Ляшук Р.М., Вичавка В.І. Правове регулювання взаємодії Державної прикордонної служби України та суб'єктів сектору безпеки і оборони. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2024. № 70. С. 51.

дорожнього руху, поліцейські виконують також стабілізаційні й підтримувальні функції у прифронтових районах, залучаються до спеціальних операцій, забезпечують пропускний режим, здійснюють охорону об'єктів критичної інфраструктури, документують воєнні злочини тощо.¹

Узгоджені спільні дії ДПСУ та Національної поліції в таких умовах істотно посилюють спроможність держави забезпечувати публічний порядок, особливо в зонах підвищеного безпекового ризику.

Відповідно до статті 14 Закону України «Про Державну прикордонну службу України» ДПСУ у своїй діяльності взаємодіє зі Збройними Силами України, Національною поліцією, Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації, Державною митною службою та органами місцевого самоврядування. Така взаємодія включає проведення спільних заходів та операцій, обмін оперативною інформацією, узгодження дій у разі виникнення загроз публічному порядку, у тому числі під час масових заходів, ліквідації наслідків надзвичайних ситуацій, а також у період дії правового режиму воєнного стану.

Особливої актуальності діяльність ДПСУ щодо забезпечення публічного порядку набуває в умовах воєнного стану. Закон України «Про правовий режим воєнного стану» передбачає розширення повноважень військових формувань і правоохоронних органів, включаючи право обмежувати пересування громадян, встановлювати особливі пропускні режими, здійснювати огляд транспортних засобів, перевірку документів, вводити комендантську годину. ДПСУ в умовах воєнного стану бере участь у територіальній обороні, протидіє диверсійним групам, забезпечує безпеку прикордонної інфраструктури, здійснює контроль за рухом внутрішньо переміщених осіб і гуманітарних колон, запобігає провокаціям і панічним настроям серед населення у прикордонних регіонах.²

Підрозділи спеціального призначення ДПСУ, такі як «Омега», «Дозор», окремі підрозділи морської охорони та авіаційні підрозділи, виконують спеціальні завдання щодо нейтралізації загроз терористичного характеру та участі в операціях із забезпечення національної безпеки. Їх залучення до надзвичайних ситуацій із загрозою масових безпорядків, блокування пунктів пропуску або масового прориву через кордон свідчить про наближеність їх діяльності до функцій спеціальних підрозділів поліції.

Підтримання публічного порядку передбачає дотримання прав і свобод громадян. Стаття 5 Закону України «Про Державну прикордонну службу України» встановлює обов'язок прикордонників поважати честь і гідність осіб, не допускати дискримінації, забезпечувати можливість оскарження

¹ Крижановська О.В. Взаємодія Національної поліції з силами безпеки та оборони як основа правопорядку в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2025. № 7. С. 402.

² Про правовий режим воєнного стану : Закон України від 12.05.2015 № 1647-III. URL: <https://zakon.rada.gov.ua/laws/show/389-19>

рішень і дій посадових осіб у судовому порядку.¹ Це базується на принципі верховенства права, закріпленому у статті 8 Конституції України.²

Відповідно до європейських стандартів у діяльності прикордонних органів пріоритет має надаватися превентивним заходам порівняно із силовими методами, а функціонування цих органів повинно ґрунтуватися на принципах максимальної відкритості та забезпечення демократичного цивільного контролю.³

Водночас чинне законодавство має низку проблем і прогалин, які ускладнюють ефективне виконання функцій ДПСУ щодо забезпечення публічного порядку. У науковій літературі (А. В. Кубаєнко, О. В. Крижановська) обґрунтовується, що ефективне функціонування правоохоронних органів у сфері публічної безпеки потребує системного, а не фрагментарного оновлення нормативно-правового регулювання, посилення координації суб'єктів сектору безпеки та чіткого визначення їх місця і ролі у єдиній системі забезпечення прав і свобод людини.

На цій основі можна дійти висновку, що для ДПСУ як складової правоохоронної системи залишаються актуальними проблеми законодавчої інтеграції її діяльності в загальнодержавний механізм охорони публічної безпеки, уточнення спільних повноважень з іншими правоохоронними органами, а також удосконалення правового регулювання застосування примусових заходів.⁴

Недостатньо врегульованим залишається й питання взаємодії ДПСУ з громадськими формуваннями у сфері забезпечення публічного порядку, хоча участь громадян в охороні державного кордону прямо передбачена Законом України «Про участь громадян в охороні громадського порядку і державного кордону».⁵

Реформування Державної прикордонної служби України неможливе без комплексного перегляду чинної законодавчої бази.

Необхідність системного оновлення правового регулювання діяльності ДПСУ пов'язується з потребою кодифікації законодавства у сфері прикордонної безпеки, розроблення окремого закону про забезпечення публічної безпеки у прикордонних регіонах, запровадження єдиної доктрини прикордонної політики, стандартизації застосування заходів примусу та підвищення рівня професійної підготовки персоналу. Водночас акцент робиться на посиленні аналітичної складової управління, широкому впровадженні сучасних інформаційних технологій і технічних засобів

¹ Про державну прикордонну службу України: Закон України від 03.04.2003 № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15#Text>

² Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <http://zakon.rada.gov.ua/laws/show/254к/96-ВР>

³ Радченя Наталія. Європейські стандарти професійної підготовки прикордонників. *Visegrad Journal on Human Rights*. 2020. № 4. С. 104

⁴ Kubaenko A., Okhrimenko I., Kryzhanovska O. Modernization of the law enforcement system at the current stage of digital transformation. *Journal of Law and Political Sciences*, 2022. P. 386.

⁵ Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 № 1835-III. URL: <https://zakon.rada.gov.ua/laws/show/1835-14#Text>

контролю, що має відповідати актуальним викликам і загрозам національній безпеці.

Важливою складовою сучасного механізму забезпечення публічного порядку на державному кордоні є застосування Державною прикордонною службою України централізованих систем відеоспостереження та відеоаналітики. Їх функціонування регулюється Інструкцією про порядок використання автоматичної фото- і відеотехніки під час виконання службових обов'язків посадовими і службовими особами ДПСУ, яка встановлює єдиний порядок застосування цих засобів, правила обліку, зберігання та використання отриманої інформації.¹

Згідно з положеннями Інструкції автоматична фото- і відеотехніка використовується з метою запобігання, виявлення та фіксації правопорушень, а також забезпечення публічної безпеки і правопорядку у пунктах пропуску, КПВВ, контрольованих прикордонних районах та у межах виключної (морської) економічної зони України. Це підкреслює превентивний та доказовий характер її застосування і відображає сучасний підхід до правоохоронної діяльності, заснований на технологічних інструментах фіксації подій та захисту прав людини.

Інструкція встановлює вимоги до відкритості використання технічних засобів фіксації: уповноважені особи зобов'язані повідомляти громадян про здійснення відеозапису, а в пунктах пропуску розміщуються інформаційні таблички українською та англійською мовами («Увага! Здійснюється фото- і відеофіксація»). Такий підхід відповідає стандартам ЄС щодо транспарентності правоохоронних заходів і принципу захисту приватного життя, закріпленого у ст. 8 Конвенції про захист прав людини і основоположних свобод.²

Упорядкований механізм отримання, архівування та зберігання інформації докладно визначено у розділі IV Інструкції. Після завершення зміни всі відеоматеріали передаються відповідальним особам, копіюються у сховище фото- і відеоінформації, яке функціонує як централізований архів. Це забезпечує достовірність матеріалів та унеможливорює їх редагування або фальсифікацію, що є важливою процесуальною гарантією. Встановлений строк зберігання становить від 15 днів до 1 року, а в окремих випадках — до 3 років, якщо матеріали становлять суспільний інтерес або вимагаються для судового провадження.

¹ Про затвердження Інструкції про порядок використання автоматичної фото- і відеотехніки під час виконання службових обов'язків посадовими і службовими особами Державної прикордонної служби України: наказ Міністерства внутрішніх справ України від 04.04.2019 №244 (Зареєстровано в Міністерстві юстиції України 22 квітня 2019 р. за № 419/33390). URL: <https://zakon.rada.gov.ua/laws/show/z0419-19#Text>

² Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) від 04.11.1950 № 995_004. (Ратифіковано Законом № 475/97-ВР від 17.07.97) URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

Інструкція містить чіткі заборонні норми, які не допускають використання отриманих записів у приватних цілях, їх редагування, знищення чи поширення всупереч закону (розділ III, пункт 6).¹

Такий режим доступу узгоджується з вимогами Законів України «Про інформацію»,² «Про захист персональних даних»,³ «Про захист інформації в інформаційно-телекомунікаційних системах»⁴ і «Про доступ до публічної інформації»⁵.

Доступ до відеоматеріалів регламентований і можливий лише з метою запобігання чи розслідування правопорушень, а також на офіційні запити суду й правоохоронних органів. Це забезпечує баланс між публічною безпекою та правом особи на приватне життя.

На практичному рівні ДПСУ використовує розгалужену систему автоматизованого спостереження, що включає мережеві відеокамери різних типів, оптико-електронні та тепловізійні комплекси, мобільні відеореєстратори, повітряні та морські платформи, інтегровані у єдині інформаційні системи прикордонної безпеки. Такі рішення підвищують рівень оперативного реагування, спрощують доказування правопорушень, сприяють запобіганню незаконній міграції, контрабанді, транснаціональній злочинності.

Важливим є те, що системи відеоспостереження та відеоаналітики працюють не лише у режимі пасивної фіксації, а й забезпечують аналітичну обробку інформації в реальному часі, дозволяючи виявляти підозрілі дії, групові скупчення, спроби порушення кордону та інші ризикові фактори.

Одним із ключових напрямів цифрової трансформації діяльності Державної прикордонної служби України є впровадження та розвиток комплексних автоматизованих систем контролю та моніторингу, які дозволяють значно підвищити рівень оперативності управління, забезпечити ефективну протидію загрозам на кордоні та покращити механізм підтримання публічного порядку у прикордонному просторі.

Центральне місце серед таких рішень посідають автоматизована система прикордонного контролю ІТС «Гарт-1» та інтелектуальна система охорони державного кордону, що створюється як сучасний інтегрований технологічний комплекс спостереження та оперативного реагування.

Автоматизована система прикордонного контролю ІТС «Гарт-1» функціонує як елемент єдиної інформаційно-телекомунікаційної мережі

¹ Про затвердження Інструкції про порядок використання автоматичної фото- і відеотехніки під час виконання службових обов'язків посадовими і службовими особами Державної прикордонної служби України: наказ Міністерства внутрішніх справ України від 04.04.2019 №244 (Зареєстровано в Міністерстві юстиції України 22 квітня 2019 р. за № 419/33390). URL: <https://zakon.rada.gov.ua/laws/show/z0419-19#Text>

² Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

³ Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

⁴ Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

⁵ Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

ДПСУ і забезпечує обробку даних про осіб, транспортні засоби та вантажі, що перетинають державний кордон.¹ Її застосування сприяє скороченню часу проходження контрольних процедур, підвищує якість ідентифікаційних процесів, а також створює умови для автоматичного виявлення ризикових осіб і правопорушень.

Система інтегрується з іншими базами даних державного значення, зокрема:

- Єдиним державним демографічним реєстром;
- базами даних Національної поліції та Служби безпеки України;
- інформаційними ресурсами Інтерполу та Європолу;
- даними системи біометричної ідентифікації.

Це дозволяє своєчасно виявляти осіб, які перебувають у розшуку, застосовувати індивідуальні профілі ризику та проводити превентивні заходи щодо запобігання загрозам публічному порядку. У межах моніторингу публічної безпеки система використовується для аналізу тенденцій, фіксації нетипових маршрутів переміщення, виявлення групових переміщень та ознак можливої диверсійної діяльності.

Важливим етапом модернізації прикордонної інфраструктури стало затвердження Стратегії інтегрованого управління кордонами на період до 2025 року, схваленої розпорядженням Кабінету Міністрів України від 24 липня 2019 року № 687-р, якою було передбачено формування сучасної моделі охорони державного кордону на основі принципів європейських стандартів прикордонної безпеки, впровадження інноваційних технологій контролю та спостереження, посилення міжвідомчої взаємодії та створення умов для поступового переходу до концепції «розумного кордону».²

У документі чітко простежується курс на технологічну модернізацію прикордонної інфраструктури та створення **інтелектуальної системи охорони кордону**, що відповідає сучасним викликам національної безпеки, зростанню ризиків терористичної й диверсійної діяльності та необхідності оперативного управління загрозами.

Одним із ключових положень Стратегії є оперативне реагування на правопорушення на державному кордоні поза пунктами пропуску, яка безпосередньо орієнтована на модернізацію систем технічного спостереження та розгортання інтегрованих інтелектуальних комплексів контролю. Документом передбачено використання передових цифрових і сенсорних технологій, зокрема безпілотних літальних апаратів, оптико-електронних систем, радарних засобів, високочутливих сенсорів та автоматизованої аналітичної обробки інформації.

¹ Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю "Гарт-1" Державної прикордонної служби України: наказ Адміністрації ДПСУ від 30.09.2008 №810 Із змінами, внесеними згідно з Наказом Адміністрації Державної прикордонної служби № 750 (з0959-10) від 05.10.2010. <https://zakon.rada.gov.ua/laws/show/z1086-08#Text>

² Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року. Розпорядження Кабінету міністрів України від 24.07.2019 № 687-р. URL: <https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text>

Особливе місце у Стратегії займає необхідність створення суцільної технологічної зони спостереження уздовж державного кордону, що базується на розгортанні мережі ультракороткохвильового радіозв'язку, сучасних інформаційних систем та засобів відеоаналітики. Це положення відповідає вимогам щодо розбудови інтелектуальної системи охорони кордону, яка має функціонувати як багаторівнева система з високою інтеграцією даних та можливістю автоматизованого прогнозування загроз.

У контексті інтелектуального моніторингу Стратегія передбачає:

- впровадження автоматизованих систем виявлення та супроводження цілей;
- запровадження механізмів автоматизації аналізу ризиків та профілювання небезпечних категорій осіб і транспортних засобів;
- інтероперабельність інформаційних систем ДПСУ з Інтерполом, Європолем, FRONTEX;
- застосування сучасних ІТ-рішень, включаючи системи PNR/APIS та біометричний контроль;
- розвиток інфраструктури центрів управління обстановкою в реальному часі.

Ключовим елементом цифрової трансформації виступає створення інтегрованої системи автоматизованого управління кордоном і міграційними процесами, що забезпечує повний цикл від виявлення загрози до реагування.

У реалізації проекту також активно залучено інструменти міжнародно-технічної допомоги та партнерські ініціативи ЄС. Таким чином, Стратегія визначає створення інтелектуальної системи охорони кордону не лише як технічну модернізацію, але й як концептуальну зміну моделі прикордонної безпеки, що базується на аналітичних, цифрових та мережевих технологіях, інтеграції міжвідомчих інформаційних ресурсів і міжнародній співпраці.

Інтелектуальна система охорони кордону, передбачена Стратегією, є ключовим елементом реформування ДПСУ та критичною умовою забезпечення публічної безпеки. Її реалізація дозволить створити суцільну технологічну лінію контролю, підвищити швидкість прийняття рішень, знизити ризики протиправної діяльності та забезпечити виконання завдань України як майбутнього члена Європейського Союзу щодо охорони зовнішніх кордонів ЄС.

Розгортання системи розпочалося на найбільш загрозливих ділянках північного кордону України, з урахуванням нових воєнних викликів. Використання цієї технології дозволяє мінімізувати людський фактор, підвищити силову спроможність підрозділів, скоротити час реагування, сформувати більш точну картину оперативної обстановки.

Використання «Гарт-1» та елементів Інтелектуальної системи охорони кордону сприяє:

- підвищенню прозорості та контрольованості правоохоронної діяльності;
- зменшенню корупційних ризиків у пунктах пропуску;
- зміцненню доказової бази щодо правопорушень;

- раціональному використанню сил і засобів ДПСУ;
- покращенню взаємодії з іншими суб'єктами сектору безпеки;
- підвищенню рівня довіри суспільства до прикордонної служби.

Сучасні технічні засоби перетворюють ДПСУ на інтегрований елемент загальноєвропейської моделі управління кордонами, що відповідає стандартам FRONTEX та вимогам євроатлантичної інтеграції України.

Впровадження автоматизованих систем відеоспостереження та аналітичної обробки даних є стратегічним напрямом розвитку ДПСУ, що суттєво підсилює її роль у забезпеченні публічного порядку, протидії злочинності та захисті державного суверенітету, особливо в умовах триваючої збройної агресії.

Таким чином, застосування автоматичної фото- і відеотехніки в діяльності ДПСУ є сучасним технологічним інструментом забезпечення публічного порядку й безпеки на державному кордоні. Нормативне врегулювання порядку її використання створює правові гарантії прозорості діяльності прикордонних підрозділів, підвищує рівень довіри суспільства, мінімізує конфліктні ситуації та забезпечує надійний доказовий матеріал у провадженнях щодо адміністративних і кримінальних правопорушень. Завдяки розвитку інформаційних систем і централізованих платформ моніторингу ДПСУ реалізує превентивну функцію в умовах складної безпекової ситуації та зростаючих загроз національній безпеці.

Підсумовуючи викладене, необхідно зазначити, що забезпечення публічного порядку органами та підрозділами ДПСУ є багатофункціональною діяльністю, яка поєднує охоронні, превентивні, правоохоронні, оперативно-розшукові та оборонні елементи.

ДПСУ є одним із ключових суб'єктів національної системи безпеки, а підтримання публічного порядку в прикордонному просторі становить важливу передумову захисту національних інтересів, забезпечення суспільної стабільності та збереження територіальної цілісності України.

Ефективна діяльність прикордонних органів, їх конструктивна взаємодія з населенням, органами державної влади та іншими суб'єктами сектору безпеки й оборони є необхідною умовою функціонування демократичної, правової та суверенної держави.

Отже, органи й підрозділи Державної прикордонної служби України відіграють провідну роль у забезпеченні публічного порядку на державному кордоні, де цей порядок нерозривно пов'язаний із дотриманням прикордонного режиму, гарантуванням міграційної та воєнної безпеки, протидією транснаціональній злочинності та захистом суверенітету держави, що набуває особливої ваги в умовах триваючої збройної агресії проти України.

Контрольні питання до розділу I

1. Поняття публічного порядку. роль публічного порядку у функціонуванні та розвитку сучасного суспільства.
2. Роль Національної поліції України у забезпеченні публічного порядку.
3. Забезпечення публічного порядку органами та підрозділами Національної поліції України під час дії правового режиму воєнного стану.
4. У чому полягає правовий статус Державної прикордонної служби України як правоохоронного органу спеціального призначення?
5. Перелічіть та охарактеризуйте основні нормативно-правові акти, що регулюють участь Державної прикордонної служби України у забезпеченні публічного порядку в прикордонних районах.
6. У чому виявляється специфіка забезпечення публічного порядку в пунктах пропуску через державний кордон України?
7. Дайте характеристику повноваженням прикордонників щодо здійснення прикордонного контролю та патрулювання в цілях підтримання публічного порядку.

II. АНАЛІЗ СУЧАСНОГО СТАНУ ПОБУДОВИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЯМИ ВІДЕОАНАЛІТИКИ: ІСТОРИЧНИЙ АСПЕКТ

Системи відеоспостереження використовуються в різних сферах діяльності людини – від забезпечення охорони конкретних об'єктів до контролю технологічних процесів, біометричної ідентифікації, а також інтелектуального пошуку об'єктів у відеоархівах тощо.

Відеоспостереження (Closed-circuit television, CCTV) – це система передачі інформації з відеокамер на обмежену кількість моніторів або пристроїв для запису.

Державні стандарти України, які регулюють застосування систем відеоспостереження, узгоджені з європейськими нормами. Згідно з Наказом ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 31 липня 2017 року № 201, що стосується прийняття національних нормативних документів та їх гармонізації з європейськими й міжнародними стандартами, застосування охоронних систем відеоспостереження регламентують такі стандарти: ДСТУ EN 62676-3:2017 (ідентичний EN 62676-3:2015), ДСТУ EN 62676-4:2017 (ідентичний EN 62676-4:2015) та ДСТУ EN 62676-1-2:2014/Поправка №1:2017 (ідентичний EN 62676-1-2:2014/AC:2015).

При вивченні цих нормативних документів виявлено протиріччя у термінології, які потребують подальшого вивчення.

Деякі автори тлумачать аббревіатуру CCTV (укр. – Система замкнутого телебачення) як телевізійну систему, сигнали якої доступні тільки обмеженому колу користувачів, та дають класифікацію таким системам: замкнуті, квазізамкнуті та відкриті системи.

В даній роботі під системою відеоспостереження пропонується розуміти програмно-технічний комплекс, призначений для організації відеоконтролю на визначених об'єктах, які можуть бути розташовані в локальних місцях зосередження так і територіально-розподіленими. Основними компонентами системи відеоспостереження є:

- пристрої формування відеосигналу;
- канали передачі відеосигналів від пристроїв формування відеосигналів до пристроїв зберігання та обробки відеосигналів;
- пристрої зберігання та обробки відеосигналів
- канали передачі даних від пристроїв зберігання та обробки відеосигналів до пристроїв відображення відеоінформації;
- пристроїв відображення відеоінформації.

Система відеоспостереження може мати різний рівень складності: від найпростішої, що включає одну камеру та монітор для відображення отриманого зображення, до розгалуженої мережі з багатьох територіально розподілених камер, об'єднаних телекомунікаційною інфраструктурою і доповнених системами зберігання та аналізу відеоданих.

Головними завданнями сучасних систем відеоспостереження є:

- моніторинг та оцінка ситуації на визначених об'єктах;

- виявлення несанкціонованих дій та позаштатних ситуацій;
- розпізнавання об'єктів та дій;
- ідентифікація об'єктів;
- прогнозування кризових ситуацій;
- ведення архіву записаної відеоінформації;
- аналіз записаної відеоінформації про події що відбулися в секторах камер спостереження та ін.

Перелік завдань, які можуть покладатися на системи відеоспостереження, має умовний характер, оскільки для кожної конкретної системи визначаються власні цілі та функції ще на етапі її проектування. При цьому додатково враховується низка критеріїв, серед яких: загальні технічні вимоги до системи, характеристика об'єкта, на якому планується встановлення, вимоги щодо безпеки (пожежної, електробезпеки, заземлення тощо), вплив зовнішніх чинників (кліматичних, механічних та інших), умови експлуатації, показники надійності майбутньої системи, особливості технічного обслуговування й ремонту, а також потенціал подальшої модернізації. Одним із ключових аспектів, що значною мірою впливає на прийняття рішень, є бюджет проекту.

Цікаво, що витoki систем відеоспостереження пов'язані не стільки з розвитком телевізійних технологій, скільки з удосконаленням фототехніки. Так, у 1913 році в адміністрації в'язниці Холлоуей (США) застосовували метод так званого «фотографічного спостереження». Охоронці здійснювали приховане фотографування ув'язнених з великої відстані. Необхідність такого підходу виникла через відмову вісімнадцяти затриманих політичних активісток погодитися на фотографування для формування досьє. Кожного разу, коли їх намагалися сфотографувати, вони ховали обличчя руками, рухалися або навмисно спотворювали міміку. Таких активісток називали суфражистками (рис. 1.1). Отримані у такий спосіб фотознімки використовувалися для подальшої ідентифікації цих осіб.



Рисунок 1.1 – Фотографії суфражисток

2.1. Витоки розвитку систем відеоспостереження (1930 – 1950-ті роки)

Зародження систем відеоспостереження безпосередньо пов'язане з розвитком телебачення у першій половині XX століття. У 1930-х роках у Німеччині та США проводилися перші експерименти з передачею відеосигналу на обмежену відстань. Зокрема, компанії Telefunken у Німеччині та RCA (Radio Corporation of America) у США випробовували можливості телевізійних камер не лише для публічної трансляції, але й для технічного контролю у промисловості та на транспорті. Це стало передумовою формування концепції замкненого телебачення (CCTV), де сигнал передавався у закритому контурі для вузького кола користувачів (Natarajan, 2016).

Першою задокументованою промисловою системою CCTV вважається розробка компанії Siemens AG у 1942 році. Під керівництвом інженера Вальтера Бруха було створено систему відеоспостереження для моніторингу запусків балістичних ракет V-2 на полігоні Пенемюнде (McCahill & Norris, 2002). Такий підхід забезпечував безпечний віддалений контроль за процесом запуску, оскільки перебування персоналу поблизу пускових установок було небезпечним. Використання телевізійних технологій у військовій сфері заклало фундамент для подальшого розвитку систем безпеки.

У 1942 році німецький інженер Вальтер Брюх уперше реалізував систему відеоспостереження для компанії Siemens на ракетному випробувальному полігоні в Пенемюнде (Німеччина). Ця система була призначена для дистанційного спостереження за процесом запуску ракет «Фау-2» та фіксації можливих технічних несправностей.

У 1949 році в США з'явилася перша комерційна система CCTV під торговельною маркою Vericon. Вона призначалася для банків, військових об'єктів та стратегічних підприємств. Хоча система не мала можливості запису, її функціонал дозволяв здійснювати моніторинг у реальному часі, що значно підвищувало рівень контролю (Welsh & Farrington, 2009). Саме Vericon стала першою спробою комерційного впровадження відеоспостереження у цивільній сфері, започаткувавши розвиток цього ринку.

У 1949 році в США з'явилася перша комерційна система CCTV під торговельною маркою Vericon. Вона призначалася для банків, військових об'єктів та стратегічних підприємств. Хоча система не мала можливості запису, її функціонал дозволяв здійснювати моніторинг у реальному часі, що значно підвищувало рівень контролю (Welsh & Farrington, 2009). Саме Vericon стала першою спробою комерційного впровадження відеоспостереження у цивільній сфері, започаткувавши розвиток цього ринку.

У 1952 році поліція Гамбурга здійснила тестування вуличної системи відеоспостереження «Zauberspiegel» («чарівне дзеркало»). Завдяки цій системі оператор міг спостерігати на моніторі за рухом транспортних засобів і, за потреби, дистанційно керувати світлофорами. Починаючи з 1959 року, у містах Ганновер і Мюнхен відеоспостереження почали застосовувати для регулювання та контролю вуличного трафіку.

1930–1950-ті роки стали початком еволюції відеоспостереження, коли з'явилися перші практичні приклади: експериментальні технології на базі телевізійних систем, військові проекти (Siemens AG, 1942), перші комерційні рішення для цивільних об'єктів (Vericon, 1949). Цей період заклав основу подальшого розвитку CCTV як окремої галузі, спочатку орієнтованої на безпеку та контроль у критичних сферах.

Таким чином, період 1930–1950-х років можна вважати етапом становлення відеоспостереження як окремої галузі, що еволюціонувала від експериментальних телевізійних технологій до практичних рішень для військових та цивільних потреб.

2.2. Розвиток аналогових CCTV-систем (1960 – 1970-ті роки)

У 1960–1970-х роках відбувається активний розвиток аналогових систем відеоспостереження, що зумовлено технічним прогресом у галузі телевізійної техніки та зростанням потреби у забезпеченні безпеки в публічних і приватних просторах. У цей період домінує чорно-біла трубкова технологія камер, яка хоча й забезпечувала відносно низьку якість зображення, але була достатньою для вирішення завдань спостереження (Goold, 2004).

Системи CCTV набули поширення у банках, магазинах, казино, аеропортах та місцях позбавлення волі, де контроль за відвідувачами та персоналом був критично важливим (McCahill & Norris, 2002). У 1960-х роках відеоспостереження починає активно застосовуватися і у міському середовищі: поліція та муніципалітети використовували його як інструмент превенції злочинності та моніторингу громадського порядку. Одними з перших відомих прикладів стали системи у Лондоні та Нью-Йорку, де камери встановлювалися у публічних просторах і транспортних вузлах (Welsh & Farrington, 2009).

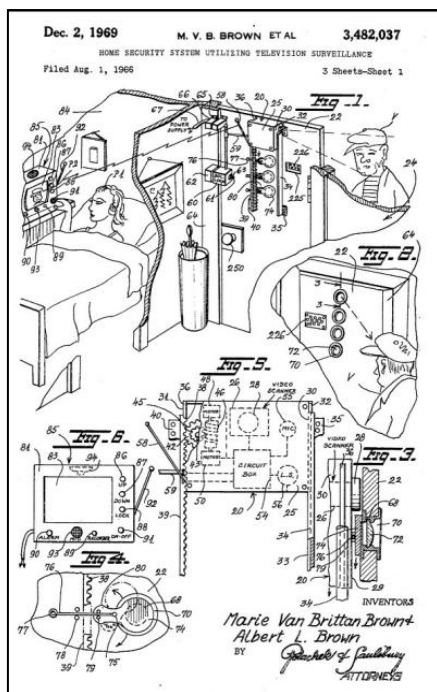
У 1960 році поліція Франкфурта-на-Майні вперше застосувала систему відеоспостереження, здатну автоматично фіксувати порушення правил дорожнього руху на світлофорах шляхом фотографування. Того ж року лондонська поліція встановила дві камери для спостереження за офіційним візитом королівської сім'ї Таїланду. Згодом ці ж камери були використані для контролю за масовими урочистостями під час святкування «Дня Гая Фокса». У 1961 році в Лондоні систему відеоспостереження розгорнули на території залізничного вокзалу, а у 1964 році поліція міста застосувала чотири камери для прихованого нагляду за великим скупченням людей у центральній частині міста.

У 1965 році Британська залізнична компанія запровадила використання відеокамер для контролю територій, що неодноразово ставали об'єктами вандалських дій.

У 1967 році британська компанія «Photo-Scan» уперше вивела на ринок комерційні системи відеоспостереження, основним призначенням яких було попередження магазинних крадіжок.

У 1968 році в місті Олін (США) була розгорнута система відеоспостереження, що складалася з восьми камер і використовувалась для охорони складських приміщень. На її проектування та встановлення було витрачено приблизно 1,4 мільйона доларів США. Камери були оснащені поворотними механізмами, завдяки чому їх поля огляду включали також частину прилеглих міських вулиць.

У 1969 році Мері Ван Браун разом із чоловіком Альбертом Брауном отримали патент на домашню систему безпеки. Конструкція включала чотири оглядові отвори та камеру, яка могла переміщуватися між ними. Крім того, система була оснащена механізмом дистанційного відкривання дверного замка. Фактично це стало раннім прототипом сучасного відеодомофона (рис. 1.2).



У 1968–1969 роках здійснювалися й інші спроби впровадження систем відеоспостереження з метою підвищення громадської безпеки, однак такі комплекси забезпечували лише перегляд трансляції з камер у реальному часі. Можливість відеозапису була обмежена: його виконували вручну, виключно за командою оператора.

Подальший етап розвитку цієї галузі настав у середині 1970-х років із появою відеомагнітофонів, що дозволяли записувати інформацію на магнітну плівку. Сама технологія магнітного запису була відома задовго до цього: уже в середині 1930-х років, зокрема у 1935 році, компанія AEG представила перший комерційний магнітофон. Спроби адаптувати концепцію запису аудіоінформації для фіксації відеосигналів здійснювалися ще у 1950-х роках, коли з'явилися перші пристрої з великими бобінами та швидкістю руху магнітної стрічки близько 1000 см/с. Для запису лише однієї години відео потрібна була стрічка довжиною приблизно 11 000 метрів.

Наприкінці 1970-х років компанія Sony запропонувала стандарт U-matic, який замість бобін передбачав використання касет і базувався на більш прогресивній технології читання інформації зі стрічки – так званому «спіральному скануванні». У 1972 році фірма Philips представила перший побутовий відеомагнітофон N1500 (стандарт System 2000). Паралельно

компанії Matsushita та JVC вийшли на ринок зі своїми пристроями, що використовували стандарт VHS (Video Home System), а Sony просувала альтернативний стандарт Beta. Після тривалої конкурентної боротьби саме система VHS здобула найбільшу популярність серед споживачів та закріпилася як домінуюча технологія запису відео.

З появою нових технологічних рішень стало можливим здійснювати безперервний запис і перегляд відеосигналу з камер спостереження. Водночас такі системи мали суттєві недоліки: зображення залишалося чорно-білим, а його якість була доволі низькою.

Наприкінці 1980-х років відбувся черговий важливий етап розвитку відеоспостереження, пов'язаний із упровадженням у камери ПЗЗ-матриць (пристроїв із зарядовим зв'язком, англ. CCD – charge coupled device). Принцип їх роботи полягає у фотоелектронному перетворенні: у сенсори генеруються електрони у кількості, пропорційній інтенсивності світла, що потрапляє на світлочутливу область. Саме це дозволило отримати значно якісніше зображення та забезпечило подальший прогрес у розвитку технологій відеофіксації.

Важливим етапом розвитку стало впровадження у 1970-х роках відеомагнітофонів (VCR), що дало змогу не лише спостерігати у реальному часі, а й зберігати відео для подальшого аналізу (Natarajan, 2016). Це розширило функціональні можливості CCTV, оскільки правоохоронні органи та служби безпеки отримали інструмент для доказової бази у кримінальних справах і внутрішніх розслідуваннях.

Таким чином, 1960–1970-ті роки стали періодом інституціоналізації CCTV: від простих технічних експериментів системи відеоспостереження перетворюються на масовий інструмент контролю у сфері безпеки, заклавши основу для подальшого переходу до цифрових технологій.

2.3. Перехід до цифрових технологій (1980 – 1990-ті роки)

1980–1990-ті роки стали переломним етапом у розвитку систем відеоспостереження, оскільки в цей час відбувся перехід від простих аналогових рішень до цифрових технологій. У цей період з'являються кольорові камери, що значно підвищило якість спостереження, удосконалюються системи зуму, нічного бачення (інфрачервоні підсвітки), поширення цифрових відеомагнітофонів (DVR) замість касетних VCR, Відеоспостереження інтегрується в охоронні системи (сигналізація, контроль доступу), масове розгортання у великих містах (Лондон, Нью-Йорк та інші).

Насамперед слід відзначити появу кольорових відеокамер, які поступово замінили чорно-білі аналоги та забезпечили значно вищу якість спостереження (McCahill & Norris, 2002). Це дало змогу ефективніше ідентифікувати об'єкти та осіб у різних умовах освітлення.

Важливим кроком стало вдосконалення систем оптичного та цифрового зуму, а також запровадження інфрачервоного підсвічування, що зробило можливим цілодобове спостереження (Natarajan, 2016). Такі

інновації значно розширили сферу застосування CCTV – від банків і підприємств до транспортних вузлів та громадських просторів.

Суттєвим технологічним зрушенням стало поширення цифрових відеомагнітофонів (DVR), які поступово витіснили касетні VCR. DVR дозволяли вести довготривалі записи без втрати якості, здійснювати швидкий пошук за часовими мітками, а також зберігати архівні матеріали у цифровому форматі (Welsh & Farrington, 2009).

У цей період системи відеоспостереження починають активно інтегруватися з іншими охоронними комплексами, зокрема сигналізацією та системами контролю доступу. Така інтеграція формувала основу для сучасних систем безпеки, які поєднують різні рівні захисту.

Особливо показовим стало масове розгортання CCTV у великих містах. Наприклад, у Лондоні наприкінці 1980-х було встановлено тисячі камер у громадських місцях, що зробило місто одним із світових лідерів за масштабами відеоспостереження (Norris & Armstrong, 1999). Подібні процеси відбувалися у Нью-Йорку та Москві, де системи CCTV розглядалися як інструмент боротьби зі злочинністю та засіб підвищення громадської безпеки.

У 1990-х роках у системах відеоспостереження почали впроваджувати матриці на основі КМОН (комплементарних металооксидних напівпровідників, англ. CMOS). Головними перевагами КМОН-матриць є значно менше енергоспоживання та нижча вартість виробництва порівняно з ПЗЗ (CCD) матрицями.

У середині 1990-х років почали з'являтися системи відеоспостереження, що працювали на основі цифрових відеореєстраторів DVR (Digital Video Recorder). Такі пристрої забезпечували можливість запису відеоінформації безпосередньо на жорсткий диск, що стало суттєвим кроком уперед порівняно з попередніми аналоговими технологіями.

У 1998 році в Лондоні була розгорнута система відеоспостереження, що включала технологію розпізнавання облич. Наприкінці 1990-х років використання цифрових відеореєстраторів із вбудованим інтерфейсом TCP/IP створило принципово нові можливості для формування розподілених систем відеоспостереження. Згодом на ринку з'явилися камери із вбудованим відеосервером і мережевим інтерфейсом – так звані IP-камери. Запровадження мережевих технологій стало черговим важливим етапом розвитку відеоспостереження, оскільки розширило його функціональні можливості: від звичайного інструмента моніторингу до комплексної системи, здатної здійснювати виявлення, розпізнавання образів та проведення відеоаналітики.

Таким чином, у 1980–1990-х роках відеоспостереження перейшло на новий якісний рівень: кольорове зображення, нічне бачення, цифровий запис і інтеграція з іншими технологіями заклали основу сучасних інтелектуальних систем безпеки.

2.4. IP-відеоспостереження (2000-ні роки)

У цей період мережеві IP-камери замінили аналогові, дозволяючи передавати відео через Інтернет, з'являється віддалений доступ – оператор міг спостерігати з будь-якого місця, використання компресії (H.264, MPEG-4) зменшило обсяг даних, відбувається інтеграція з комп'ютерними мережами, поява централізованих систем управління (VMS), поширення камер у громадських місцях для профілактики тероризму після 11 вересня 2001 року.

Початок XXI століття ознаменувався переходом від аналогових до цифрових технологій у сфері відеоспостереження. Ключовою подією стало впровадження мережевих IP-камер, які поступово замінили традиційні аналогові системи CCTV. На відміну від попередніх рішень, IP-камери передавали відеосигнал у цифровому вигляді через комп'ютерні мережі, що забезпечувало значно ширші можливості для зберігання та обробки інформації (Zhang, 2010).

Однією з головних переваг IP-технологій став віддалений доступ: оператор отримав можливість спостерігати за об'єктом із будь-якої точки світу, маючи підключення до Інтернету. Це суттєво розширило сферу використання систем відеоспостереження у бізнесі, транспортній інфраструктурі та правоохоронній діяльності (Gouda & Du, 2013).

Ще одним важливим кроком стала поява нових стандартів відеокompresії (MPEG-4, H.264), які дозволили суттєво зменшити обсяг переданих даних без втрати якості. Це забезпечило ефективніше використання мережевих ресурсів і зробило можливим створення систем із великою кількістю камер (Cheung & Kamath, 2004).

У цей період відбувається інтеграція відеоспостереження з комп'ютерними мережами та поява централізованих систем управління відео (VMS – Video Management Systems), що дозволяло адміністраторам контролювати великі комплекси камер, організовувати архіви відео та здійснювати пошук записів за параметрами.

Особливе значення IP-відеоспостереження набуло після терактів 11 вересня 2001 року, коли держави та приватні організації почали масово інвестувати у системи моніторингу громадських місць для підвищення рівня безпеки та профілактики терористичних загроз (Norris & Armstrong, 2007).

У 2010-х роках у сфері відеоспостереження почали активно впроваджувати «хмарні технології». Їх популярність була зумовлена низкою переваг: простотою розгортання, мінімальними вимогами до налаштування, можливістю доступу до відеозаписів з будь-якої точки світу та підвищеною надійністю зберігання даних на віддалених хмарних серверах. Саме ці фактори зробили хмарні рішення важливим етапом подальшого розвитку систем відеоспостереження.

Таким чином, 2000-ті роки стали етапом становлення цифрових мережевих систем відеоспостереження, які створили основу для подальшої інтеграції з аналітичними алгоритмами та штучним інтелектом.

2.5. Інтелектуальні системи (2010-ті – сьогодення)

Характерними ознаками цього періоду є: застосування відеоаналітики автоматичного розпізнавання номерів авто, облич, підозрілої поведінки; використання штучного інтелекту та машинного навчання для прогнозування інцидентів; поширення хмарних технологій для зберігання та аналізу відео; висока роздільна здатність (Full HD, 4K і навіть 8K); інтеграція з «розумними містами» та системами IoT; зростання ролі біометрії у системах безпеки.

Починаючи з 2010-х років системи відеоспостереження зазнали кардинальних змін, пов'язаних із впровадженням інтелектуальних технологій. Однією з ключових тенденцій стала відеоаналітика, яка дозволяє автоматично здійснювати розпізнавання номерних знаків транспортних засобів, ідентифікацію облич та виявлення підозрілої поведінки. Це зменшує навантаження на операторів і забезпечує своєчасне реагування на потенційні загрози (Zhang et al., 2019).

Важливим кроком стало застосування штучного інтелекту (AI) та машинного навчання, що забезпечує можливість прогнозування інцидентів на основі аналізу патернів поведінки людей і транспортних потоків. Такі рішення активно використовуються у сферах громадської безпеки, транспорту та торгівлі (Feng et al., 2020).

Не менш значущим фактором є поширення хмарних технологій, які забезпечують зберігання та обробку великих обсягів відеоінформації. Використання хмарних платформ дозволяє реалізувати віддалений доступ, масштабованість та гнучкість систем, що особливо важливо для великих міських інфраструктур (Rahman et al., 2018).

Технічний прогрес призвів до переходу на відео високої роздільної здатності – від Full HD до 4K і 8K, що дозволяє отримувати детальне зображення та підвищує ефективність автоматизованого аналізу. Паралельно відбувається інтеграція відеоспостереження у концепцію «розумних міст» та Інтернету речей (IoT), де камери стають частиною єдиної мережевої екосистеми управління міськими процесами (Khan et al., 2020).

Важливою тенденцією також є зростання ролі біометричних технологій. Сучасні системи поєднують відеоаналітику з біометричними методами ідентифікації (розпізнавання облич, райдужної оболонки, поведінкової біометрії), що значно розширює можливості безпеки як у публічному, так і в корпоративному середовищі (Li & Jain, 2019).

Таким чином, інтелектуальні системи відеоспостереження перетворилися із засобу пасивної фіксації подій на активний інструмент аналізу, прогнозування та управління ризиками, що визначає їх ключову роль у сучасній безпековій інфраструктурі.

2.6. Тенденції майбутнього розвитку систем відеоспостереження

Сучасні системи відеоспостереження швидко розвиваються у напрямку інтеграції з інтелектуальними технологіями, що дозволяє не лише фіксувати події, а й забезпечувати превентивну безпеку (табл. 1.1).

Таблиця 1.1

Зведена таблиця «Тенденції майбутнього у відеоспостереженні»

Напрямок розвитку	Приклад застосування	Значення для майбутнього
Інтеграція штучного інтелекту	Розпізнавання обличчя, поведінкова аналітика	Підвищення точності виявлення загроз, зменшення людського фактору
Хмарні технології	Зберігання відео у хмарних сервісах, доступ з будь-якої точки	Масштабованість, зниження витрат на інфраструктуру
Інтернет речей (IoT)	Смарт-камери, що взаємодіють із сенсорами та системами сигналізації	Створення комплексних систем «розумного міста»
Кібербезпека відеоданих	Шифрування відеопотоку, захист від атак	Забезпечення конфіденційності та цілісності даних
Аналітика великих даних	Аналіз потоків із тисяч камер у реальному часі	Прогнозування інцидентів, підтримка прийняття рішень
Мобільні рішення	Перегляд камер через смартфони, керування на відстані	Зручність доступу, оперативність реагування
Автоматизація управління	Автономні системи сповіщення про загрози	Швидкість реагування без участі людини
Етичні та правові стандарти	Регламентація використання розпізнавання облич	Баланс між безпекою та захистом приватності

Зведена таблиця демонструє, що майбутнє систем відеоспостереження визначатиметься комплексним поєднанням технологічних та соціальних факторів. Технічні напрями, такі як інтеграція штучного інтелекту, хмарні рішення, аналітика великих даних і автоматизація управління, забезпечують якісно новий рівень ефективності, дозволяючи не лише фіксувати події, а й передбачати потенційні загрози. Паралельно з цим зростає значення кібербезпеки та правового регулювання, адже підвищення інтелектуалізації

систем неминуче супроводжується ризиками витоку персональних даних і порушенням приватності. Таким чином, розвиток відеоспостереження буде відбуватися у двох взаємопов'язаних площинах: технічній (інноваційні рішення) та етичній (суспільний контроль і правове забезпечення).

Одним із ключових напрямів є інтеграція з нейромережами та алгоритмами штучного інтелекту. Це забезпечує автономне виявлення загроз, автоматичне розпізнавання підозрілої поведінки чи об'єктів без участі оператора. Такі рішення вже застосовуються у сфері «розумних міст» та транспортних хабах, де потрібна висока швидкість реагування (Redmon et al., 2016).

Другим важливим вектором є використання 360° панорамних камер та безпілотних літальних апаратів (дронів) для розширення можливостей моніторингу. Панорамні камери дозволяють отримати цілісну картину без «сліпих зон», а дрони забезпечують мобільність та застосовуються для спостереження у важкодоступних місцях, а також у сфері охорони кордонів та під час надзвичайних ситуацій (Khan et al., 2020).

Розвиток предиктивної аналітики стає одним із головних викликів майбутнього. Системи відеоспостереження переходять від пасивного запису та фіксації подій до прогнозування небезпечних ситуацій. Завдяки машинному навчанню такі рішення дозволяють визначати потенційні інциденти до того, як вони відбудуться, що особливо важливо для запобігання терористичним атакам або масовим заворушенням (Wang et al., 2021).

Особливої уваги потребує питання кіберзахисту систем відеоспостереження. Оскільки сучасні IP-камери фактично є повноцінними елементами комп'ютерних мереж, вони виступають потенційними цілями для хакерських атак. Дослідження підтверджують, що вразливості у прошивках та недостатньо надійні механізми автентифікації можуть бути використані для несанкціонованого перегляду відеопотоків або навіть для формування ботнет-мереж (Kolias et al., 2017). Тому подальший розвиток технологій відеоспостереження неможливий без комплексного впровадження кіберзахисних рішень на всіх рівнях – від окремих пристроїв до хмарних інфраструктур.

Узагальнені історичні відомості розвитку систем відеоспостереження наведено у табл. 1.2.

Таблиця 1.2

Зведені історичні відомості розвитку систем відеоспостереження

Період	Ключові події	Особливості
1930–1950-ті	1942 – Siemens AG створила систему спостереження за пусками ракет V-2 (Німеччина). 1949 – у США з'явилася перша комерційна система Vericon.	Перші CCTV-системи, передача відео у реальному часі без запису.
1960–1970-ті	Використання у банках, аеропортах, магазинах, тюрмах. 1970-ті – з'явився запис на відеомагнітофони (VCR).	Масове впровадження у сфері безпеки; чорно-білі камери; можливість зберігати відео.
1980–1990-ті	Кольорові камери. Інфрачервоне підсвічування, зум. Перехід на цифрові відеомагнітофони (DVR).	Покращення якості відео; інтеграція з охоронними системами; масове встановлення у містах.
2000-ті	Поява IP-камер. Відео через Інтернет, віддалений доступ. Компресія H.264, MPEG-4. Активне розгортання після 2001 року.	Перехід до цифрових мережевих систем; централізоване управління; доступ із будь-якої точки світу.
2010-ті – сьогодні	Відеоаналітика: розпізнавання облич, номерів, поведінки. Штучний інтелект і машинне навчання. Хмарні сервіси; відео у HD, 4K, 8K. Інтеграція з IoT та «розумними містами».	Інтелектуальні системи; використання біометрії; автоматичне виявлення загроз.
Майбутнє	Використання дронів і 360°-камер. Предиктивна аналітика. Інтеграція з нейромережами. Посилення кіберзахисту.	Автономні системи, що прогнозують небезпеку; комплексна інтеграція у міську та військову інфраструктуру.

Отже, майбутнє відеоспостереження визначається поєднанням інтелектуальних алгоритмів, мобільних платформ, предиктивних аналітичних

систем та надійного кіберзахисту, що дозволить зробити системи безпеки більш ефективними, автономними та стійкими до загроз.

Контрольні питання до розділу II

1. Які основні етапи розвитку системи відеоспостереження від 1930-х років до сьогодення?
2. Що таке ССТV і які основні стандарти регламентують його застосування в Україні?
3. Які технології використовуються в сучасних системах відеоспостереження для обробки відеоданих?
4. Які основні технічні проблеми виникають при побудові інтелектуальних систем відеонагляду?
5. Що таке ІР-відеоспостереження та які переваги має ця технологія?
6. Як відбувається перехід від аналогових до цифрових систем відеоспостереження?
7. Що таке відеоаналітика і які її основні функції?
8. Які тенденції розвитку системи відеоспостереження можна відзначити для майбутнього?
9. Як міжнародний досвід впливає на побудову системи відеонагляду в Україні?
10. Які сучасні архітектурні моделі системи відеонагляду зображення?
11. Що таке хмарна та туманна архітектура системи відеоспостереження?
12. Як нові технології, такі як AI і машинне навчання, змінюють функціональну систему відеоспостереження?

III. ТЕХНОЛОГІЧНА БАЗА ТА АРХІТЕКТУРА СУЧАСНИХ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО ВІДЕОСПОСТЕРЕЖЕННЯ

3.1. Технологічна база сучасних систем відеоспостереження

Технологічна база сучасних систем стрімко еволюціонує, рухаючись у напрямку інтелектуалізації, децентралізації та уніфікації. Ключовими трендами, що визначають цей розвиток, є повсюдне впровадження відеоаналітики на основі штучного інтелекту, перехід до розподіленої обробки даних та широке прийняття галузевих стандартів, яскравим прикладом яких є ONVIF у системах безпеки. Ці тенденції взаємопов'язані і спрямовані на створення більш гнучких, масштабованих та ефективних рішень. Сучасні системи відеоспостереження перетворилися з пасивних засобів запису на потужні інструменти аналізу. В основі цієї трансформації лежить відеоаналітика, що використовує алгоритми машинного навчання та штучного інтелекту для інтерпретації відеоданих у реальному часі.

Основні можливості сучасної відеоаналітики. Сучасна відеоаналітика – це комплекс алгоритмів і технологій оброблення відеопотоку в реальному часі з метою автоматичного виявлення, класифікації, ідентифікації та прогнозування подій. Вона є ключовим елементом «розумних» систем безпеки, управління транспортом, комерційного моніторингу та аналітики поведінки. Основні можливості відеоаналітики охоплюють такі напрями (рис. 3.1, табл. 3.1): детекцію та класифікацію об'єктів; розпізнавання облич і номерних знаків; поведінковий аналіз; бізнес-аналітику.

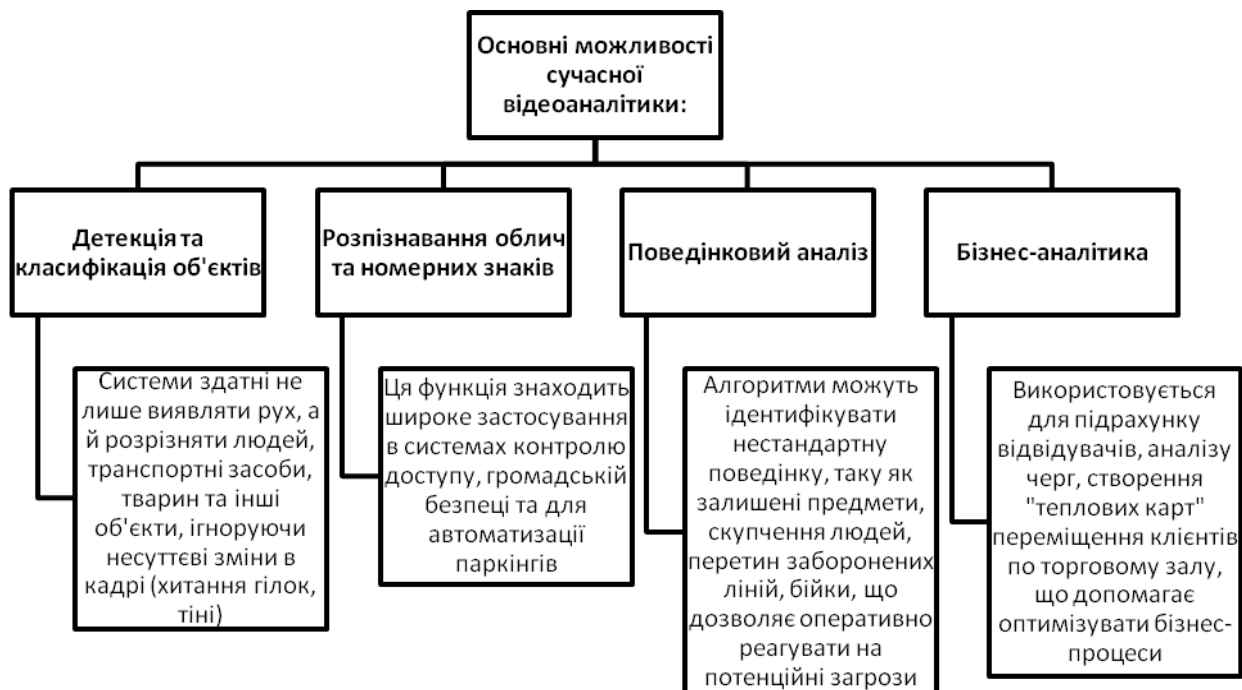


Рисунок 3.1 – Основні можливості сучасної відеоаналітики

Детекція об'єктів – це процес автоматичного виявлення в кадрі певних об'єктів, що відрізняються від фону, з використанням методів комп'ютерного зору. До таких об'єктів можуть належати люди, транспортні засоби, тварини, залишені предмети, зброя тощо. Алгоритми детекції базуються на поєднанні методів аналізу руху (motion detection), фонового моделювання (background subtraction), а також глибинного навчання, що дозволяє системам адаптуватися до складних умов освітлення, погодних змін або часткового перекриття об'єктів.

Класифікація об'єктів полягає у визначенні типу об'єкта після його виявлення. Наприклад, система може відрізнити людину від автомобіля чи велосипеда, а також уточнити підкатегорії (легковий або вантажний транспорт, чоловік або жінка, дорослий або дитина тощо). Завдяки застосуванню нейронних мереж (зокрема, архітектур типу CNN – Convolutional Neural Networks) забезпечується висока точність класифікації навіть у динамічних або багатолюдних середовищах.

Практичне застосування: контроль периметра та виявлення несанкціонованих об'єктів; автоматичне відстеження транспортних потоків; підрахунок людей у громадських місцях; пошук об'єктів за заданими ознаками у великих архівах відео.

Розпізнавання облич – одна з найрозвиненіших функцій відеоаналітики, що використовує біометричні характеристики людини для ідентифікації або верифікації особи. Процес включає кілька етапів: виявлення обличчя у відеопотоці; нормалізація зображення (вирівнювання, масштабування, освітлення); екстракція ознак (наприклад, відстані між очима, форма щелепи, структура шкіри); порівняння з еталонними зображеннями з бази даних.

Сучасні алгоритми (наприклад, FaceNet, DeepFace, ArcFace) досягають точності понад 99% при ідентифікації за якісного освітлення. Такі системи широко використовуються для контролю доступу, відеоспостереження у громадських місцях, розшуку осіб та безконтактної ідентифікації.

Розпізнавання номерних знаків (ANPR – Automatic Number Plate Recognition) призначене для автоматичного зчитування ідентифікаційних символів на автомобільних номерах. Алгоритми ANPR застосовують фільтрацію зображення, локалізацію області номерного знаку, сегментацію символів і подальше їх розпізнавання. Це забезпечує: автоматизований в'їзд/виїзд на територію; контроль швидкісного режиму; аналітику транспортних потоків; фіксацію порушень ПДР у реальному часі.

Поведінковий аналіз (behavioral analytics) дозволяє системі не лише виявляти об'єкти, а й розуміти контекст їхньої поведінки. Завдяки машинному навчанню відеоаналітика здатна розпізнавати типові та аномальні дії – наприклад, біг у забороненій зоні, залишення предмета, масові скупчення людей або агресивну поведінку.

Основні функції поведінкового аналізу: виявлення підозрілих дій (вторгнення, крадіжки, напад); аналіз руху натовпу (щільність, напрямок,

швидкість); прогнозування подій (виявлення небезпеки до її настання); виявлення падіння людини (у лікарнях, домах для літніх людей, на виробництві).

Поведінковий аналіз має вирішальне значення у безпеці об'єктів критичної інфраструктури, транспортних вузлів, стадіонів, торгових центрів тощо. Він дозволяє оперативно реагувати на потенційні інциденти та мінімізувати людський фактор у процесі моніторингу.

Бізнес-аналітика. Окрім завдань безпеки, відеоаналітика дедалі активніше використовується у комерційному секторі для отримання статистичних та маркетингових даних. Так звана бізнес-аналітика на основі відео (Video Business Intelligence) спрямована на аналіз поведінки клієнтів, ефективності роботи персоналу та оптимізацію бізнес-процесів.

Основні можливості: підрахунок відвідувачів (footfall analysis) – визначення кількості клієнтів у певні години або дні; теплові карти руху (heat maps) – відображення зон найбільшої активності покупців; черговий моніторинг – аналіз довжини черг і часу обслуговування; демографічний аналіз – оцінка віку, статі, емоційного стану клієнтів для персоналізації маркетингу; оцінка залученості – аналіз того, скільки часу людина проводить біля певного стенду або вітрини.

Завдяки цим інструментам компанії отримують можливість приймати рішення, засновані на реальних даних (data-driven decisions), підвищувати рівень обслуговування та ефективність бізнесу.

Таблиця 3.1

Основні функції сучасної відеоаналітики, їх призначення та сфери застосування

Функція відеоаналітики	Призначення	Основні сфери застосування
Детекція та класифікація об'єктів	Автоматичне виявлення рухомих або статичних об'єктів, визначення їх типу (людина, транспорт, предмет тощо)	Охоронні системи, контроль периметра, транспортний моніторинг, міський нагляд
Розпізнавання облич	Ідентифікація або верифікація особи за біометричними параметрами	Контроль доступу, правоохоронна діяльність, розшук осіб, системи безпеки підприємств
Розпізнавання номерних знаків (ANPR)	Автоматичне зчитування та фіксація номерних знаків транспортних засобів	Транспортна аналітика, автоматизований пропуск, фіксація порушень ПДР
Поведінковий аналіз	Виявлення та прогнозування підозрілої, аномальної або небезпечної поведінки об'єктів	Безпека громадських місць, охорона критичної інфраструктури, медичний моніторинг
Бізнес-аналітика (Video BI)	Збір і аналіз даних про поведінку людей для підвищення ефективності бізнес-процесів	Роздрібна торгівля, транспорт, маркетинг, управління персоналом
Підрахунок об'єктів і щільності руху	Визначення кількості людей або транспорту в певній зоні	Транспортні системи, торгові центри, організація заходів, міський моніторинг
Геоаналітика та теплові карти активності	Візуалізація зон найбільшої активності об'єктів для оптимізації простору	Торгові площі, виставкові зали, аеропорти, вокзали
Аналітика інцидентів і тривог	Автоматичне створення подій і сповіщень при виявленні аномалій	Центри безпеки, системи «розумного міста», моніторингові центри

Наведені функції (табл. 3.1) взаємодоповнюють одна одну. У комплексі вони утворюють інтелектуальну систему, здатну автоматично сприймати, аналізувати й інтерпретувати візуальні дані, що надходять із відеокамер. Завдяки цьому знижується навантаження на операторів, підвищується точність і швидкість прийняття рішень у режимі реального часу

Таким чином, сучасна відеоаналітика перетворює відеоспостереження з пасивного засобу фіксації на активний інтелектуальний інструмент аналізу середовища. Її можливості охоплюють безпеку, управління, маркетинг і прогнозування подій, що робить цю технологію невід’ємною складовою «розумних міст», транспортних систем і об’єктів стратегічного значення.

3.2. Архітектура сучасних систем відеоспостереження

Загальна структура систем відеоспостереження

Історичний розвиток систем відеоспостереження пройшов кілька ключових етапів, кожен із яких відображає зміну технологічних можливостей та зростання вимог до безпеки. Традиційно виділяють три основні підходи: аналогові системи (CCTV), цифрові системи з DVR¹ та гібридні архітектури, які стали проміжним кроком до сучасних IP-рішень.

Сучасні системи відеоспостереження є складними технічними комплексами, що забезпечують збір, передавання, оброблення, зберігання та аналіз відеоінформації з метою забезпечення безпеки, моніторингу об’єктів і підтримки управлінських рішень. Архітектура таких систем формується за принципами модульності, масштабованості та інтеграції з іншими інформаційними системами безпеки.

Типова архітектура системи відеоспостереження включає такі основні підсистеми (рис. 3.2, 3.3): збору відеоданих; передавання даних; оброблення та аналізу відео; підсистема зберігання даних та відображення та управління.

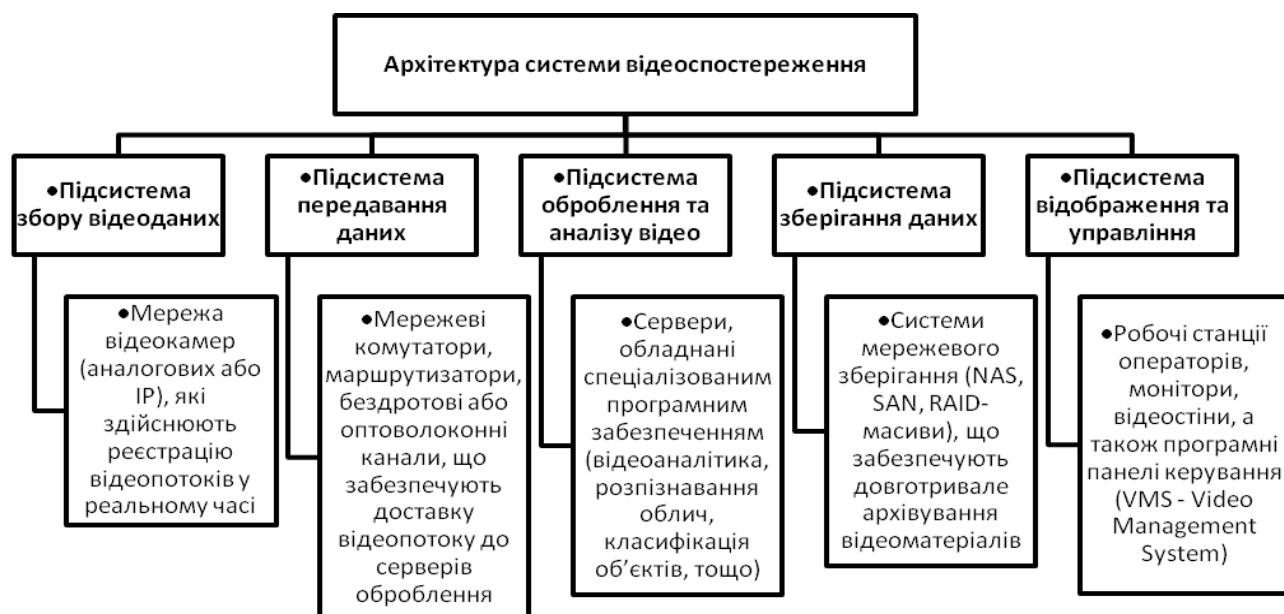


Рисунок 3.2 – Типова архітектура системи відеоспостереження

¹ DVR (цифровий відеореєстратор) — це цифровий відеороликореєстратор, пристрій, призначений для запису, зберігання та відтворення відеоінформації. DVR традиційне використання в системах відеоспостереження, працює з аналогами відеокамерами, приймаючи з них аналоговий сигнал, який потім оцифровується, кодується та записується на жорсткий диск або інші цифрові носії.



Рисунок 3.3 – Архітектура системи відеоспостереження

Підсистема збору відеоданих (камери та датчики) – це «очі» системи, які захоплюють візуальні дані та служать основними компонентами будь-якої системи. Аналогові камери (CCTV) передають відеосигнали через коаксіальний кабель до DVR. Вони простіші в установці та доступніші, але мають нижчу роздільну здатність. IP-камери (Інтернет-протокол) передають відеодані через мережу Ethernet або Wi-Fi. Вони мають вищу роздільну здатність, розширені функції, як-от вбудована відеоаналітика, та більшу масштабованість. PTZ-камери (поворотні, нахилені та масштабовані) дозволяють дистанційно керувати рухом (горизонтальне обертання та нахил) і масштабуванням, що ідеально для моніторингу великих відкритих просторів. 360° камери використовують об'єктив типу «риб'яче око» або кілька датчиків для повного огляду області, що дозволяє замінити кілька традиційних камер.

Підсистема передавання даних (мережевий зв'язок) є основою, що з'єднує всі компоненти системи, забезпечуючи передачу відеопотоків та зв'язок. Ethernet це найпоширеніший дротовий мережевий стандарт, важливий для стабільного високошвидкісного з'єднання відеопотоків високої роздільної здатності. PoE (живлення через Ethernet) дозволяє передавати як живлення, так і дані по одному кабелю. Бездротова технологія Wi-Fi забезпечує гнучкість у розміщенні камер. Може бути схильною до перешкод та обмежень пропускної здатності. Також бездротова технологія наступного покоління 5G пропонує надзвичайно високу швидкість та низьку затримку, підтримуючи відеопотоки високої роздільної здатності для віддалених або мобільних застосувань. Мережеве обладнання включає маршрутизатори та комутатори, які забезпечують транспорт відео.

Підсистема оброблення та аналізу відео – це «мозок» системи, що надає інструменти для керування та автоматичного аналізу відеоданих. Обробка може бути централізованою (на сервері) або децентралізованою (edge-computing). Програмні платформи (VMS – Video Management Systems) входять до централізованої системи управління, що дозволяє користувачам переглядати прямі трансляції, керувати налаштуваннями камер, шукати та відтворювати записані матеріали. Відеоаналітика – це програмне забезпечення, яке автоматично аналізує відеоматеріали для виявлення певної поведінки, об'єктів або подій. У децентралізованих моделях базову аналітику

виконує сама камера (edge-processing), передаючи лише метадані або тривожні події, що знижує навантаження на мережу.

Структура підсистеми зберігання даних залежить від обсягу даних, політики зберігання та вимог до доступності. Вона включає: локальні сервери (виділені комп'ютери або сервери на місці, що забезпечують повний контроль над даними); NAS (мережеве сховище даних – спеціалізований мережевий пристрій для економічно ефективного керування великими обсягами відеоданих); SAN (мережа зберігання даних – високошвидкісна мережа, що забезпечує доступ до даних на рівні блоків, використовується у великих корпоративних середовищах, де критична висока продуктивність); хмарне сховище, яке виконує функцію зберігання відеоданих на віддалених серверах постачальника послуг. Пропонує високу масштабованість, резервування та віддалений доступ, але вимагає стабільного підключення до Інтернету.

Підсистема відображення та управління забезпечує взаємодію оператора із системою, надаючи інтерфейс для моніторингу та адміністрування. Ця підсистема включає: монітори для відображення прямого відеопотоку та записаного матеріалу: програмне забезпечення VMS, яке виступає основним інтерфейсом управління для перегляду, пошуку, відтворення та адміністрування всієї системи та робочі станції оператора – комп'ютери, з яких здійснюється доступ до VMS для контролю та реагування на події. У централізованих моделях забезпечують централізований контроль.

Моделі архітектури відеоспостереження

Архітектурна побудова систем відеоспостереження може реалізовуватись за кількома моделями: централізована архітектура; децентралізована (розподілена) архітектура; хмарна архітектура; гібридна архітектура (рис. 3.4).



Рисунок 3.4. Моделі архітектури побудови систем відеоспостереження

Централізована архітектура систем відеоспостереження

Централізована архітектура систем відеоспостереження це класична модель побудови системи відеоспостереження, у якій всі відеопотоки з камер спостереження передаються до єдиного центру оброблення та зберігання даних. Центральний сервер (або група серверів) виконує функції приймання, запису, аналітики й управління відеоінформацією.

До складу типової централізованої системи входять такі компоненти: камери спостереження – аналогові або IP-пристрої, які здійснюють реєстрацію відеопотоку; мережеве обладнання – комутатори, маршрутизатори, мережеві відеореєстратори (NVR), що забезпечують зв'язок із центром оброблення; центральний сервер або дата-центр – виконує зберігання відеоархівів, відеоаналітику, обробку подій і керування системою; робочі станції операторів – підключаються до центрального сервера для перегляду відео та керування камерами; архівне сховище – RAID-масиви або мережеві системи зберігання NAS/SAN, де зберігаються відеозаписи.

Принцип роботи: відеопотік від усіх камер передається через мережу до центрального сервера; сервер проводить компресію, оброблення та збереження відео в архів; оператори через програмне забезпечення (VMS – *Video Management System*) мають доступ до потоків у реальному часі або архівних записів. Всі налаштування, аналітичні сценарії та сповіщення також централізовано керуються з цього сервера.

Переваги централізованої архітектури: єдина точка адміністрування, яка спрощує контроль, моніторинг та оновлення системи; цілісність даних (усі записи зберігаються в одному місці, що полегшує пошук і аналіз; можливість централізованої аналітики; високий рівень безпеки, адміністратор може централізовано контролювати права доступу та моніторити підключення.

Недоліки централізованої архітектури: високе навантаження на мережу через одночасну передачу великої кількості відеопотоків; залежність від центрального вузла (збій сервера може призвести до втрати запису або зупинки системи); високі вимоги до каналів зв'язку та серверних ресурсів; обмежена масштабованість (додавання нових камер потребує розширення апаратних ресурсів сервера).

Сфери застосування. Централізована архітектура найчастіше використовується у системах: відеоспостереження державних установ і великих підприємств, банківських і фінансових структур, транспортних вузлів (вокзали, аеропорти), об'єктів критичної інфраструктури, де необхідна повна централізована координація та контроль.

Децентралізована (розподілена) архітектура систем відеоспостереження

Децентралізована або розподілена архітектура систем відеоспостереження (рис. 3.5) передбачає, що основні функції збору, оброблення та зберігання відеоінформації виконуються безпосередньо на периферійних пристроях – інтелектуальних IP-камерах або локальних вузлах

оброблення (edge devices). Це означає, що кожен елемент системи працює автономно, має власні ресурси обчислення і пам'яті, а центральний сервер виконує лише функції координації, моніторингу та архівації важливих даних.

Така архітектура суттєво відрізняється від традиційної централізованої моделі, де всі відеопотоки передаються на центральний сервер для оброблення. У розподілених системах ключовим принципом є edge processing – виконання відеоаналітики на місці реєстрації даних.

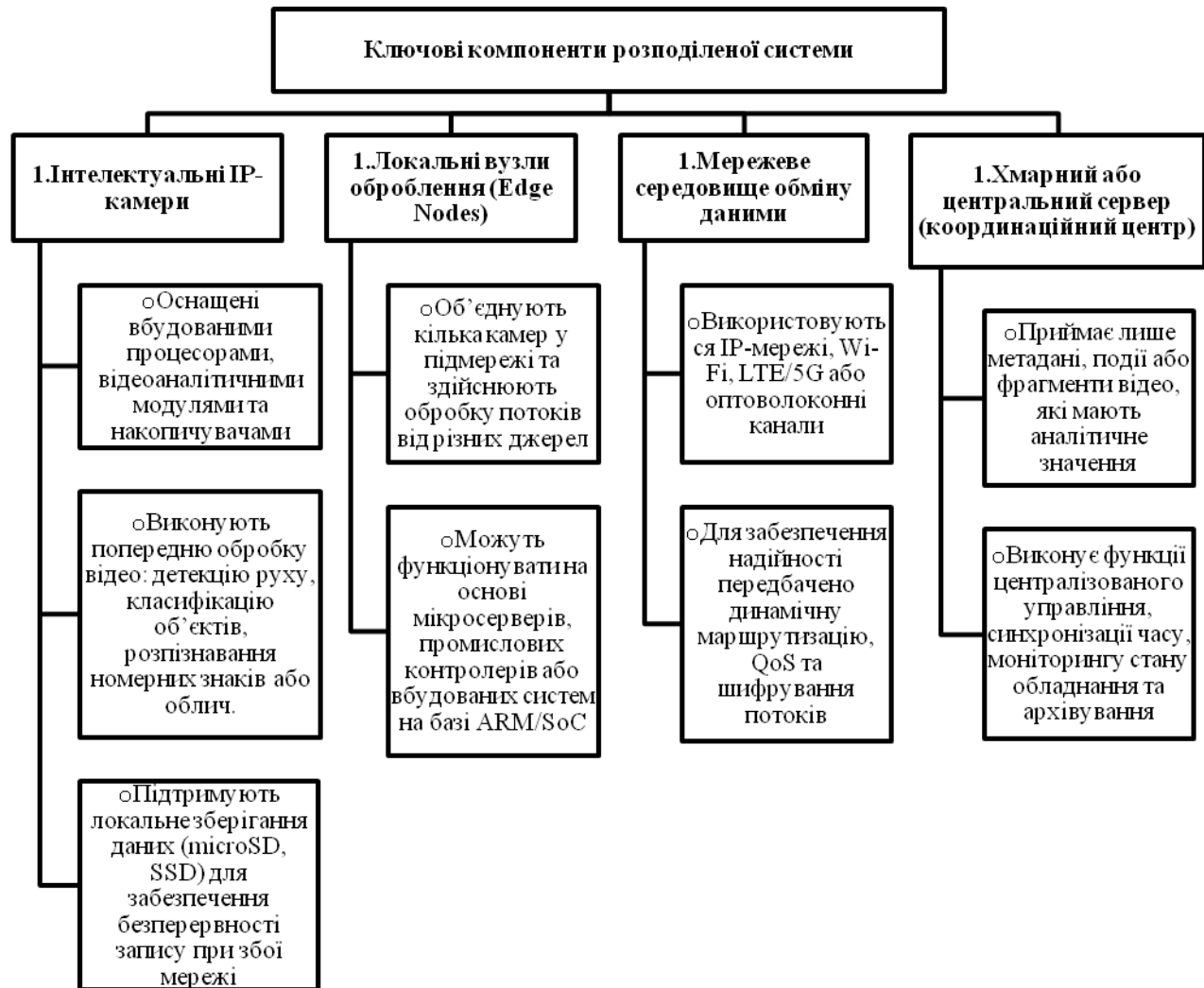


Рисунок 3.5. Ключові компоненти розподіленої системи

Переваги децентралізованої архітектури: висока відмовостійкість (у разі виходу з ладу центрального сервера система продовжує функціонувати локально); зменшення навантаження на мережу (передаються лише релевантні дані (події, тривожні фрагменти); зниження затримки оброблення (відеоаналіз здійснюється на місці, що особливо важливо для задач оперативного реагування); гнучкість масштабування (додавання нових камер не потребує суттєвих змін у структурі системи); можливість автономної роботи, навіть при відсутності зв'язку із сервером відео продовжує записуватись локально.

Недоліки: підвищені вимоги до «розумних» камер, дорожча апаратура з високими обчислювальними ресурсами; складність централізованого адміністрування та синхронізації великої кількості автономних вузлів;

більша кількість точок доступу потребує комплексного кіберзахисту; при використанні обладнання різних виробників потрібна підтримка стандартів формату даних ONVIF, RTSP, MQTT тощо.

Типові сфери застосування: системи відеоспостереження у транспортній інфраструктурі (станції, порти, перехрестя); розумні міста (Smart City) та муніципальні системи моніторингу; мобільні комплекси безпеки (патрульні автомобілі, дрони, наземні роботизовані платформи); військові та оборонні системи спостереження, де необхідна стійкість до втрат зв'язку та автономність.

Децентралізована архітектура є сучасним напрямом розвитку систем відеоспостереження, що поєднує інтелектуальні технології оброблення даних на периферії з можливостями хмарної інтеграції. Вона забезпечує високу ефективність, оперативність та гнучкість у побудові систем безпеки різного масштабу – від локальних об'єктів до розподілених державних і військових мереж.

Хмарна архітектура систем відеоспостереження

Хмарна архітектура (Cloud-based Video Surveillance Architecture) – це сучасна модель побудови систем відеоспостереження, у якій основні процеси зберігання, оброблення та аналізу відеоданих виконуються у віддалених дата-центрах за допомогою хмарних сервісів (рис. 3.6). Така архітектура стала популярною завдяки розвитку широкосмугового інтернету, технологій віртуалізації та сервісних моделей типу *Video Surveillance as a Service* (VSaaS). Ключовим принципом такої архітектури є перенесення більшості функцій системи (зберігання відеоархіву, аналітика, управління користувачами, моніторинг) із локальної інфраструктури (серверів і реєстраторів) до хмари. Камери відеоспостереження підключаються до інтернету і передають потоки відео безпосередньо у хмарний центр оброблення даних (ЦОД).

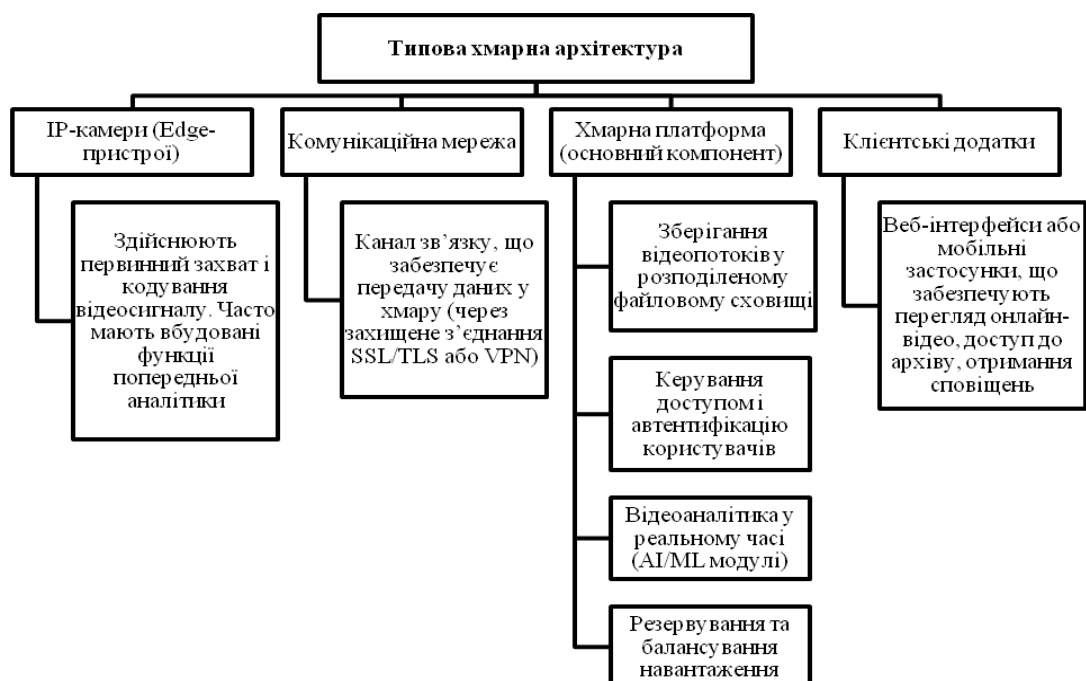


Рисунок 3.6 – Структурна схема хмарної системи

Переваги хмарної архітектури: масштабованість (легке додавання нових камер і користувачів без фізичного розширення інфраструктури); гнучкість і мобільність (доступ до системи з будь-якого місця через інтернет); зниження капітальних витрат (немає потреби у власних серверах і сховищах); автоматичне оновлення та технічна підтримка (програмне забезпечення підтримується провайдером); інтеграція з аналітичними сервісами (застосування хмарного штучного інтелекту для розпізнавання облич, поведінкових патернів, підрахунку людей тощо); висока надійність і резервування (використання географічно розподілених дата-центрів).

Недоліки та виклики хмарних технологій. Залежність від стабільності інтернет-з'єднання – у разі втрати мережі доступ до системи обмежується. Безпека даних – ризик несанкціонованого доступу або витоку інформації через віддалене зберігання. Регуляторні обмеження – зберігання персональних даних у закордонних хмарах може порушувати вимоги законодавства. Операційні витрати (OPEX) – щомісячна абонентська плата за зберігання відео та використання сервісу.

Типи хмарних рішень. Публічні хмари (Public Cloud) – ресурси спільні для багатьох клієнтів (Amazon AWS, Microsoft Azure, Google Cloud). Приватні хмари (Private Cloud) – інфраструктура розгортається для одного замовника, наприклад у силових структурах або великих корпораціях. Гібридні хмари (Hybrid Cloud) – поєднання локального зберігання (Edge recording) і хмарного архіву, що забезпечує баланс між безпекою та гнучкістю.

Приклади практичної реалізації. VSaaS-платформи: *Eagle Eye Networks*, *Verkada*, *Ivideon*, *Axis Companion Cloud*. Інтеграція з системами Smart City – віддалене керування тисячами камер для моніторингу дорожнього руху, безпеки громадських місць, аналітики потоків людей.

Таким чином, хмарна архітектура є одним із найбільш перспективних напрямів розвитку систем відеоспостереження. Вона забезпечує високу гнучкість, масштабованість і доступність, але водночас потребує надійних механізмів кіберзахисту, політик конфіденційності та резервного зберігання даних. Перспективними тенденціями є інтелектуальна аналітика на базі ШІ, edge-computing і інтеграція з IoT-платформами, що формують основу для концепції «розумного відеоспостереження» (Smart Surveillance).

Гібридна архітектура систем відеоспостереження

Гібридна архітектура поєднує елементи централізованих і децентралізованих систем, забезпечуючи баланс між гнучкістю, надійністю та керованістю. Такий підхід став особливо поширеним у період переходу від аналогових систем CCTV до IP-відеоспостереження, коли виникла потреба одночасно підтримувати наявне обладнання і впроваджувати сучасні цифрові рішення.

Основна ідея гібридної архітектури полягає у тому, що частина відеокамер підключається до аналогових пристроїв реєстрації (DVR – Digital Video Recorder), а інша – до мережевих серверів або відеореєстраторів IP-типу (NVR – Network Video Recorder). Дані з обох підсистем об'єднуються через спеціалізоване програмне забезпечення або центральний сервер управління, який забезпечує спільний доступ, моніторинг та аналітику.

Типова гібридна архітектура містить такі ключові компоненти: аналогові камери, які передають відеосигнал по коаксіальному кабелю до DVR; IP-камери – передають потоки відео через Ethernet-мережу (LAN/WAN) до NVR або безпосередньо до серверів зберігання; відеореєстратори DVR/NVR, які забезпечують запис, архівацію та базовий аналіз відео; центральний сервер керування (CMS/VMS), який призначений для об'єднання різних підсистем, здійснення централізованого моніторингу, керування доступом, аналітики та інтеграції з іншими системами безпеки; користувацькі станції (операторські місця) – дозволяють здійснювати перегляд у реальному часі, пошук архіву, формування звітів тощо.

Переваги гібридної архітектури. Поступовий перехід до IP-технологій. Організації можуть модернізувати систему поетапно, без необхідності повної заміни обладнання. Існуюча інфраструктура CCTV використовується паралельно з новими цифровими компонентами. У разі збою центрального вузла окремі підсистеми (аналогова чи IP) можуть продовжувати функціонувати автономно. Підтримка різних стандартів камер і протоколів (ONVIF, RTSP, H.264/H.265 тощо). Можливість використання відеоаналітики, розпізнавання облич, номерів, виявлення руху тощо на IP-ділянках мережі.

Недоліки. Складність адміністрування. Необхідність синхронізації налаштувань різних типів пристроїв. Вищі вимоги до мережевої інфраструктури. Передача великих обсягів даних потребує високошвидкісних каналів та резервування. Невідповідність протоколів. Деякі старі аналогові системи можуть бути несумісними з сучасними VMS.

Приклади застосування. Гібридні системи активно використовуються у: муніципальних системах безпеки, де поєднано старі камери спостереження та нові IP-зони; транспортних вузлах (вокзали, аеропорти), де одночасно функціонують різні типи камер; великих підприємствах із поетапною модернізацією охоронних систем; банківських структурах, де важлива безперервність запису та збереження історичних даних.

Гібридна архітектура є проміжним, але стратегічно ефективним рішенням між аналоговими й повністю IP-орієнтованими системами. Вона забезпечує гнучкість модернізації, знижує фінансові ризики переходу та дозволяє поєднати традиційні й інноваційні технології відеоспостереження у єдиному безпековому комплексі.

Таким чином, класичні архітектурні підходи стали основою сучасних систем відеоспостереження. Вони продемонстрували еволюцію від простих аналогових каналів спостереження до цифрових та гібридних моделей, що забезпечили підґрунтя для повноцінного переходу до мережевих IP-рішень і хмарних платформ.

Таблиця 3.1

Порівняння класичних архітектурних підходів до побудови систем відеоспостереження

Архітектурний підхід	Ключові характеристики	Переваги	Недоліки	Типові сфери застосування
Аналогова архітектура (CCTV)	Використання коаксіальних кабелів, аналогових камер, відеомагнітофонів/ DVR	Простота впровадження; низька вартість; відсутність затримок сигналу	Обмежена якість зображення; складність масштабування; відсутність інтелектуальних функцій	Банківські відділення, невеликі магазини, склади
Цифрова архітектура з DVR	Камери з оцифруванням сигналу, DVR з жорсткими дисками, можливість архівації	Краща якість відео; простота перегляду архівів; відносно низька ціна	Обмежена масштабованість; залежність від ємності DVR	Малі та середні підприємства, школи, офіси
Мережна (IP) архітектура з NVR	Використання IP-камер, Ethernet/PoE, мережевого відеореєстратора	Висока якість зображення; масштабованість; віддалений доступ; підтримка аналітики	Вища вартість обладнання; потреба в кваліфікованому персоналі; залежність від мережі	Міське відеоспостереження, транспорт, великі корпорації
Гібридна архітектура	Поєднання аналогових та IP-камер, гібридні DVR/NVR	Гнучкість; можливість модернізації старих систем; поступовий перехід до IP	Складність управління; різна якість сигналу	Організації, що оновлюють систему поетапно (торгові мережі, державні установи)

Класичні архітектурні підходи до побудови систем відеоспостереження еволюціонували від простих аналогових рішень до комплексних мережеских структур з інтелектуальною аналітикою. Аналогові системи залишаються актуальними для невеликих об'єктів з мінімальними вимогами, тоді як IP-архітектури забезпечують масштабованість, високу якість зображення та інтеграцію з іншими інформаційними системами безпеки. Гібридні рішення виступають компромісом для організацій, які прагнуть зберегти існуючі інвестиції, поступово переходячи до сучасних технологій. Таким чином, вибір архітектурного підходу визначається балансом між вартістю, технічними вимогами та стратегічними потребами користувача.

Порівняльний аналіз показує, що еволюція класичних архітектур відбувалася у напрямі підвищення якості зображення, масштабованості та гнучкості інтеграції. Аналогові системи відігравали ключову роль на ранніх етапах, однак їх обмеженість зумовила перехід до цифрових рішень із DVR. Вони забезпечили якісніший запис і довший архів, проте залишалися обмеженими в масштабуванні. Гібридні системи стали компромісом, дозволивши зберегти інвестиції в аналогові камери й водночас інтегрувати сучасні IP-рішення. Таким чином, класичні підходи заклали основу для повної міграції до IP-архітектур, які нині є стандартом індустрії.

3.3. Класифікація систем відеоспостереження

Сучасні системи відеоспостереження можна класифікувати наступним чином: системи відеоспостереження побудовані на аналоговому обладнанні; системи побудовані на комбінованому, як аналоговому так і цифровому обладнанні та системи відеоспостереження побудовані на базі IP-технологій підключення цифрових пристроїв.

Аналоговою системою відеоспостереження є система в якій відеосигнал формується аналоговими камерами та передається за допомогою каналів зв'язку в аналоговій формі (рис. 3.7).

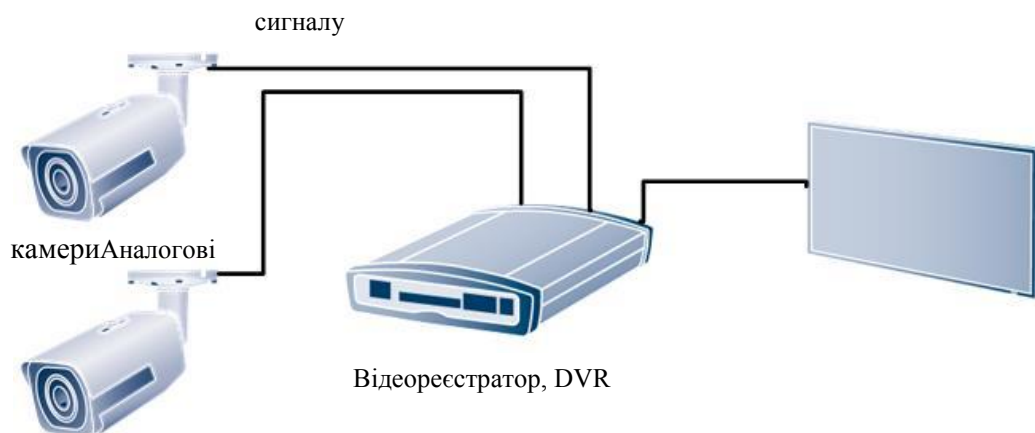


Рисунок 3.7 – Аналогова система відеоспостереження

Основними перевагами аналогових систем відеоспостереження є їх порівняно низька вартість за умови забезпечення достатньо високої якості зображення, простота налаштування, взаємна сумісність обладнання різних виробників у межах одного стандарту (АHD, TVI, CVI), а також повна відсутність затримки під час передавання сигналу. Для розгортання сучасної аналогової системи відеоспостереження зазвичай потрібні такі компоненти:

1. Аналогові камери спостереження (при цьому обробка сигналу всередині камери може бути цифровою);
2. Відеореєстратори, серед яких:
 - PC based DVR – персональний комп'ютер із встановленою платою відеозахоплення та спеціальним програмним забезпеченням;
 - Stand Alone DVR – окремий пристрій, призначений для цифрового запису аналогового відеопотоку (такі відеореєстратори мають виключно входи для аналогових камер);
3. Блоки живлення для камер;
4. Середовище передавання відеосигналу (найчастіше коаксіальний кабель);
5. Пристрої для відображення відеоінформації.

Попри свої переваги, аналогові системи відеоспостереження мають низку суттєвих обмежень. Передусім вони є локальними: відстань між камерами та відеореєстратором зазвичай не перевищує 500 метрів. Це пов'язано з тим, що коаксіальний кабель із хвильовим опором 75 Ом має значне затухання – приблизно 2,6 дБ для кабелю діаметром 6 мм та близько 1,4 дБ для діаметра 9 мм. Для того щоб відеореєстратор коректно приймав сигнал, рівень відеосигналу на його вході має становити від 3 до 6 дБ.

Конструкція аналогової системи обов'язково включає такі елементи, як відеореєстратор, жорсткий диск, блоки живлення та кабельні лінії для передавання відеосигналу і живлення камер. Крім того, аналогові камери використовують черезрядкову розгортку, що призводить до появи ефекту «розмиття» зображення під час спостереження за швидкорухомими об'єктами. Їхні технічні параметри обмежені чинними телевізійними стандартами (SECAM, NTSC, PAL), що визначає максимальну роздільну здатність і частоту кадрів та унеможливорює значне вдосконалення якості зображення в межах цих систем.

Цифровою системою відеоспостереження вважають таку систему, у якій відеосигнал формується цифровими камерами і передається каналами зв'язку вже в цифровому форматі (рис. 3.8).



Рисунок 3.8 – Цифрова система відеоспостереження

Сучасні цифрові системи відеоспостереження зазвичай включають такі компоненти:

1. IP-камери відеоспостереження;
2. Мережеві відеореєстратори (NVR – network video recorder);
3. Мережеве обладнання та середовище передавання даних;
4. Спеціалізоване програмне забезпечення.

Переваги цифрових систем відеоспостереження полягають у такому:

1. Використання прогресивної розгортки, що забезпечує відсутність спотворень під час фіксації швидко рухомих об'єктів.
2. Відсутність обмежень телевізійних стандартів, що дозволяє отримувати відеозображення з високою роздільною здатністю та підвищеною частотою кадрів.
3. Простота створення розподілених інфраструктур відеоспостереження.
4. Можливість функціонування системи без традиційних відеореєстраторів – запис може виконуватися на хмарний відеосервер або на вбудовану карту пам'яті камери.
5. Підтримка бездротового передавання даних за допомогою технологій Wi-Fi, Wi-Max та інших безпроводних стандартів.
6. Забезпечення відеоаналітики через спеціалізоване програмне забезпечення, яке може обробляти відеодані як на серверних потужностях, так і безпосередньо на камері.

У випадках, коли для отримання відеозображення та його передавання каналами зв'язку одночасно застосовуються цифрові й аналогові камери (рис. 3.9), така система класифікується як комбінована. До її складу можуть входити як аналогові, так і цифрові камери, а для запису й обробки відеоінформації використовуються різні типи обладнання: PC-based DVR, Stand Alone DVR, NVR (мережеві відеореєстратори, що приймають відеосигнал від IP-камер) та спеціалізовані гібридні реєстратори HDVR

(hybrid digital video recorder), які забезпечують роботу з обома типами камер – аналоговими та IP.

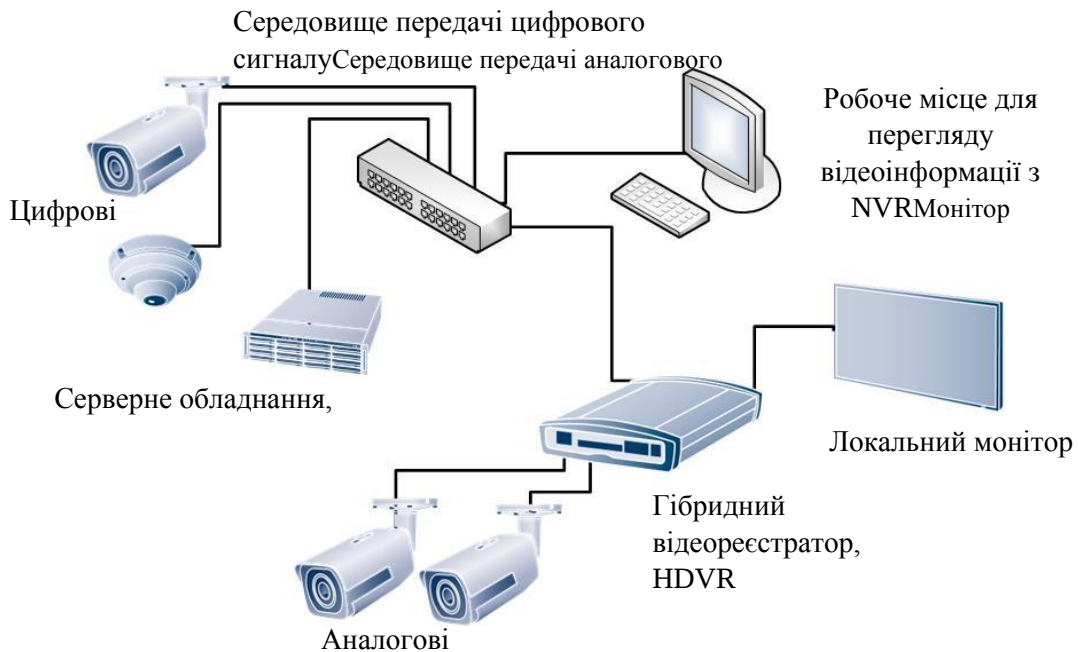


Рисунок 3.9 – Комбінована система відеоспостереження

Широкий функціонал цифрових камер відеоспостереження актуалізує проблему ефективної передачі даних від камери до відеосервера. Більшість таких камер оснащені інтерфейсом Ethernet і працюють на основі стеку протоколів TCP/IP. Пропускна здатність найпоширенішого стандарту Fast Ethernet становить 100 Мбіт/с, тому для передавання відео необхідно застосовувати компресію, що неминуче впливає на якість зображення. Зазвичай у IP-камерах відеосигнал, сформований ПЗЗ або КМОП матрицею, стискається за допомогою методів відеокompresії – покадрових (MJPEG) або поточкових (MPEG-4, H.264). Сучасні IP-камери орієнтовані на підтримку стандарту «H.264/AVC/MPEG-4 Part 10». Цей стандарт визначає процес декодування, тоді як варіанти кодування можуть відрізнятися.

Перспективним напрямом еволюції H.264 є технологія H.264 SVC, яка дозволяє здійснювати багаторівневе кодування відео з різною якістю. За умов обмеженої пропускної здатності мережі відеопотік нижчої деталізації можна отримати шляхом «відкидання» частини пакетів із повного потоку, стисненого за допомогою H.264 SVC. Таким чином, IP-камера з підтримкою цього кодека здатна одночасно передавати відео, оптимізоване під можливості кожного мережевого пристрою – від робочої станції оператора та сервера архівування до мобільного телефону.

Існують також цифрові камери, які передають відеодані без застосування компресії. До них належать пристрої, що підтримують стандарти HD CCTV та HD-SDI, які дають змогу передавати сигнал по коаксіальному кабелю на відстань до 170 м. Крім того, використовується

стандарт GigE Vision, який забезпечує передавання некомпресованого відео мережею Gigabit Ethernet, а також інтерфейси USB 2.0 та USB 3.0, що зазвичай застосовуються у системах невеликого масштабу. Ще одним поширеним варіантом є інтерфейс «Camera Link». Подібні камери найчастіше використовують у комплексах відеоаналітики, де потрібна висока точність обробки зображення.

Для усунення проблеми несумісності обладнання та технологій різних виробників було запроваджено низку промислових стандартів, серед яких найпоширенішими є ONVIF, PSIA та інші. Створений у 2008 році компаніями Axis Communications, Bosch Security Systems і Sony міжнародний форум ONVIF (Open Network Video Interface Forum) розробив відкритий стандарт для мережевих систем відеоспостереження. Його специфікації базуються на вебслужбах, описаних мовою WSDL, а також на протоколах RTP/RTSP, SOAP і стандартах відеокомпресії H.264, MPEG-4 та MJPEG.

Стандарт визначає протоколи взаємодії між IP-камерами, кодеками, відеореєстраторами, системами керування відео та комплексами контролю доступу. Він регламентує такі аспекти, як конфігурація мережевого інтерфейсу, налаштування потокової передачі відео та метаданих відеоаналітики, автоматичне виявлення пристроїв за протоколом WS-Discovery, параметри відеозапису та пошуку в архіві, управління профілями роботи камери, підтримка функцій повороту, нахилу й масштабування (PTZ), передавання та обробка подій, функції відеоаналітики та забезпечення безпеки, включаючи керування доступом і шифрування.

У сучасних цифрових системах відеоспостереження, що підтримують функції відеоаналітики, для зменшення навантаження на мережеву інфраструктуру застосовують принцип розподіленої обробки даних. Частина обчислювальних операцій виконується безпосередньо на IP-камері. Через обмежену продуктивність вбудованих процесорів на цьому рівні зазвичай реалізуються базові функції відеоаналітики, такі як «перетин забороненої лінії», «детектор руху», «контроль маршруту» та інші. Натомість більш ресурсомісткі завдання – наприклад, зіставлення виявлених об'єктів з еталонними зразками чи розпізнавання символів – виконуються на серверній стороні.

Прикладом такого підходу є технологія DEPA (Distributed Enhanced Processing Architecture), розроблена компанією Sony. Вона передбачає дворовісну схему обробки відеоінформації:

- на першому етапі, який виконується на IP-камері, відбувається відокремлення об'єктів від фону та їх попередня класифікація як рухомих або статичних. Потім ці відомості перетворюються в метадані й передаються мережею окремо від основного відеопотоку;

- на другому етапі, що реалізується на сервері, отримана інформація зберігається, проходить подальшу обробку відповідно до заданих алгоритмів, і при виявленні певних умов система генерує відповідну реакцію – відображення події на моніторі, активацію сигналу тривоги тощо. Історично, системи відеоспостереження будувались на телевізійних стандартах. Але, з

розвитком технологій, почали зростати вимоги до систем відеоспостереження, і це в результаті призвело до того, що ці стандарти стали обмежувати можливості розвитку систем відеоспостереження. Такі тенденції і стали поштовхом до переходу від аналогових пристроїв та систем до цифрових.

На сьогодні під час побудови систем відеоспостереження застосовуються як аналогові, так і цифрові компоненти, однак зберігання відеоданих у переважній більшості випадків здійснюється виключно у цифровому форматі. Попри активний розвиток цифрових технологій, аналогові системи також продовжують удосконалюватися, зокрема у напрямі підвищення роздільної здатності камер та впровадження форматів високої чіткості, таких як HD CVI, AHD та HD TVI.

Сучасні комплекси відеоспостереження виконують не лише функції забезпечення безпеки, а й дозволяють ефективніше керувати процесами, що відбуваються на контрольованому об'єкті. Розширені можливості цих систем активно застосовуються правоохоронними та військовими структурами для якісного виконання покладених на них завдань.

Контрольні питання до розділу III

1. Які ключові проєкти формують китайську модель «Тотального контролю» та їхні основні цілі?
2. Опишіть принципи централізації даних у китайській системі «Небесне око» (Tianwang/Skynet).
3. Які технології штучного інтелекту використовуються в китайській моделі для аналізу відео?
4. Які ризики та критика пов'язані з китайською моделлю «Тотального контролю»?
5. Що таке проєкт CROMATICA та його призначення в ЄС?
6. Опишіть функціональність проєкту ARGUS-IS (США) для спостереження.
7. Які основні функції проєкту SURVEIRON для захисту критичної інфраструктури?
8. Що таке проєкт DIVA (Deep Intermodal Video Analytics) та його мета?
9. Опишіть систему «Відеоконтроль-Рубіж» та її застосування в Україні.
10. Як системи відеоспостереження інтегруються в проєкти Smart City в Україні (наприклад, «Безпечне місто» в Києві)?
11. Які переваги використання «хмарних технологій» у системах відеоспостереження за міжнародним досвідом?
12. Перелічіть ключові проєкти ЄС для захисту кордонів та критичної інфраструктури (наприклад, EWISA, SUBITO).

IV. СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОАНАЛІТИКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ТА ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

4.1. Системи відеоспостереження та відеоаналітики Національної поліції України

Відеоспостереження в діяльності Національної поліції України має ключове значення для профілактики, розкриття та документування кримінальних правопорушень, забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і держави. Воно допомагає ідентифікувати підозрюваних, фіксувати докази злочинних діянь, моніторити ситуацію в публічних місцях тощо. Системи відеоспостереження в режимі реального часу моніторять публічні місця, тим самим допомагаючи працівникам поліції швидко виявляти підозрілі дії або предмети, а отже вносять вагомий внесок у запобігання та протидію кримінальним правопорушенням та розкриття вже вчинених злочинних діянь.

Відповідно до Закону України «Про Національну поліцію» поліція під час виконання покладених на неї завдань може застосовувати як превентивний поліцейський захід застосування технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису (ст. 31).¹

Крім того, відповідно до ст. 40 вищезазначеного Закону, 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.

Такі технічні прилади та технічні засоби, як фото- і відеотехніка, у тому числі техніка, що працює в автоматичному режимі, технічні прилади та технічні засоби з виявлення та/або фіксації правопорушень; технічні прилади та технічні засоби з виявлення радіаційних, хімічних, біологічних та ядерних загроз; поліція може закріплювати на однострої, у/на безпілотних повітряних судах, службових транспортних засобах, судах чи інших плавучих засобах, у тому числі тих, що не мають кольорографічних схем, розпізнавальних

¹ Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19?find#Text> (дата звернення: 15.11.2025).

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

Строки та порядок зберігання матеріалів фото- і кінозйомки, відеозапису та результатів їх аналізу встановлюються Міністерством внутрішніх справ України.¹

Що стосується застосування відеореєстраторів, то основною метою їх використання 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.²

Застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису визначається інструкцією, яка затверджується наказом Міністерства внутрішніх справ 18.12.2018 року № 1026.

Отже, 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.

¹ Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19?find#Text> (дата звернення: 15.11.2025).

² Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 46-47.

Під час здійснення повноважень поліцейський забезпечує збереження та належні умови експлуатації виданого йому портативного відеореєстратора та не допускає його розряджання.

У разі пошкодження портативного відеореєстратора поліцейський негайно доповідає про це відповідальній особі та керівнику органу, підрозділу поліції. Після прибуття до місця постійної дислокації портативний відеореєстратор або карта пам'яті передається відповідальній особі. Під час приймання портативного відеореєстратора відповідальна особа проводить його візуальний огляд та за відсутності видимих пошкоджень приймає під підпис зазначений портативний відеореєстратор або карту пам'яті. Відповідальна особа забезпечує безперебійне заряджання портативного відеореєстратора впродовж 4 годин та експорт інформації під час під'єднання до док-станції в автоматичному режимі або в інший спосіб, визначений виробником такого відеореєстратора. У разі виявлення механічних пошкоджень портативного відеореєстратора або карти пам'яті відповідальна особа здійснює відповідний запис у Журналі обліку й письмово доповідає про цей факт керівнику органу, підрозділу поліції. За необхідності портативний відеореєстратор може застосовуватися під час проведення поліцейськими навчальних занять та навчальних зборів зі службової підготовки з метою здійснення аналізу дій поліцейських.

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. У разі пошкодження портативного відеореєстратора поліцейський негайно доповідає про це відповідальній особі та керівнику органу, підрозділу поліції. Після прибуття до місця постійної дислокації портативний відеореєстратор або карта пам'яті передається відповідальній особі. Під час приймання портативного відеореєстратора відповідальна особа проводить його візуальний огляд та за відсутності видимих пошкоджень приймає під підпис зазначений портативний відеореєстратор або карту пам'яті. Відповідальна особа забезпечує безперебійне заряджання портативного відеореєстратора впродовж 4 годин та експорт інформації під час під'єднання до док-станції в автоматичному режимі або в інший спосіб, визначений виробником такого відеореєстратора. У разі виявлення механічних пошкоджень портативного відеореєстратора або карти пам'яті відповідальна особа здійснює відповідний запис у Журналі обліку й письмово доповідає про цей факт керівнику органу, підрозділу поліції. За необхідності портативний відеореєстратор може застосовуватися під час проведення поліцейськими навчальних занять та

навчальних зборів зі службової підготовки з метою здійснення аналізу дій поліцейських.

Автомобільні системи встановлюються на службових транспортних засобах ситуаційних центрів, командно-штабних автомобілях, спеціальному автотранспорті для перевезення затриманих та взятих під варту осіб. У спеціальному автотранспорті, призначеному для перевезення затриманих та взятих під варту осіб, кількість відеокамер автомобільної системи визначається відповідно до технічних завдань та норм належності, затверджених у встановленому порядку.

Автомобільні системи спеціального автотранспорту включаються під час здійснення конвоювання з моменту поміщення затриманих та взятих під варту осіб до його камер.

Що стосується порядку застосування засобів фото- та відеозапису на БпЛА слід зазначити, що 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.

Слід зазначити, що 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.¹

За фактами втрати або пошкодження портативного відеореєстратора чи карти пам'яті, відеореєстраторів, установлених на службових транспортних засобах, БпЛА складових стаціонарних та автомобільних систем, призначається та проводиться службове розслідування в установленому законодавством порядку.

¹ Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : наказ Міністерства внутрішніх справ України від 18.12.2018 р. № 1026. URL: <https://zakon.rada.gov.ua/laws/show/z0028-19#Text>

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: з портативних та відеореєстраторів, установлених у службових транспортних засобах, БпЛА, – 30 діб; з автомобільної або стаціонарної системи залежно від технічних характеристик – не менше 30 діб.

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.¹

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.²

¹ Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : наказ Міністерства внутрішніх справ України від 18.12.2018 р. № 1026. URL: <https://zakon.rada.gov.ua/laws/show/z0028-19#Text>

² Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : наказ Міністерства внутрішніх справ України від 18.12.2018 р. № 1026. URL: <https://zakon.rada.gov.ua/laws/show/z0028-19#Text>

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-камери.

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.¹

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.²

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 60.

² Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 61.

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 відеоспостереження¹

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.

Камери нічного бачення та тепловізори²

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.

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 62-63.

² Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 64-65.

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 камер¹

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

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 65-66.

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.¹

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. Малоімовірно, що поліцейський у прямому ефірі певної муніципальної відеокамери побачить, наприклад, крадіжку з вітрини вуличного магазину.²

До пристроїв обробки відеосигналів та відеозапису відносять: відеоквадратори, відеомультіплексори, 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 мультіплексорів систем відеоспостереження.

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 66.

² Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 66-67.

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.¹

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 спрацювання 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).

Відеомультіплексор – 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 відеомультіплексор дозволяє відобразити на одному екрані зображення відразу з декількох відеокамер. Наприклад, 16-канальний мультіплексор дозволить зобразити на моніторі зображення з 16 (або менше) камер. Взагалі слово мультіплексація означає об'єднання декількох каналів даних в один.

Так само відеомультіплексор 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») відеомультіплексор може працювати у наступних режимах (тут ми розглядаємо варіант, коли мультіплексор продовжив працювати у стандартному режимі).²

- 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.

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025.

² Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 67-68.

- Режим індивідуального налаштування. Оператор сам може настроїти порядок демонстрації зображень у разі виникнення тривожної ситуації. Також він може самостійно перемикає відображення сигналів із відеокамер.¹

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.

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 68-69.

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.¹

4.2. Системи відеоспостереження та відеоаналітики Державної прикордонної служби України

4.2.1. Система відеоспостереження Державної прикордонної служби України «ЗІР ПРО»

Комплекс відеоспостереження «ЗІР Про»: загальні відомості

Повномасштабна війна зумовила нагальну потребу ЗСУ в технологіях для дистанційного контролю території. Київські фахівці з Compass Engineering оперативно створили інноваційне рішення – комплекс «ЗІР Про» (ZIR Pro). Його унікальність полягає у використанні нейромереж та штучного інтелекту для ідентифікації противника, а модульна конструкція дозволяє легко його вдосконалювати.

Хронологія створення комплексу. 21–28 грудня 2023 р. відбулася перша велика публічна поява анонсу. Низка українських медіа опублікувала повідомлення про розробку комплексу ЗІР Про компанією Compass Engineering, з описом основних можливостей (оптика з 50-кратним збільшенням, сучасний тепловізор, нейромережі для відеоаналітики). Джерела: Rubryka, Shotam, сайт компанії. Рубрика+2#ШоТам+2. 22 грудня 2023 р. у системі ProZorro з'явилася процедура/опис закупівлі, де згадуються комплекти «Зір Про +» / «Зір +» як предмет закупівлі для місцевих/територіальних потреб (ID UA-2023-12-22-009136-a). Це свідчить про швидке опанування товару у держзакупівлях або застосування терміну в описах закупівель. У закупівельних описах також фігурують комплектні рішення для територіальної оборони. У 2024 р. відбулися тестування й прийняття на озброєння/використання. Державна прикордонна служба України проводила тестування рішень машинного зору/аналітики, а Compass Engineering у 2024 році повідомила про постачання пристроїв для виявлення БПЛА типу «Shahed». Серпень 2024 р. – повідомлення про передачу/донацію нових тепловізійних приладів від Compass Engineering для мобільних груп ДПСУ з метою детекції «Shahed» на відстанях до ~5 км. Публічні статті та репортажі вказують на еволюцію/модифікації комплексу або спрощених прицільних блоків. 2024–2025 рр. в ЗМІ та на сайті компанії фігурує інформація про подальшу розробку модулів аналітики, масштабування і

¹ Калугін В.Ю., Форос Г.В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. С. 69-70.

використання системи у тактичних сценаріях. Детальної публічної документації про етапи R&D, бюджет чи партнерів-підрядників не знайдено.

«ЗІР Про» використовує штучний інтелект для виявлення цілей і може використовуватись для цілевказання. Його ефективність забезпечується високоякісними сенсорами: оптичним зумом та тепловізійною камерою нового покоління, що дозволяє «бачити» ворога в умовах поганої видимості. Наприклад, система вже зарекомендувала себе у виявленні безпілотників «Шахед» вночі за 7 кілометрів. Наразі компанія продовжує роботу над розширенням можливостей комплексу.

Комплекс відеоспостереження ЗІР Про є зразком сучасного технічного рішення для реалізації безпеки об'єктів різного типу – від промислових зон до адміністративних будівель чи стратегічних пунктів. Його особливість полягає у використанні біспектральних PTZ-камер, що працюють як у видимому, так і в інфрачервоному діапазоні. Це дає змогу вести спостереження як вдень, так і вночі, а також у складних погодних умовах.

Комплект відеоспостереження «ЗІР Про+» призначений для виявлення спроб порушення режиму державного кордону України, а також для протидії потенційним спробам вторгнення, диверсійного проникнення, нелегальній міграції та контрабанді. Головна мета досягається шляхом цілодобового дистанційного оптичного і тепловізійного контролю за кордоном, що забезпечує моніторинг обстановки в реальному часі за будь-яких погодних умов. Пристрій сумісний з будь-яким FPV дроном-камікадзе. Оснащений власною камерою, підключається до польотного контролера і штатного VTX. Система ЗІР Про не потребує додаткового обладнання для дрона або пульта керування – управління здійснюється стандартним пультом.

Переваги системи ЗІР Про: зниження вимог до кваліфікації пілота, підвищена ефективність завдяки стійкості до засобів РЕБ після активації автопілота, точність ураження понад 95% та можливість ураження цілей на глибшій далині шляхом подолання радіогоризонту.



Рисунок 4.1 – Зовнішній вигляд комплексу ЗІР Про

Інтеграція з системами позиціювання на місцевості (GNSS¹), охорони периметру, автономного і резервного електроживлення робить ЗІР Про універсальним рішенням для комплексного захисту важливих об'єктів.

Основна мета комплексу ЗІР Про: забезпечити постійний відеоконтроль територій, оперативне реагування на будь-які загрози, автоматизоване збереження архіву подій, зручний доступ до даних для користувачів й адміністраторів (рис. 4.2).



Рисунок 4.2 – Ключові завдання комплексу ЗІР Про

Комплекс ЗІР Про надає такі можливості:

- 1) одночасна робота у видимому й тепловізійному режимі;
- 2) камери можуть обертатися у восьми напрямках, змінювати кут огляду та зум для детального спостереження;
- 3) система дозволяє вимірювати температуру об'єктів у кадрі, автоматично фокусуватись на цікавих ділянках;
- 4) ручний та автоматичний трекінг рухомих цілей, інтелектуальна реакція на визначені сценарії;
- 5) збереження фрагментів на сервер або SD-карту, можливість віддаленого перегляду;
- 6) розмежування прав доступу, журналізація дій операторів, захист облікових записів.

ЗІР Про використовується для охорони держустанов, складів, виробничих та промислових зон, приватних об'єктів, стратегічних

¹ GNSS (Global Navigation Satellite System) — це глобальна навігаційна супутникова система, комплекс електронно-технічних засобів, що складається з сукупності навігаційних супутників, наземної та приймальної апаратури. Вона призначена для визначення просторового положення об'єктів у географічній системі координат, часу, а також параметрів руху (швидкості, напрямку тощо) для об'єктів на землі, у морі та повітрі.

інфраструктур; на кордонах, в аеропортах, критичних об'єктах енергетики, транспортних вузлах; у місцях із високими ризиками (збройні конфлікти, пожежна небезпека, теракти). Структура комплексу та його компоненти Структура комплексу та його компоненти наведена на рис. 4.3.

Інтеграція з системами позиціонування дозволяє точно фіксувати розташування об'єктів та подій, що надзвичайно важливо для великих територій та рухомих цілей.

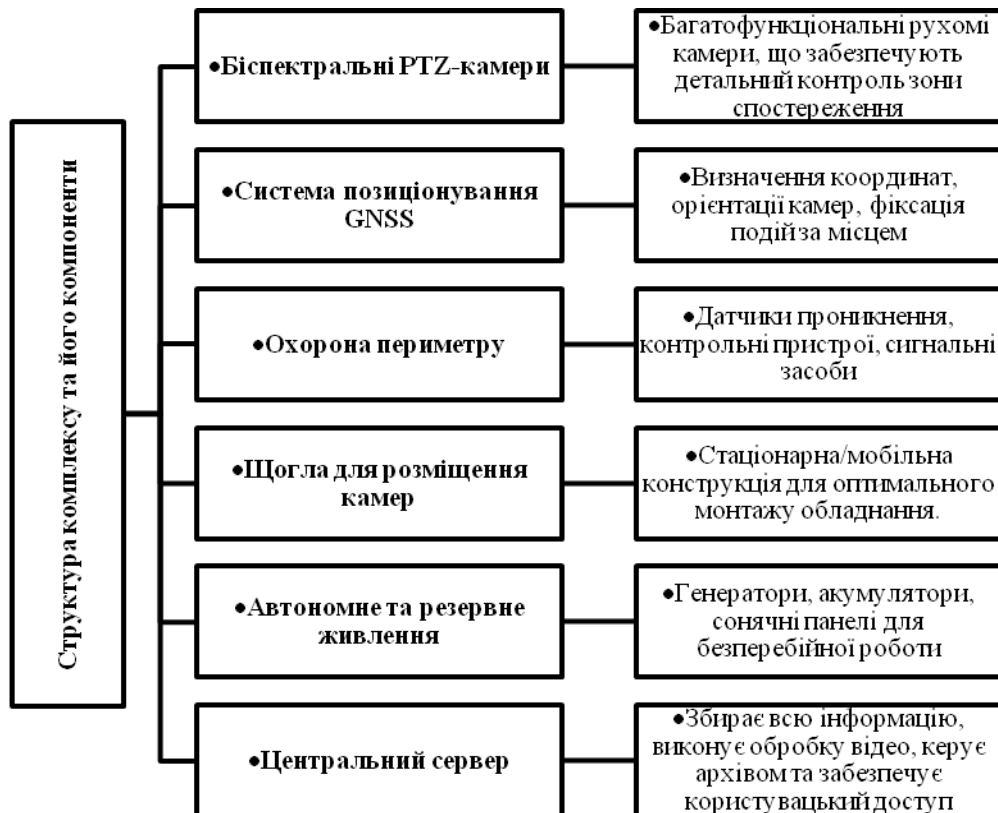


Рисунок 4.3 – Склад комплексу ЗІР Про

Система має багаторівневий захист – апаратний (заземлення, блискавкозахист), програмний (шифрування даних, фільтри IP). Комплекс підтримує додавання нових камер, датчиків, розширення архіву, інтеграцію нових алгоритмів. Спеціальні механізми забезпечують роботу у складних умовах: резервне живлення, антикорозійне покриття, погодостійкі матеріали.

Структура та апаратна архітектура комплексу «ЗІР Про».

Комплекс відеоспостереження ЗІР Про – це багаторівнева, модульна система, яка поєднує різні типи апаратних засобів і мережевого обладнання для організації безперервного цілодобового моніторингу об'єктів. Всі компоненти побудовані навколо центральних PTZ-камер, доповнених допоміжними засобами для підвищення ефективності відеоконтролю і безпеки.

Основні апаратні компоненти комплексу.

Біспектральна PTZ-камера є основою всього комплексу. Камера підтримує одночасне відеоспостереження у видимому та інфрачервоному (тепловізійному) спектрах. Робота PTZ (панорамування, нахили, зум) забезпечує максимально гнучкий огляд території. Параметри камери налаштовуються з WEB-інтерфейсу: вибір режиму (день/ніч), баланс білого, яскравість, контраст і багато іншого. Тепловізор дозволяє виявити людей, автомобілі чи інші об'єкти навіть уночі, крізь дим або негоду.

Система позиціонування GNSS використовує GPS/ГЛОНАСС¹ для точного визначення геолокації кожної камери. Реалізовано синхронізацію місцевих координат з архівом подій – це дозволяє швидко аналізувати переміщення і локалізувати інциденти.

Система охорони периметру реалізована через додаткові датчики руху (пасивні ІЧ-сповіщувачі), сигналізація, партія відеокамер для фіксації вторгнень/спроб проникнення. Може включати різні типи приймально-контрольних приладів, комунікаційні модулі (Ethernet, GSM), клавіатури, світлозвукові оповіщувачі, пам'ять подій.

Стаціонарна щогла спеціально розроблена для оптимального монтажу камер на потрібній висоті. Щогла має ряд монтажних опцій, антикорозійне покриття, захист від впливу зовнішніх чинників. Передбачено комплект для безпечної установки, заземлення, захисту від блискавки.

Інтегрована система автономного та резервного живлення здійснюється через акумулятори, генератори, сонячні станції. Ємність батарей, тип (Li-NMC, LiFePo4) – залежить від комплектації, забезпечує роботу без електромережі до 12 годин. Всі схеми монтажу електроживлення передбачають захист від короткого замикання, перенапруги, перегріву, балансування елементів.

Мережевий сегмент і комунікації. Комплекс об'єднано через мережу **Ethernet** (локальна мережа, комутатори, маршрутизатори), підтримуються TCP/IP, RTSP, HTTP, UPnP, Multicast, SNMP. Особливості: IP-фільтри дозволяють обмежити доступ до камер, використання динамічного DNS – для доступу через інтернет, налаштування PPPoE – для гібридних сценаріїв підключення. Можна налаштувати кількість підключень, вибрати потрібну схему потоків відео, задати параметри портів для інтеграції з іншими системами.

Монтаж та експлуатація. Важливо забезпечити оптимальне місце установки – висота, огляд, підведення кабелів. Встановлення щогли і монтаж кронштейнів проводиться з дотриманням вимог безпеки та захисту від погодних умов. Перед підключенням перевіряється якість з'єднань, коректність монтажу, наявність всіх комплектуючих.

Монтаж системи живлення. Акумулятори/генератори монтують окремо від основного обладнання (техніка, шафи з термоізоляцією). Сонячні

¹ GPS (Global Positioning System) і ГЛОНАСС (Глобальна навігаційна супутникова система) – це дві глобальні супутникові навігаційні системи, які призначені для визначення точного місця розташування, швидкості та часу об'єктів на поверхні Землі або в атмосфері.

панелі розміщують на ділянках з оптимальним рельєфом, монтують у систему, здатну швидко демонтуватись, очищується від іржі за рахунок цинкового покриття. Передбачена система блискавкозахисту (ізолюваний блискавкоприймач), заземлення, система захисту від перенапруги, несприятливих факторів.

Комплекс підтримує розширення – додаткові камери, датчики, нові модулі. Передбачені різні схеми електроживлення (мережа, автономія, резерв). Вся апаратура сертифікована відповідно до стандартів безпеки, розроблена з урахуванням сучасних вимог до довготривалої роботи у складних умовах.

Взаємодія між компонентами. Камери передають відео на сервер обробки даних, де це зберігається, архівується, аналізується з допомогою програмного забезпечення. Датчики периметру інтегруються із відеосистемою для автоматичної фіксації та реакції на події. GNSS-модуль ідентифікує положення камер і подій, щогла забезпечує безпечну висоту монтажу, система живлення відповідає за безперебійну роботу. Сповіщення передаються оператору, автоматично записуються у архів подій.

Програмне забезпечення та інтерфейс користувача комплексу ЗІР Про

Доступ до основних налаштувань здійснюється через веб-інтерфейс з будь-якого браузера, вводячи IP-адресу пристрою. При першому вході потрібно встановити захисний веб-плагін. За замовчуванням використовується адміністраторський обліковий запис (admin/admin); при первинному вході система ініціює зміну пароля для безпеки.



Рисунок 4.4 – Інноваційний комплекс тепловізійного спостереження ЗІР Про

Головне меню містить розділи (рис. 4.4): попередній перегляд (реальний час); системне меню; конфігурація камер і мережі; налаштування PTZ; управління подіями та архівом.

Інтерфейс перегляду містить: панелі відеопотоків з різних каналів; контекстні кнопки для масштабування, фокусування, моментального знімка, запуску запису; модулі виміру температури (для тепловізійних каналів), виділення областей фокусування; PTZ-консоль (обертання по 8 напрямках, зум, фокус, швидке позиціонування, патрулювання, пресети); керування аудіо та інтерком.

Режим «Попередній перегляд» дозволяє оцінити поточну ситуацію на об'єкті в реальному часі, якісно контролювати проблемні зони, а також швидко реагувати на інциденти.

Налаштовуються профілі (день/ніч), яскравість, контраст, насиченість, різкість, гамма-корекція та рівень шумозаглушення. Передбачено режими електронної стабілізації, зміна напрямку відображення, робота з балансом білого та компенсацією заднього підсвічування.

Для тепловізійного каналу можна змінювати палітру, налаштовувати масштаби, вибирати режим фокусування (ручний/авто), керувати чутливістю та компенсацією за туманних умов.

Відеокодек і потоки підтримує H.264/H.265/MJPEG, задаються роздільна здатність, частота кадрів, тип бітрейту, якість, інтервали ключових кадрів, включення/виключення підпотоків для оптимізації навантаження на мережу або зберігання.

Передбачено встановлення масок конфіденційності, відображення часу, каналу, OSD-індикації, накладання логотипів, відображення стану PTZ (координати, зум), повідомлення про події. Користувач може визначити пріоритетні області кадру для підвищеної якості запису – наприклад, зони входу, ворота, проїзди.

Камера підтримує TCP/IP, RTSP для потокового відео, має функції DDNS для роботи з динамічними адресами, PPPoE для прямого підключення до провайдера, Multicast для багатокористувацького доступу, UPnP для автоматичної мережевої конфігурації. Доступні IP-фільтри, SNMP для віддаленого моніторингу та управління.

Управління подіями (аналітика подій та тривоги). Окремий розділ інтерфейсу призначений для налаштування сценаріїв реагування:

виявлення руху, налаштування області чутливості, фільтри хибних спрацювань (“Anti-Dither”);

виклик спалаху/сирени, створення і затримка тривожних записів;

зв'язок тривоги із PTZ-функціями (камери автоматично наводяться на зум або пресет);

сповіщення електронною поштою, інтеграція з релейними пристроями.

Управління архівом та сховищем даних. Можливість розкладу запису, вибору носія (SD-карта, FTP, NAS), очищення і архівування даних, резервне копіювання. Записи підтримуються як за розкладом, так і за сценаріями (наприклад – по тривозі чи детекції руху).

Адміністрування, керування доступом та обслуговування. WEB-інтерфейс містить розділ управління користувачами – створення груп, розмежування прав (адміністратор, оператор, гість), ведення журналу подій, аудит дій користувачів. Є функції резервного копіювання конфігурацій, оновлення прошивки камер і системних модулів, автоматичне планування перезавантаження та очищення журналів.

Програмне забезпечення ZIR-Pro охоплює весь спектр налаштувань та дій – від базової роботи з відеопотоками, PTZ-контролю і налаштування камер до аналітики подій, управління архівами та адміністративних функцій. Політика безпеки передбачає персоніфікацію доступу, ведення аудиту і резервування налаштувань для швидкого відновлення працездатності.

Тактико-технічні та якісні характеристики комплексу відеоспостереження ЗІР Про+

Головна мета розгортання комплексу ЗІР ПРО+ полягає у виявленні спроб порушення режиму державного кордону України. Крім того, комплекс призначений для ефективної протидії потенційним спробам вторгнення, диверсійного проникнення, нелегальній міграції та контрабанді. Функціональність комплексу реалізується шляхом цілодобового дистанційного оптичного і тепловізійного контролю за кордоном. Це забезпечує можливість моніторингу обстановки на державному кордоні в реальному часі за будь-яких погодних умов.

Комплект відеоспостереження «ЗІР ПРО+» являє собою набір засобів та приладдя, необхідних для розгортання системи та пристроїв нагляду та охорони.

Система включає шість основних взаємопов'язаних компонентів:

1. Щогла з платформою для встановлення камери. Конструкція операторського класу призначена для експлуатації у відкритому середовищі та має бути оснащена системами захисного заземлення й блискавкозахисту.
2. Система зв'язку, що забезпечує стабільне бездротове підключення для критично важливих застосувань і підтримує режими Wi-Fi 6 та робочого моста (WGB).
3. Комплекс охорони периметра.
4. Система заземлення та блискавкозахисту.
5. Інтегрована система автономного й резервного електроживлення.
6. Кабеленесучі елементи та кабельно-провідникова інфраструктура, необхідні для монтажу та підключення обладнання.

Усі компоненти мають відповідати суворим вимогам, забезпечуючи безпеку товару та його технічні, якісні характеристики відповідно до встановлених норм. Якщо в документації зазначена конкретна торговельна марка, допускається постачання еквіваленту, технічні характеристики якого не повинні бути гіршими за заявлені.

Тактико-технічні характеристики основних підсистем

Детальні технічні вимоги до кожного компонента комплексу «ЗІР ПРО+» обґрунтовані у контексті необхідності забезпечення ефективності та надійності системи в польових умовах.

1. Щогла з площадкою для кріплення камери

Щогла повинна належати до обладнання операторського класу та бути придатною для встановлення в умовах відкритого середовища. Її конструкція обов'язково має включати систему захисного заземлення та блискавкозахисту, виконані відповідно до чинних українських норм і стандартів.

Основні характеристики	Вимоги
Тип	Щогла
Застосування	Вуличне
Висота	36 м
Матеріал	Придатний для тривалого вуличного використання (Алюмінієвий сплав/ Оцинкована сталь/Фарбована сталь)
Кількість секцій відтяжок	6 шт.
Максимальне вітрове навантаження	30 м/сек
Номінальне навантаження	150 кг
Температура експлуатації	Від –40°C до +50°C

2. Система зв'язку. Комунікаційний модуль має забезпечувати стабільне та надійне бездротове підключення, придатне для критично важливих завдань. Він повинен підтримувати роботу в різних режимах, зокрема Wi-Fi 6, робочого моста (Working Group Bridge, WGB) або у форматі безперервного бездротового з'єднання. Використовуване обладнання повинно бути сумісним з електронною комунікаційною мережею Державної прикордонної служби України, а також мати можливість перемикання в режим стандартного Wi-Fi за потреби.

Система зв'язку включає направлену антену для максимального підсилення та охоплення частот промислових бездротових застосунків, дві точки доступу, два інжектори живлення, чотири радіочастотні кабелі, а також маршрутизатор з функціями безпеки та комутатор на 8 портів Fast Ethernet.

Характеристики точки доступу. Точки доступу мають підтримувати режими Wi-Fi 6 (802.11ax) та WGB. Підтримка 4x4 MIMO та до чотирьох просторових потоків (2.4 ГГц 4x4: канали 20 МГц; 5 ГГц 4x4: канали 20, 40, 80 МГц; 5/6 ГГц 4x4: канали 20, 40, 80, 160 МГц). Підтримка Мультигігабітного Ethernet (два порти зі швидкістю не менш 5 Гбіт/с). Вбудований приймач GNSS. Можливість налаштування контролеру ключової інформації РТК/GTK. Підтримка безпеки передачі даних за рахунок шифрування AES. Підтримка

TDMA та CSMA механізмів розподілу доступу до радіополоси. Керування потужністю точки доступу з можливістю автоматичного зменшення споживаної потужності при зменшенні навантаження клієнтів. Передбачено режим сну для клієнтів (активація лише в цільові моменти).

Маршрутизатор з функціями безпеки. Маршрутизатор повинен мати промислове виконання та модульну архітектуру з можливістю розширення не менш ніж двома модулями.

Характеристики основного пристрою	Вимоги
Номінальне живлення	від 12В
Порти	Комбо-порт 10/100/1000 GE (RJ45 чи SFP) + 4 порти 10/100BASE-T Fast Ethernet
Інтерфейси	Порт RS232, Порт вхідної сигналізації, Консольний порт Mini type-B USB
Модем	Слот для встановлення dual-active 3G/4G/LTE модему
Додатково	Вбудований GPS
Умови експлуатації	Від –40 до +60°C

Можливості програмного забезпечення (маршрутизатор). Сегментація (VPN, VRF, VLAN), підтримка DHCP, Netflow, QoS, ACL, а також протоколів маршрутизації (RIP, OSPF, EIGRP – RFC 7868, IGMP, IP). Побудова шифрованих тунелів з підтримкою стандартів Next Generation Encryption та Quantum Computer Resistant алгоритмів, IPSec, IKEv2. Підтримка криптографічної верифікації автентичності програмного та апаратного забезпечення. Підтримка вбудованого механізму генерування подій та реакцій з використанням скриптової мови автоматизації. Можливість роботи в SDWAN архітектурі.

Комутатор. Комутатор на 8 портів Fast Ethernet також має бути на модульній платформі з можливістю розширення не менш ніж двома модулями. Він підтримує ключові механізми безпеки, включаючи port security, BPDU guard, Storm Control, RADIUS та TACACS клієнт, MAC Authentication Bypass. Також підтримується управління через Веб-інтерфейс, VLAN, IGMP, DHCP snooping, STP, LLDP, Etherchannel та SNMP v2/v3.

3. Система охорони периметру. Система охорони периметру призначена для захисту щогли та змонтованого на ній обладнання від несанкціонованого доступу. Система складається з приймально-контрольного приладу (ПКП), клавіатури, комунікаційного Ethernet-модуля, двох оглядових відеокамер, двох карт пам'яті microSD class 10 (256 Гб) та сповіщувачів.

Характеристики ПКП: дротові зони – до 16; програмовані виходи – до 16; модулі розширення – до 64; обов'язкова наявність модулів підключення бездротових датчиків та модулів зв'язку для роботи в мережі Ethernet;

джерело живлення ПКП має забезпечувати автономну роботу протягом не менше 12 годин (за рахунок акумулятора та ДБЖ).

Характеристики оглядових відеокамер:

роздільна здатність – 6 Мп (2048 x 2048);

тип – Fisheye;

чутливість – 0.1 Люкс;

дальність підсвічування – 15 м;

стиснення відео – H.264/H.265/MJPEG;

цифрове PTZ – 8-кратне;

захист – Ударостійкість IK10 та Ступінь захисту IP66.

Сповіщувачі (Пасивний інфрачервоний):

горизонтальне виявлення – кут 180°;

максимальна відстань виявлення – не менше 12 м;

кількість зон детекції – горизонтальна (14) та нижня (14) зон;

підтримка антимаскінгу та регулювання чутливості;

робочий діапазон температури – від -25°C до +60°C.

4. Система блискавкозахисту та заземлення. Ця система забезпечує захист обладнання й особового складу від небезпечних проявів атмосферної електрики. Для побудови комплексу необхідно використовувати блискавкоприймач ізольованого типу заввишки щонайменше 4 м.

Основні елементи та технічні вимоги такі: ізольований блискавкоприймач висотою не менше 4 м; струмовідвід із гарячеоцинкованої сталі діаметром щонайменше 8 мм; заземлювальні стрижні діаметром від 16 мм і довжиною не менше 1,5 м, з безмуфтовим способом з'єднання, виготовлені з гарячеоцинкованої сталі; металева полоса перерізом не менше 25×4 мм із того ж матеріалу. Комплекс також має включати зовнішні та внутрішні пристрої захисту від перенапруг, установлені згідно з вимогами чинних нормативних документів.

5. Інтегрована система автономного та резервного електроживлення. Комплекс має забезпечувати безперервне енергоживлення всіх елементів системи спостереження та бути адаптованим до автоматизованої роботи в умовах зовнішнього розміщення. Конструкція повинна містити повний комплект обладнання, необхідного для стабільного основного та резервного живлення впродовж усього циклу роботи.

Ключові вимоги та складові. Корпус обладнання має відповідати класу захисту від вологи та пилу не нижче IP54. Охолодження повинно здійснюватися через активну припливно-витяжну систему з автоматизованим керуванням і фільтрацією повітря. Підігрів – активний, автоматичний, із використанням інтегрованих датчиків контролю. Конструкція корпусу має забезпечувати підвищений рівень фізичного захисту, не нижче триточкового механізму фіксації, із вологостійким замком. Кріпильні елементи повинні дозволяти встановлення на будь-яких типах ґрунтів та забезпечувати швидкий процес монтажу й демонтажу.

Елементи живлення та керування. Джерела енергії включають шість сонячних панелей, кожна з яких має потужність не менше 550 Вт, а їх

встановлення здійснюється на наземній або консольній конструкції. Інвертор із потужністю не менше 1000 Вт повинен забезпечувати режим прискореного заряджання акумуляторних батарей. Генератор потужністю від 2000 Вт, бензиновий, однофазний (220 В, 50 Гц), має бути оснащений системою автоматичного запуску та керування. Для нього передбачається окремий корпус і відсік для пального об'ємом щонайменше 30 л. Типи акумуляторних елементів – Li-NMC або LiFePO₄.

Система керування батареями (BMS) повинна забезпечувати повний спектр захисту: від перезаряду, надмірного розряду, короткого замикання, перегріву, а також підтримувати балансування напруги між осередками. Передбачено можливість дистанційного керування, моніторингу роботи споживачів і технічних систем. До складу входить промисловий модуль зв'язку, що підтримує стандарти 2G, 3G, 4G та LTE.

Комплекс відеоспостереження «ЗІР ПРО+» функціонує як автономний кібернетичний вартувий. Висока щогла (36 м) є його «оком» (платформою для зору), яке працює незалежно завдяки потужній системі живлення (сонячні панелі та резервний генератор). Маршрутизатор та точки доступу утворюють його «нервову систему», яка швидко та безпечно передає інформацію (через Wi-Fi 6 та шифровані тунелі), а система охорони периметру з датчиками та камерами виконує роль його «шкіри» та «рефлексів», захищаючи самого вартового від зовнішніх загроз.

Порівняння тактико-технічних характеристик комплексу відеоспостереження ЗІР Про з типовими закордонними аналогами

У сучасних системах безпеки та спостереження біспектральні комплекси, що поєднують тепловізійні та оптичні канали, відіграють ключову роль у забезпеченні ефективного моніторингу в умовах обмеженої видимості. Український комплекс «ЗІР Про» від ZIR Robotics позиціонується як універсальне рішення для прикордонної та тактичної охорони, з акцентом на високу роздільну здатність і інтеграцію з мобільними платформами. У цій статті ми порівнюємо його з трьома типовими закордонними аналогами в різних сегментах ринку: комерційними PTZ-модулями (Teledyne FLIR PT-Series), промислово-периметровими тепловими камерами з PTZ (Hanwha Wisenet TNU-4041T) та високопродуктивними військовими EO/IR-системами (HENSOLDT NightOwl M). Порівняння базується на ключових параметрах, таких як роздільна здатність сенсорів, зум, дальність виявлення та стабілізація, з короткими коментарями щодо призначення.

1. Комерційні PTZ біспектральні модулі: Teledyne FLIR PT-Series HD

Ця лінійка орієнтована на захист критичної інфраструктури, де потрібна надійна робота в темряві, яскравому сонці чи несприятливих погодних умовах. FLIR PT-Series HD – це стабілізований dual-sensor PTZ-комплекс з акцентом на комерційну доступність і інтеграцію з системами керування, такими як FLIR United VMS. Він підходить для промислових об'єктів, аеропортів та портів, де пріоритет – автоматизоване відстеження цілей.

Параметр	ЗІР Про	Teledyne FLIR PT-Series HD
Теплова роздільна здатність	1280 × 1024	640 × 480
Оптична роздільна здатність	4 Мп ($\approx 2560 \times 1440$)	1080p HD (1920×1080)
Оптичний зум (тепловий/видимого)	3× (25–75 мм фокусна відстань) / 50×	14× / 30× (з 12× цифровим)
Дальність виявлення	До 6 км (лазерний далекомір)	До 3–5 км (залежно від моделі, для транспортних засобів)
PTZ-функціонал	Стабілізований позиціонер з поворотом 360°	Pan: 360° безкінечний, Tilt: +90° до -90°; швидкість до 60°/с
Чутливість теплового сенсора	Не вказано (VOx мікроболометр)	<35 mK @ 25°C

ЗІР Про перевершує FLIR за роздільною здатністю теплового каналу, що забезпечує кращу деталізацію на середніх дистанціях, тоді як FLIR виграє в швидкості PTZ і чутливості для комерційних сценаріїв. Обидва комплекси стабілізовані, але FLIR акцентує на автоматизованому трекінгу. Джерела: ZIR Robotics (офіційний сайт), Teledyne FLIR (продуктова сторінка).

2. Промислові/периметрові теплові камери з PTZ/позиціонером: Hanwha Wisenet TNU-4041T

Hanwha Wisenet thermal PTZ серії TNO/TNU призначена для периметрової охорони промислових зон, портів та гірничовидобувних об'єктів, де критична 24/7-детекція людей і техніки в умовах низької освітленості. Модель TNU-4041T фокусується на фіксованому тепловому лінзі для довготривалого моніторингу великих територій, з підтримкою H.265 для ефективного стиснення.

Параметр	ЗІР Про	Hanwha Wisenet TNU-4041T
Теплова роздільна здатність	1280 × 1024	640 × 480 (з опціями 640×360, 320×240)
Оптична роздільна здатність	4 Мп ($\approx 2560 \times 1440$)	Відсутня (чисто тепловий)
Оптичний зум (тепловий/видимого)	3× (25–75 мм) / 50×	Фіксований 19 мм (HfOV 32°) / Немає
Дальність виявлення	До 6 км (лазерний далекомір)	До 3,157 м (для транспортних засобів)
PTZ-функціонал	Стабілізований позиціонер з поворотом 360°	Pan: 360° безкінечний, Tilt: -90° до +40°; швидкість до 120°/с (pan)
Чутливість теплового сенсора	Не вказано	<50 mK (NETD)

ЗІР Про пропонує біспектральність і вищу роздільну здатність, роблячи його гнучкішим для тактичних завдань, тоді як Hanwha оптимізована для чисто теплового периметрового сканування з акцентом на швидкість PTZ і низьке енергоспоживання. Hanwha дешевша в експлуатації для промисловості, але поступається в дальності. Джерела: ZIR Robotics (офіційний сайт), Hanwha Vision (продуктова сторінка).

3. Військові/високопродуктивні EO/IR комплекси: HENSOLDT NightOwl M

HENSOLDT NightOwl M –це модульна стабілізована турель EO/IR для оборонних платформ, з турбогіростабілізацією та інтеграцією в C2-системи. Вона призначена для ISTAR-операцій (розвідка, спостереження, наведення), включаючи морську та наземну охорону кордонів, з фокусом на екстремальні дальності в бойових умовах.

Параметр	ЗІР Про	HENSOLDT NightOwl M
Теплова роздільна здатність	1280 × 1024 (LWIR)	HD (MWIR, точна не вказано; опціонально >640×512)
Оптична роздільна здатність	4 Мп (≈ 2560 × 1440)	HD low-light (денний канал)
Оптичний зум (тепловий/видимого)	3× (25–75 мм) / 50×	Високий зум (до 11× для IR, екстремальний для EO)
Дальність виявлення	До 6 км (лазерний далекомір)	До 40 км (DRI для кораблів/цілей)
PTZ-функціонал	Стабілізований позиціонер з поворотом 360°	Точна стабілізована PT-одиниця (360° азимут, повний елеваційний діапазон)
Чутливість теплового сенсора	Не вказано	Оптимізована для низької видимості (MWIR)

ЗІР Про конкурує за роздільною здатністю, але HENSOLDT домінує в дальності та стабілізації для військових платформ, з лазерним далекоміром і авто-трекінгом. ЗІР Про – бюджетніша альтернатива для тактичних підрозділів, тоді як NightOwl M –для стратегічного рівня з інтеграцією AI. Джерела: ZIR Robotics (офіційний сайт), HENSOLDT (продуктова сторінка).

Узагальнена порівняльна таблиця ключових ТТХ комплексу ЗІР Про з аналогічними системами

Параметр	3IP Про (Україна)	Teledyne FLIR PT-Series (закорд.)	Hanwha Wisenet thermal/PTZ (закорд.)	HENSOLDT EO/IR (високий клас)
Тепловізійний детектор	заявлено 1280×1024 640×512 залежно від конфігурації	типово 640×480 (uncooled VOx) у PT-Series; є модифікації	різні моделі: прикладні теплові матриці в серії – 640×512/384×288; фокусні лінзи 13/19/35 мм; виявлення авто до ~3157 м у рекламі	широкий спектр: MWIR/SWIR/LWIR детектори, високі роздільності для військових задач; модульні заміни детекторів можливі
Оптична (видима) камера	~4 МР (у описах) з ~50× оптичним зумом	Visible: 1080p або 4K в новіших моделях; оптичні зуми від ~4× до 30–60× залежно від опції	Видимі / NIR модулі доступні; PTZ-ринок Hanwha має високі оптичні зуми для серії PTZ (залежно від моделі)	Висока оптична роздільність, часто професійні телеоб'єктиви; призначені для далекого виявлення та ідентифікації
Лазерний далекомір (LRF)	заявлено LRF до ~6 km (у ТТЗ/описах)	Деякі конфігурації PT-Series можуть мати LRF як опцію (залежить від збірки)	Деякі промислові/спеціальні моделі мають LRF-опції; але типово – немає в базових термальних камерах	В арсеналі військових EO/IR – LRF як стандарт/опція з дальностями, що можуть перевищувати десятки км залежно від калібру та умов
Призначення / застосування	Прикордонні/тактичні задачі, периметр, мобільні платформи; комплект поставки включає щогли/живлення	Критична інфраструктура, аеропорти, порти, охорона – стаціонарні розгортання	Периметр/інфраструктура, промислові майданчики, логістика	Тактичні/стратегічні розвідка, інтеграція на бронетехніку й морські платформи
Аналітика (відео/ШІ)	Є модулі відео-аналітики (виявлення людей, техніки, фільтрація хибних спрацьовувань)	Підтримка AI/VI в нових серіях (інтеграція з VMS, аналітика)	Має вбудовані алгоритми виявлення/тривоги для периметра	Високорівнева обробка, turbulence correction, stabilisation, іноді інтеграція з системами розпізнавання/цілеукладкою
Ціновий/клас продукту	Націлений на тактичний /державний сегмент; ціна залежить від конфігурації (комплект щогл/постачання)	Комерційний преміум-клас (ціни – десятки тисяч \$ за конфігурацію)	Комерційний/промисловий сегмент (помірні до преміум цін залежно від опцій)	Високовартісні військові системи, контрактні поставки оборонним структурам

Примітка: виробники дають багато варіантів конфігурації –тому порівняння тут робиться за типовими/публічними конфігураціями, приведеними у відкритих джерелах. Детальні ТТХ потрібно зіставляти по конкретних моделях/модифікаціях.

Як підсумок, ЗІР Про демонструє конкурентоспроможність у комерційному та промисловому сегментах завдяки високій роздільній здатності та біспектральності, але для військових завдань поступається в дальності HENSOLDT. Вибір залежить від сценарію: для прикордонної охорони ЗІР Про –оптимальний баланс ціни та продуктивності.

Типові задачі користувача комплексу ЗІР Про

Підготовка до експлуатації. Перед початком роботи оператору необхідно перевірити правильність монтажу камер, наявність живлення, підключення до мережі, відкрити WEB-інтерфейс, пройти авторизацію, змінити пароль за замовчуванням з міркувань безпеки та ініціалізувати всі пристрої та провести самотестування.

Основні налаштування камер. Вибрати профіль («день», «ніч», «звичайний»), відрегулювати яскравість, контраст, насиченість, різкість, параметри гамма-корекції та шумозаглушення. Налаштувати експозицію (автоматичний, ручний, пріоритет діафрагми, затвора, посилення), коефіцієнти компенсації заднього освітлення та баланс білого з урахуванням специфіки локації. Встановити режим кольорового чи чорно-білого зображення, рівень чутливості перемикання день/ніч.

PTZ-керування. Використання PTZ-консолі для повного управління положенням камери: панорамування, нахили, зум, автоматичне фокусування. Збереження пресетів та створення маршрутів патрулювання, організація лінійного сканування чи автопанорамування для покриття всього периметру. Вибір та запуск шаблонів патрулювання залежно від типу об'єкта та задач спостереження.

Керування подіями та тривогами. Встановлення зон детекції руху, налаштування чутливості, фільтрація хибних спрацювань («Anti-Dither»). Автоматична реакція на тривогу: запуск спалаху, сирени, архівація фрагменту відео, відправка email-сповіщення. Прив'язка тривог до PTZ-функцій для автоматичної переорієнтації/зуму на зону події.

Робота з архівом та сховищем даних. Організація розкладу запису на сервер, SD-карту, FTP або NAS. Встановлення циклічного запису, автоочищення «старих» фрагментів для підтримки безперервної роботи сховища. Пошук і перегляд відео за датою, подією або ключовими зонами, експорт необхідних фрагментів для аналізу чи використання у правоохоронних/службових процедурах.

Адміністрування доступу та основні процеси обслуговування. Створення користувачів і груп з різними рівнями прав – адміністратор, оператор, гість. Контроль онлайн-з'єднань, аудит дій користувачів, журналізація змін і подій. Організація резервного копіювання конфігурацій,

оновлення прошивки, планове перезавантаження та очищення журналів. Керування периферією (склоочисники, релейні виходи), налаштування планування їхньої роботи.

Реалізація задач у ЗІР Про побудована на принципах максимального автоматизму, надійності та гнучкості. Оператор має інструменти для тонкого налаштування та ефективного реагування на широкий спектр сценаріїв, забезпечуючи високий рівень інформаційної та фізичної безпеки об'єкта.

Практичні приклади роботи оператора з комплексом ЗІР Про

Початок роботи та підготовка системи. Перш ніж розпочати експлуатацію, оператор повинен виконати ряд обов'язкових дій: перевірити фізичне підключення камер, стан мережі, наявність живлення і цілісність монтажних вузлів; провести зовнішній огляд камер та периметральних пристроїв на предмет забруднення, ушкоджень, впливу погодних чинників; підключитися до WEB-інтерфейсу з авторизованого пристрою, здійснити базове самотестування всіх вузлів системи; оновити програмне забезпечення до актуальної версії, перевірити ліцензії й налаштування IP-адрес за документацією.

Типові ситуації реагування оператора

Моніторинг об'єкта у режимі реального часу. Оператор використовує функцію багатокамерного огляду для контролю периметра та ключових об'єктів. При виявленні підозрілої ситуації застосовується миттєве PTZ-керування: зміна ракурсу, масштабування для наближення деталей. Запускається ручний трекінг цілі через тепловізійний канал для перевірки руху поза межами видимої частини.

Виявлення та фіксація інциденту. При спрацюванні детекторів руху або периметральної сигналізації система автоматично виконує:

- архівацію відповідних фрагментів відео,
- світлове/звукове оповіщення персоналу,
- автоматичну зміну положення камери на запрограмовану пресетну точку,
- відправку сповіщення електронною поштою за підпискою.

Пошук і аналіз подій у архіві. Використовується пошук записів за ключовими параметрами: час, зона, тип події (рух, тривога, ручне збереження). Фрагменти відео можна завантажити для передачі правоохоронним органам або проведення внутрішнього розслідування. Здійснюється порівняльний аналіз зміни обстановки на різних часових етапах для уточнення сценаріїв подій.

Обслуговування та типові процедурні завдання

Регулярний технічний огляд. Один раз на місяць здійснюється перевірка стану об'єктивів, очистка лінз, контроль герметичності корпусів камер, перевірка антикорозійних покриттів щогли. Тестування резервного живлення (акумуляторів, генераторів), перевірка контакту заземлення, працездатності блискавкозахисту.

Відновлення та профілактика програмного забезпечення. Періодичне створення резервних копій конфігурацій, відновлення «заводських» налаштувань у разі некоректної роботи. Оновлення версій мікропрограм камер, мережевих модулів та серверної частини. Перевірка журналу подій та аудит прав доступу.

Робота з несправностями та збої системи. При виявленні втрати відеопотоку перевіряється підключення живлення, стан мережі, справність комутуючого обладнання. У разі провалу підключення до WEB-інтерфейсу перевіряються локальні IP-адреси, конфігурація маршрутизаторів, справність мережевих карт. Локалізація збоїв у записі відео – перевірка вільного простору, статусу сховища (SD-карта, NAS чи FTP), журналу помилок системи.

Типові помилки та заходи з відновлення роботи. При помилках мережевого підключення необхідно оновити IP-адресу, переконатись у відсутності конфлікту адрес, протестувати кабелі. У разі відмови PTZ-керування необхідно перезапустити модуль руху, перевірити наявність фізичних завад, виконати «Lens Init» через інтерфейс. При збоях архіву необхідно включити режим циклічного перезапису або очистити неактуальні дані, провести дефрагментацію носія.

Практичний досвід роботи із ЗІР Про формується на основі регулярного контролю, належного реагування на всі сценарії розвитку подій, дотримання процедур технічного обслуговування і швидкого відновлення функціональності системи у разі виникнення несправностей.

Поради та рекомендації щодо експлуатації комплексу ЗІР Про

Основні вимоги до експлуатації біспектральної PTZ-камери

Підготовка до роботи. Перед монтажем камери перевірити середовище встановлення: уникати зон із сильними електромагнітними завадами, забезпечити захист від впливу агресивних атмосферних факторів і механічних ушкоджень. Ретельно підготувати кабелі: використовувати сертифіковані силові та мережеві кабелі із захистом від перешкод, забезпечити правильне шинування й заземлення. Підготувати всі необхідні інструменти згідно з настановою, застосовувати оригінальну упаковку для зберігання й транспортування компонентів.

Монтаж та перевірка. Дотримуватись рекомендованих схем прокладання кабелів, схем монтажних кронштейнів, засобів захисту від корозії та вимог щодо водонепроникності. Після інсталяції провести самотестування камери, перевірити ініціалізацію PTZ, коректність зміни напрямків, масштабування та фокусування. Особливу увагу приділити системі блискавкозахисту, заземленню, резервним джерелам живлення.

Важливі повідомлення про безпеку. Завжди змінювати стандартний пароль адміністратора та регулярно оновлювати паролі облікових записів. Обмежувати права доступу: створювати окремі групи користувачів з мінімально необхідними повноваженнями. Слідкувати за актуальністю прошивки камер, серверного забезпечення, антивірусного захисту комп'ютерів операторів.

Враховувати ризики, пов'язані зі зберіганням даних у хмарних сервісах, для критично важливих об'єктів використовувати локальне сховище. Всі дії з нарощуванням/заміні елементів здійснювати лише у вимкненому та знеструмленому стані, відповідно до настанови виробника.

Встановлення камери: інструкція та нюанси. Перед установкою перевірити повний комплект виробу та аксесуарів: інструменти, кабелі, кронштейни, герметики, комплекти захисту. Організувати прокладання кабелів так, щоб мінімізувати механічний вплив та захистити від пошкоджень тваринами, гризунами, погодними факторами. Монтажний кронштейн повинен бути встановлений строго горизонтально, з дотриманням рекомендацій по висоті, кутах огляду й зонах патрулювання.

Експлуатація та системний контроль. Регулярно проводити перевірку працездатності всіх компонентів: камери, датчики, щогли, модулі живлення, сховище. Дотримуватись динаміки профілактичного огляду: раз на місяць очищення об'єктів, тест резервного живлення, аудит журналу подій. Оновлювати конфігурацію, резервувати й дублювати важливі налаштування у захищені архіви. У разі появи нестандартних подій/збоїв негайно ініціювати процедури діагностики: перевірка кабелів, переналаштування мережі, відновлення заводських налаштувань.

Типові помилки, які призводять до збоїв, та способи їх уникнення. Залишення типових паролів – підвищує ризик несанкціонованого втручання. Встановлення камер занадто низько або з «мертвими зонами» знижує ефективність відеоконтролю. Ігнорування резервного копіювання конфігурацій ускладнює швидке відновлення системи при збоях. Недостатній догляд за оптикою призводить до погіршення якості відеозапису (запотівання, бруд, корозія). Некоректне шинування, погане заземлення підвищує ризик виходу з ладу електроніки через перенапругу.

Оптимізація відеоспостереження. Для цього необхідно вивчати WEB-інтерфейс та всі функціональні можливості для ефективного використання PTZ, налаштування зон детекції та автоматизації роботи комплексу. Впроваджувати систему моніторингу на основі журналу подій, логів, аудитів дій користувачів, ведення статистики інцидентів і оцінки ризиків. Для відповідальних користувачів (адміністрація, IT-відділ) рекомендується розрахувати необхідний обсяг сховища, канали резервного копіювання, інтеграцію з іншими системами безпеки.

Системний контроль, своєчасна профілактика, безпека паролів і прав доступу, якісний монтаж і грамотне адміністрування – це основа продуктивної роботи комплексу ЗІР Про і запорука створення сучасної, безпечної інфраструктури відеомоніторингу.

Рекомендації щодо впровадження, інтеграції та розширення комплексу ЗІР Про

Перед впровадженням слід виконати детальний аналіз місця установки: рельєф, зони огляду, тип і розташування щогли, маршрути прокладання

кабелів, умови для резервного електроживлення. Встановлення комплексу повинно здійснюватись із врахуванням потенційних кліматичних впливів – іржа, конденсат, обмерзання, підвищені навантаження від вітру тощо. Використовуйте сертифіковані монтажні матеріали, дотримуйтесь стандартів ізоляції, захисту від енергетичних імпульсів та перенапруг. Плануйте регулярний технічний огляд всієї системи (камери, щогли, джерела живлення, датчики) з перевіркою на герметичність корпусів, цілісність кронштейнів, працездатність кабельних трас та антикорозійного захисту.

Розширення системи та підключення додаткових модулів. При необхідності розширити роботу комплексу – наприклад, додати нові камери, охоронні датчики або автоматизовану систему реагування на пожежні сигнали – використовуйте мережеву інфраструктуру для гнучкого підключення без порушення вже функціонуючих сегментів. Нові камери інтегруються через стандартні протоколи TCP/IP, RTSP, Multicast, налаштовуються у WEB-інтерфейсі, додаються до логіки реагування PTZ та архівування. Необхідно враховувати енергетичні потреби розширеної системи: плануйте додаткові джерела живлення, оптимізуйте балансування навантажень, використовуйте генератори та сонячні панелі для незалежної роботи окремих компонентів.

Інтеграція зі сторонніми системами. Комплекс ZIR-Pro підтримує інтеграцію з більшістю сучасних систем охоронної сигналізації, автоматизованих модулів керування доступом, серверів архіву, пожежних датчиків, GNSS-модулів та периферійного обладнання. Використовуйте стандартні інтерфейси: RJ45, USB, релейні виходи для керування сторонніми пристроями, SNMP для віддаленого моніторингу та адміністрування. Для великих або розподілених об'єктів застосовуйте протоколи Multicast, DDNS, VPN для централізованого керування із збереженням високого рівня безпеки й контролю доступу.

Впровадження сучасних функцій та автоматизація. Впроваджуйте інтелектуальні алгоритми аналізу поведінки – детекція порушень периметру, тривожні сценарії, автоматичне PTZ-патрулювання, фільтрація хибних позитивних спрацювань. Реалізуйте автоматизоване резервне копіювання архівів, інтегруйте систему в корпоративні рішення або хмарне середовище із захищеним доступом. Плануйте впровадження нових стандартів відеокодування, оптимізуйте роздільну здатність і частоту кадрів для збереження балансу між якістю запису та розміром архіву.

Керування безпекою та захистом системи. Використовуйте сучасні засоби обмеження доступу: розмежування прав, шифрування даних, аудит дій користувачів, створення груп та ролей із різними рівнями повноважень. Слідкуйте за оновленням прошивок всіх компонентів, контролюйте стан антивірусного захисту робочих станцій операторів та адмінінтерфейсів. При підключенні комплексу до мережі Інтернет впроваджуйте фільтри IP, VPN-тунелі, DDNS з захищеним паролем і регулярною ревізією конфігурації.

Реалізація та підтримка комплексу відеоспостереження ZIR-Pro вимагає системного підходу, постійного контролю стану апаратного та

програмного забезпечення, гнучкого впровадження сучасних технологій та належного рівня інтеграції із зовнішніми системами. Це забезпечує довготривалу, надійну, масштабовану та захищену експлуатацію комплексу – на рівні сучасних стандартів корпоративної безпеки.

4.2.2. Інтелектуальна система відеоспостереження та відеоаналітики для Державної прикордонної служби України INCORESOF Vezha

Програмна платформа для інтелектуальної відеоаналітики Incoresoft Vezha: загальна характеристика

Інтелектуальні системи відеоспостереження здійснюють ключову роль у забезпеченні безпеки та контролю державних кордонів. Впровадження автоматизованої системи з використанням сучасних технологій відеоаналітики забезпечує ефективність охорони, дозволяє оперативно виявляти деякі загрози, а також суттєво зменшує навантаження на персонал прикордонної служби.

Incoresoft Vezha – це програмна платформа для інтелектуальної відеоаналітики, розроблена компанією Incoresoft. Якщо говорити простіше, це «мозок», який підключається до існуючих камер відеоспостереження (CCTV) і за допомогою штучного інтелекту (ШІ) та комп'ютерного зору аналізує все, що потрапляє в кадр. Основна мета платформи – автоматизувати процеси моніторингу, підвищити безпеку та збирати аналітичні дані без необхідності постійного спостереження людиною.

Архітектура системи відеоспостереження. Архітектура системи відеоспостереження Incoresoft Vezha складається з низки ключових компонентів, які разом забезпечують комплексний, надійний та високоефективний відеоконтроль для державної прикордонної служби України.

1. Відеокамери. Відеокамери системи Вежа охоплюють широку роздільну здатність від 0,3 МП (640x512) до 19 МП (5120x3840), що дозволяє вибирати необхідний рівень деталізації залежно від завдань. Камери підтримують частоту кадрів від 10 до 30 FPS, з компресією відео у форматах H.264 та H.265, що оптимізує зберігання та передачу даних. Наявність PTZ-камери (з поворотом, нахилом і зумом) додає гнучкості, дозволяючи вести детальний моніторинг важливих зон. Камери мають клас захисту IP66, що забезпечує працездатність у широкому температурному режимі від -30°C до +50°C, а також підтримує живлення по Ethernet (PoE) для спрощення монтажу.

2. Сервери зберігання і обробки відео. Сервери відповідають для запису, архівування та зберігання відеопотоків у реальному часі в якості Full HD і 4K. Для забезпечення безпеки та цілності даних використовуються сучасні методи шифрування, такі як MD5 і AES. Зберігання організовано з

резервним копіюванням і можливістю масштабування дискових ресурсів, що гарантує тривалу надійність і швидкий доступ до архіву.

3. Мережеві протоколи і передача даних. Передача відеоданих розвивається через стандартизовані мережеві протоколи TCP, UDP, HTTP/HTTPS, RTSP, FTP, SMTP, що забезпечує високу сумісність із різними типами мережевої інфраструктури. Система підтримує мережі Fast Ethernet (100 Мбіт/с) і Wi-Fi, із вбудованими механізмами контролю якості сервісу (QoS). Реальне прорахування завантаження в мережу враховує роздільну здатність камери, кількість кадрів і формат розміщення відео, що дає можливість підтримувати стабільну передачу навіть при великій кількості камер.

4. Програмне забезпечення (VMS, Middleware). Програмний комплекс Incoresoft Vezha VMS керує всіма елементами системи: від прийому відеопотоків до аналітики та збереження. ПЗ має інтуїтивний інтерфейс оператора, Web-клієнти для віддаленого доступу, а також мобільні додатки для Android та iOS. Система підтримує інтеграцію з іншими VMS, наприклад Milestone XProtect, і стандартами ONVIF (профілі S, T, G) для взаємодії з іншими камерами і серверами. Middleware-компоненти забезпечують взаємодію та обробку аналітичних даних, дозволяючи автоматично виявляти та класифікувати об'єкти.

5. Енергозабезпечення та стабільність роботи. Система оснащена джерелами безперебійного живлення (UPS), що гарантує стабільну роботу навіть при непередбачених збоїв в електроживленні. Камери, сервери та мережеве обладнання конструктивно пристосовані до суворих умов експлуатації на території з температурною температурою від -30°C до +50°C, вологою та пилом (стандарт IP66), що забезпечує надійність експлуатації навіть в екстремальних умовах.

Така структура забезпечує комплексне управління відеоспостереженням та аналітикою, що дозволяє державним прикордонним службам ефективно контролювати держкордон із застосуванням сучасних технологій високої надійності та інтелектуальної обробки даних.

Основні функціональні можливості відеоаналітики. Система базується на передових технологіях штучного інтелекту та нейронних мереж, що дають можливість автоматизувати комплексну обробку відеопотоку для забезпечення безпеки державного кордону України.

1. Розпізнавання обличчя (Face Recognition). Високотехнологічний модуль розпізнавання осіб забезпечує ідентифікацію з точністю понад 99%. Система розпізнає навіть вигляд за складних умов: при русі, в умовах недостатнього освітлення, а також коли людина носить захисні засоби (маски, окуляри, головні убори). Це особливо важливо для контролю прохідності через прикордонні пункти та оперативного виявлення осіб, які перебувають у розшуку або під підозрою.

2. Розпізнавання номерних знаків (LPR/ANPR). Модуль автоматично читає номерні знаки автотранспорту, що перетинає кордон, з високою швидкістю та точністю. Це дозволяє ефективно моніторити транспортні

потоки, автоматизувати пропускний контроль і задіяти швидкий пошук авто за базами даних.

3. Детекція об'єктів і подій. Детекція об'єктів (Object Detection) – система, яка відображає об'єкти на відео в реальному часі: транспортні засоби, люди, виявлені підозрілі предмети. Детекція руху (Motion Detection) забезпечує виявлення рухомих об'єктів і автоматичне оповіщення про рух у заданих зонах. Детекція диму і вогню (Smoke and Fire Detection) дозволяє оперативно реагувати на пожежну безпеку в прикордонних зонах.

4. Смарт-трекінг (Smart Tracking System). Автоматичне стеження за рухомими об'єктами, яке підтримує багатоцільове відстеження в режимі реального часу. Система може одночасно контролювати осіб або інші групи об'єктів, які рухаються в межах зони контролю. Це є основою для аналітики поведінки та виявлення аномалій.

5. Спеціалізовані модулі. Виявлення зброї (Gun Detection) –модуль, що дозволяє розпізнавати наявність вогнепальної зброї в кадрі, підвищуючи рівень безпеки на точках контролю. Виявлення військової техніки (Military Equipment Detection) – засіб для розпізнавання та відстеження військового транспорту та техніки, що знаходиться в місці у прикордонній службі.

6. Додаткові можливості. Відеоаналітика працює в реальному часі, що забезпечує миттєве реагування на деякі загрози та події. Системи аналітичних сценаріїв є гнучкими і можуть наслідувати правила виявлення під особливі завдання прикордонної служби. Можливість інтеграції з іншими системами безпеки, базами даних, панелями моніторингу та мобільними додатками, що дозволяє побудувати комплексний захист кордону.

Загалом, система Vezha надає широкий спектр інструментів відеоаналітики, які сприяють підвищенню ефективності контролю та безпеки на державному кордоні шляхом автоматизації розпізнавання, моніторингу та реагування на інциденти.

Технічні характеристики та вимоги системи Incoresoft Vezha.

1. Відеокамери та відеопотік. Система підтримує роботу з відеокамерами високої роздільної здатності, зокрема Full HD (1920x1080) та 4K (3840x2160), зі швидкістю до 30 кадрів на секунду (FPS) за стандартом H.264 і H.265. Відео може кодуватися в різних форматах (H.264, H.265), що дозволяє збалансувати якість з обсягом мережевого трафіку та обробкою.

2. Протоколи передачі даних і мережеві вимоги. Система використовує стандартні мережеві протоколи TCP/IP та UDP для передачі відеопотоків і команд управління, а також підтримує HTTP/HTTPS, RTSP, SMTP, FTP і DNS для комплексної інтеграції в IT-інфраструктуру. Підтримка протоколу ONVIF забезпечує сумісність з іншими камерами та системами відеоменеджменту (VMS), зокрема Milestone XProtect. Для стабільної роботи використовуйте мережу LAN з пропускнуою здатністю не нижче 100 Мбіт/с зі стандартом FastEthernet або краще. Використовується якість обслуговування (QoS) для пріоритезації відеопотоків.

3. Зберігання та архівування відео. Відеодані можуть зберігатися на локальних серверах, мережових сховищах (NAS), відеореєстраторах (NVR) з підтримкою стандартних форматів і функціями архівування. Система забезпечує можливість резервного копіювання та криптографічного захисту (MD5) для гарантії безпеки відеоархівів.

4. Операційні умови. Обладнання забезпечене класом захисту IP66 для стійкості до вологи та пилу. Робочий температурний діапазон становить від -30°C до +50°C, що дозволяє зберегти систему в складних кліматичних умовах прикордонних регіонів.

5. Енергозабезпечення та інфраструктура. Камери та інші пристрої підтримують живлення по Ethernet (PoE), що спрощує монтаж і зменшує кількість кабелів. Використання джерела безперебійного живлення (UPS) рекомендовано для забезпечення безперебійності системи роботи у випадку перебоїв з електропостачанням.

6. Продуктивність аналітики. Аналітичні модулі працюють як на центральних серверах, так і на камерах (зокрема камер Axis ACAP з процесорами ARTPEC-8/9), що дозволяє зупинити завантаження в мережі та забезпечити аналіз у реальному часі. Підтримуватися апаратне прискорення (Intel OpenVINO, NVIDIA TensorRT).

7. Сумісність та інтегрованість. Система інтегрована з безкоштовним VMS, ключовим продуктом є Milestone XProtect. Підтримуватися централізованому управлінню, подіям та сповіщенню можуть бути інтегровані в сторонні рішення через REST API. Підтримувати шифрування даних і розмежування доступу до ролей і груп через LDAP та Active Directory.

Такий рівень технічного оснащення гарантує безперервне функціонування системи у режимі 24/7 для Державної прикордонної служби України, забезпечує результативну обробку значних обсягів відеоданих та підтримує оперативний моніторинг і безпеку з високою точністю та надійністю.

Практичне застосування в діяльності Державної прикордонної служби. Система Incoresoft Vezha істотно посилює контроль за державним кордоном завдяки автоматизованому виявленню порушників, моніторингу транспортного потоку та забезпеченню швидкого реагування на надзвичайні ситуації. Використання інтелектуальної аналітики скорочує час обробки даних і зменшує вплив людського фактора, що підвищує точність і надійність роботи комплексу в умовах служби на кордоні. Інтелектуальна система відеоспостереження «Вежа» є ефективним інструментом комплексної безпеки та контролю, забезпечуючи оперативну ідентифікацію осіб і транспортних засобів та дозволяючи реагувати на загрози в реальному часі. Завдяки цьому система автоматизує процеси контролю доступу, підвищуючи рівень захищеності пунктів пропуску та інших критично важливих об'єктів.

Практичне застосування системи включає:

1) автоматичне розпізнавання облич із порівнянням зі спеціальними базами даних (чорними, білими, VIP) та веденням журналів відвідуваності, що покращує контроль над особами, які перетинають кордон;

2) розпізнавання номерних знаків транспортних засобів контролю руху на прикордонних переходах, що спрощують пропускні операції та забезпечують швидке виявлення автомобілів, що знаходяться в розшуку або належать до небажаних категорій;

3) виявлення рухомих об'єктів, диму, вогню та інших наявних небезпек за допомогою модуля виявлення подій, що значно сприяє оперативності реагування прикордонних служб;

4) використання системи смарт-трекінгу для автоматичного відстеження осіб, транспортних засобів та інших важливих об'єктів під час патрулювання кордону;

5) інтеграція з існуючими системами управління відеоспостереженням (VMS) для централізованого моніторингу та аналізу подій, що забезпечують швидкість прийняття рішень та координації дій.

Крім того, за рахунок використання алгоритмів штучного інтелекту, система Vezha оптимізує обробку відеоданих, зменшує завантаження на операторів і мінімізує людський фактор помилок, що є критичним виробництвом у діяльності державної прикордонної служби. Впровадження таких інтелектуальних систем дозволяє підвищити загальний рівень безпеки кордону, скоротити час контролю та провести превентивний захист від порушення.

Таким чином, Vezha полегшує перехід від пасивного відеоспостереження до проактивної системи безпеки, де відеоаналітика не тільки фіксує події, а й самостійно аналізує та сповіщає про надзвичайну ситуацію, що забезпечує ефективність роботи прикордонної служби України.

Інтелектуальні системи відеоспостереження, такі як Incoresoft Vezha, є основою для модернізації охорони державного кордону України. Дальший розвиток впровадження нових аналітичних алгоритмів, використання штучного інтелекту для глибшого аналізу інтегрованих відеопотоків, а також іїзація з безпілотними системами, що підвищує ефективність і автоматизацію кордонного контролю.

Рекомендації щодо розрахунку пропускної спроможності каналів зв'язку для забезпечення потреб систем відеоспостереження

Розрахунок вимог до пропускної спроможності каналу зв'язку до відеокамери

Розрахунок вимог до пропускної спроможності каналу зв'язку $P \left(\frac{\text{Мбіт}}{\text{с}} \right)$ для одного потоку з камери (при використанні рекомендованого кодексу стиснення відео H.264 та частоті кадрів 30 FPS) відбувається спрощено за формулою:

$$P \left(\frac{\text{Мбіт}}{\text{с}} \right) \approx xMP \times 2 \left(\frac{\text{Мбіт}}{\text{с}} \right),$$

де xMP – це кількість мегапікселів камери.

Наприклад на сьогодні камери, які встановлені на кордоні здебільшого мають роздільну здатність 4 МР. Виходячи з цього, потреба у пропускній спроможності каналу зв'язку для передачі одного потоку з однієї камери (одного сенсору) становитиме:

$$4MP \times 2 \left(\frac{\text{Мбіт}}{\text{с}} \right) = 8 \left(\frac{\text{Мбіт}}{\text{с}} \right).$$

В залежності від вимог до якості потоку згідно задач певної ділянки та від налаштувань аналітичної підсистеми необхідним і достатнім як для запису так і для перегляду в реальному часі може визначатись частота кадрів 15 FPS. Таке налаштування відеопотоків дозволить зменшити в два рази вимоги до пропускної здатності каналу зв'язку.

Тобто для частоти кадрів 15 FPS та кодексу H.264 можемо спрощено користуватись формулою:

$$P \left(\frac{\text{Мбіт}}{\text{с}} \right) \approx xMP.$$

Слід зауважити те, що при підключенні до камери і трансляції ще одного потоку або інших клієнтів до того ж потоку, вимоги збільшуються відповідно. Наприклад, камера має додатковий потік в якості FullHD (1920x1080) 30FPS H.264, який має транслюватись напяму з камери на окремому ПК.

Тобто, при підключенні 2 клієнтів напяму до камери і трансляції 2 відеопотоків в якості 4 МП та 2 МП (30FPS H.264), отримаємо мінімальну ширину каналу 12 Мбіт/с.

Нижче наведено таблицю відповідності максимальної роздільної здатності кількості мегапікселів в матриці камери та швидкості потоку (бітрейт) при стисненні H.264 та 30 FPS:

Роздільна здатність (мегапікселів)	Відеокодек	FPS (кадрів в секунду)	Бітрейт, Мбіт/с
640x512 (0.3MP 5:4)	H.264 (Добра якість)	30	0,7
800x600 (0.5MP 4:3)	H.264(Добра якість)	30	1,0
1280x720 (1MP 16:9)	H.264(Добра якість)	30	1,9
1280x960 (1.2MP 4:3)	H.264(Добра якість)	30	2,6
1280x1024 (1.3MP 5:4)	H.264(Добра якість)	30	2,7
1600x1200 (2MP 4:3)	H.264(Добра якість)	30	4,0
1920x1080 (2MP 16:9)	H.264(Добра якість)	30	4,3
2048x1536 (3MP 4:3)	H.264(Добра якість)	30	6,6
2560x1440 (4MP 16:9)	H.264(Добра якість)	30	7,7
2560x1920 (5MP 4:3)	H.264(Добра якість)	30	10,3
3072x1728 (5MP 16:9)	H.264(Добра якість)	30	11,1
3072x2048 (6MP 3:2)	H.264(Добра якість)	30	13,1
3296x2472 (8MP 4:3)	H.264(Добра якість)	30	17,0
3840x2160 (8MP 16:9)	H.264(Добра якість)	30	17,3
3648x2752 (10MP 4:3)	H.264(Добра якість)	30	21,0
4000x3000 (12MP 4:3)	H.264(Добра якість)	30	25,1
5120x3840 (19MP 4:3)	H.264(Добра якість)	30	41,1

Важливо також уточнити, що необхідна ширина каналу залежить від кількості користувачів, які тягнуть потоки з камери (сервери запису, сервери аналітики, мобільні та веб клієнти, тощо). Крім того вона також залежить від наявності декількох сенсорів у камери. Тому що кожний оптичний та тепловізійний сенсор має свій потік. Також необхідно передбачити резерв пропускної спроможності для цілей управління камерою приблизно в 1 Мбіт/с. У випадку з камерами 3iP маємо розрахунок:

Отже загальна вимога до пропускної спроможності каналу зв'язку до відеокамери для H.264 спрощено може розраховуватись як:

$$\times \left(\frac{xFPS}{12} \right) + T_{xMP} \times \left(\frac{xFPS}{12} \right) + \dots$$

де xМП – це кількість Мегапікселів відповідного потоку камери;

xFPS – частота кадрів відповідного потоку камери;

N - кількість користувачів основного потоку камери (оптичний сенсор);

n - кількість користувачів другого потоку камери (оптичний сенсор);

T - кількість користувачів основного потоку камери (тепловізійний сенсор).
... + всі наявні потоки та їх користувачі...

Розрахунок вимог до пропускної спроможності каналів зв'язку до серверу відеозапису підрозділу

Методика розрахунку для каналів зв'язку підрозділу де розташований сервер відеореєстрації базується на тих же принципах, що і для окремої камери, але додатково враховується:

- 1) кількість потоків з камер, підключених до сервера відеореєстрації через конкретний зовнішній канал передачі даних;
- 2) параметри якості таких відеопотоків (і відповідні бітрейти);
- 3) кількість та бітрейт потоків до зовнішніх клієнтів через конкретний зовнішній канал поза локальною мережею відеосerverа, які споживають інформацію з нього – (сервери відеоаналітики, мобільні та веб-клієнти, сервери та клієнти старших підрозділів, клієнти підлеглих підрозділів);
- 4) перспективи підключення нових камер та клієнтів до сервера;
- 5) вимоги до гарантованої пропускної спроможності інших високопріоритетних ІТ сервісів та додатків, які використовують конкретний канал передачі даних – такі вимоги слід резервувати при розрахунках параметрів каналу зв'язку;
- 6) резерв пропускної спроможності – по можливості 10-30 %.

Такий розрахунок необхідно проводити для кожного зовнішнього каналу передачі даних підрозділу, через який планується або вже здійснюється передача потоків відеоданих.

Слід зауважити, що якщо камери транслюють та ведуть запис за протоколом UDP всі пакети, які не вміщуються в ширину каналу, просто відкидаються, що в свою чергу призводить до зменшення кадрів відео або навіть означає, що деякі дані можуть бути втрачені під час передачі. Це впливає як на онлайн-трансляцію, так і на запис в архів. Якщо це TCP з'єднання, яке є більш надійним для передачі даних ми отримаємо дуже великі затримки при перегляді, так як, TCP вимагає встановлення з'єднання та передачі кожного пакету даних окремо. Це може зайняти багато часу і ресурсів, якщо пропускна здатність каналу обмежена.

Наприклад, якщо до кінця року планується загальна кількість камер на підрозділі 30 штук, з розрахунків мінімального потоку з камер в 8 Мбіт/с, маємо:

$$30 \times 8 \text{ Мбіт/с} = 240 \text{ Мбіт/с.}$$

Слід зауважити, що це вхідний потік з всіх камер, які далі мають транслюватись. Таким же чином треба вирахувати вихідний трафік. Наприклад ми маємо 15 клієнтів, які будуть отримувати відеопотоки оброблені сервером, та кожен клієнт буде дивитись відеокамери своєї зони відповідальності по 2-3 шт. Отже при одночасному підключенні всіх користувачів і перегляді камер в FullHD якості (1920x1080), маємо додатково:

$$15 (\text{клієнт}) \times 3 (\text{камери}) \times 4 \text{Мбіт/с} = 180 \text{ Мбіт/с}$$

Якщо кількість клієнтів, чи камер буде змінюватись, можна все перерахувати за формулами, що вказані вище, або використати он-лайн калькулятори. Наприклад такий, як за посиланням: <https://www.jvsg.com/storage-bandwidth-calculator/>.

Як можна побачити з наведених вище прикладів, вимоги до пропускної спроможності каналів передачі даних легко перетинають швидкість стандартних мереж FastEthernet – 100 Мбіт/с. Тому необхідно крім зовнішніх каналів переглянути можливі маршрути руху відеоданих по локальній обчислювальній мережі з метою виявлення можливих вузьких місць – комутатори LAN, маршрутизатори, брандмауери тощо.

Для заощадження пропускної спроможності каналів зв'язку слід використовувати параметри якості відеопотоків необхідні та достатні для вирішення службових задач а також найбільш сучасні кодеки відеостиснення (H.265) при умові їх сумісності з компонентами системи.

Налаштування обладнання інтегрованої системи відеоспостереження

Облаштування місця встановлення обладнання. Під час розрахунку фізичного простору необхідно враховувати фізичні розміри обладнання, яке буде розміщено в кімнаті та відповідних шаф для його монтажу. Враховуйте технологічні коридори навколо шаф з обладнанням мінімум 60 см з двох боків. Вільний простір перед передньою стороною шафи має бути не меншим ніж 120 см. Передбачайте простір для можливості обслуговування зовнішніх каналів зв'язку, ліній електропостачання та кабельних трас локальної мережі та їх введення у приміщення місця розташування обладнання (через стелю, підлогу або стіни суміжних приміщень). Для серверів, які будуть надані централізовано для запуску системи враховуйте 2 сервери по 2 юніти – разом 18 см заввишки в шафі та глибина 80 см.

Уникайте розміщення обладнання відеоспостереження у підвальних, мансардних та горищних приміщеннях, а також у тих приміщеннях де проходять такі магістральні інженерні комунікації, як водопостачання, опалення, каналізація та водовідвід з даху. Також не рекомендовано розміщувати обладнання під такими приміщеннями як кухня, туалет, духова, пральня та подібні. Не рекомендується розміщувати обладнання також поруч або над приміщеннями з підвищеними температурами – сушильні, сауни або котельні. Найкраще розміщення з точки зору безпеки, обслуговування та мінімізації кабельних мереж всередині будівлі це ізольоване приміщення у центральній частині будівлі на першому поверсі, яке не має контактів з зовнішніми стінами будинку (правило двох стін), не має вікон та відсутність радіаторів або теплових джерел поблизу обладнання.

Оцініть вимоги до живлення на основі потужності та кількості серверів, телекомунікаційного, кліматичного та іншого обладнання, щоб уникнути перевантаження системи живлення. Застосовуйте диференційні автомати або

пристрої захисного відключення (УЗО) для запобігання ураження персоналу електричним струмом та виникнення загоряння. Має бути обов'язково передбачене заземлення, незалежне від інших систем будівлі. Слід також передбачити кабельне введення для резервного джерела живлення якщо будівля цілком не забезпечується резервним джерелом (генератором) централізовано. Генератор не слід розташовувати поруч з ввідною підстанцією містечка та безпосередньо поруч з будівлею, де розміщена серверна. Дотримуйтесь протипожежних вимог по розміщенню залежно від оточення місця розташування генератора.

Переконайтеся, що належні системи охолодження встановлені для підтримки оптимальної для обладнання температури (18-23 С) та вологості 45-55%. Розрахунок охолоджувальної потужності системи кондиціонування має здійснюватися виходячи з суми номінальних потужностей блоків живлення обладнання, яке має бути розміщено у приміщенні, розмірів самого приміщення та інших факторів. Рекомендований запас охолоджувальної потужності має становити щонайменше 30% від розрахункової потреби. При виборі кондиціонера надавайте перевагу інверторним моделям. Потік охолодженого повітря від кондиціонерів необхідно спрямовувати безпосередньо до передньої (фасадної) частини монтажних шаф. Установлення та розміщення кліматичного й вентиляційного обладнання слід виконувати з повним дотриманням технічних вимог і рекомендацій виробників як технологічних, так і кліматичних систем. Вільний простір навколо обладнання має забезпечувати безперешкодний доступ для проведення профілактичних робіт, а також для монтажу і демонтажу технологічного обладнання в монтажні шафи та монтажу і демонтажу кліматичного обладнання. Внутрішній блок кондиціонера та його дренажну систему не слід розташовувати безпосередньо над шафою з обладнанням та системою живлення.

Мережеве обладнання включає комутатори, маршрутизатори, брандмауери та кабельну інфраструктуру для підтримки мережі. Проектуйте та забезпечуйте додержання топології локальної мережі типу «Зірка». Уникайте прокладання кабельних трас локальної мережі та телефонії паралельно з лініями електроживлення. Не допускайте використання додаткових комутаторів біля кінцевих пристроїв мережі. Можливе використання комутаторів рівня доступу на поверхах будівлі, які розміщені у окремих комутаційних шафах. Кабельна інфраструктура (СКС) має будуватись дотримуючись вимог стандарту Cat5e. Не бажано використовувати саморобні патч-корди для комутації обладнання в комутаційних шафах та для підключення кінцевих пристроїв мережі.

Передбачайте заходи фізичної безпеки, такі як системи пожежної сигналізації та пожежогашіння, при наявності системи контролю доступу (СКД) та камери відеоспостереження, щоб захистити обладнання та контролювати доступ до нього. Тільки авторизовані особи повинні мати доступ до серверного приміщення. У випадку відсутності СКД слід вести журнали обліку доступу до місць розміщення серверного обладнання. Доступ

обслуговуючого персоналу має здійснюватися тільки під наглядом відповідальних за обладнання осіб.

За можливості плануйте резервне джерело живлення (UPS), резервні системи охолодження та резервне копіювання важливих даних та конфігурацій обладнання на віддалені площадки, щоб мінімізувати час простою. Потужність та час роботи ДБЖ має бути розрахований таким чином, щоб забезпечити роботу встановленого обладнання протягом часу, який потрібен для запуску резервного джерела живлення і переключення на нього. ДБЖ має бути оснащений інтерфейсом та ПЗ для комунікації з серверним обладнанням, функцією подачі сигналу на запуск резервного генератора.

Налаштування камер відеоспостереження

Сучасні системи відеоспостереження є невід'ємною частиною комплексних рішень безпеки. Їх ефективність значною мірою залежить від коректного вибору та налаштування камер, особливо при використанні систем відеоаналітики.

Вимоги до апаратних характеристик камер.

Роздільна здатність (Resolution). Висока роздільна здатність є ключовою вимогою для ефективної роботи відеоаналітики. Вона безпосередньо впливає на точність розпізнавання об'єктів та якість аналітики. Мінімальною вимогою є роздільна здатність 1080p (Full HD). Це забезпечує базову деталізацію для ідентифікації людини на відстанях до 10-15 метрів. Однак для сучасних систем відеоаналітики цього часто буває недостатньо. Рекомендованою вимогою є роздільна здатність 4K (Ultra HD) або вище. Камери 4K забезпечують значно кращу деталізацію, дозволяють охоплювати більші площі без втрати якості та дають змогу ефективно використовувати цифрове збільшення. Це особливо важливо для розпізнавання дрібних деталей, таких як номери автомобілів на великих дистанціях або облич людей.

Частота кадрів (FPS). Частота кадрів визначає плавність відео та здатність системи аналізувати швидкі рухи. Мінімальна вимога – 10 кадрів за секунду. Це дозволяє фіксувати базові рухи, але для аналітики швидких переміщень може бути недостатньо. Рекомендована частота – 15 FPS і вище, ідеально 25-30 FPS. Вища частота кадрів забезпечує плавність відео, покращує точність відстеження рухомих об'єктів і зменшує ймовірність пропуску важливих подій між кадрами.

Кут огляду (Field of View). Кут огляду визначає площу простору, яку охоплює камера. Стандартний кут огляду (90°-120°) підходить для моніторингу коридорів, приміщень середньої площі та вхідних груп. Ширококутні камери (120° і більше) дозволяють охоплювати великі території, що робить їх ідеальними для моніторингу парковок, складів та відкритих просторів. Вони дозволяють зменшити кількість камер, необхідних для покриття великої площі.

Нічне знімання та підсвічування. Для цілодобової роботи системи необхідне ефективне підсвічування в умовах темряви. Інфрачервоне (ІЧ) підсвічування забезпечує видимість на відстанях від 20 до 150 метрів. Воно енергоефективне і відносно недороге, але дає чорно-біле зображення. Лазерне підсвічування забезпечує якісне освітлення на відстанях до 1000 метрів і більше. Воно дає більш рівномірне освітлення, але коштує значно дорожче. Для найскладніших умов може розглядатися використання тепловізійних камер, які фіксують теплове випромінювання об'єктів і працюють незалежно від освітлення.

Широкий динамічний діапазон (WDR). Технологія WDR має ключове значення для формування якісного відеозображення в умовах різко вираженої контрастності освітлення. Вона забезпечує коректну передачу як надмірно освітлених, так і темних фрагментів сцени одночасно. Це особливо актуально під час зйомки зон входу чи виходу з приміщень, де виникає значна різниця між яскравими ділянками та затіненими областями. Рекомендується використання камер з апаратним WDR з діапазоном 120 дБ і вище, оскільки програмні аналоги (DWDR) значно поступаються за ефективністю.

Алгоритми стиснення відео. Вибір кодека стиснення впливає на обсяг даних, що зберігаються, та навантаження на мережу. H.264 є надійним стандартом, який демонструє стабільну роботу навіть при нестабільному з'єднанні. Він рекомендований для використання в бездротових мережах (Wi-Fi, радіоканали). H.265 (HEVC) є більш сучасним кодеком, який забезпечує на 40-50% ефективніше стиснення при тій же якості зображення. Він рекомендований для стабільних проводних мереж і особливо ефективний при роботі з відео високої роздільної здатності (4K).

Функціональні та програмні аспекти Incoresoft Vezha.

Вбудована аналітика (детекція руху, перетин ліній, розпізнавання об'єктів) зменшує навантаження на сервери. Підтримка AI покращує аналітичні можливості. Камери повинні підтримувати стандарт ONVIF (профілі S, T, G) для забезпечення взаємодії з VMS (наприклад, Milestone XProtect). Для зовнішнього використання необхідний ступінь захисту IP66 та робочий діапазон температур від -30°C до +50°C. Підтримка PoE спрощує установку. Для критичних об'єктів рекомендовано використання джерел безперебійного живлення.

Інтелектуальні функції та вбудована аналітика. Сучасні камери комплексу Vezha обладнані інтегрованими аналітичними модулями, які не просто фіксують відео, а й здійснюють його обробку в режимі реального часу. Завдяки цьому значно скорочується навантаження на центральні сервери та підвищується загальна продуктивність системи. До ключових функцій відеоаналітики належать: детекція руху (розумний алгоритм відрізняє корисні події (рух людини чи автомобіля) від незначних змін (опале листя, тіні, дощ)); перетин віртуальної лінії (система генерує тривогу при перетині об'єктом заданої межі у визначеному напрямку); контроль

входу/виходу із зони (функція для контролю доступу до заборонених або обмежених зон); розпізнавання об'єктів (камера може класифікувати об'єкти на типи: «людина», «автомобіль», «вантажівка», що дозволяє фільтрувати сповіщення за типами подій).

Підтримка штучного інтелекту (AI) значно розширює аналітичні можливості. AI-камери можуть розпізнавати конкретні атрибути (колір одягу, тип транспортного засобу), виявляти специфічні події (залишені предмети, скупчення людей) та працювати з високою точністю в складних умовах.

Інтеграційна сумісність: стандарт ONVIF. Камера обов'язково має підтримувати стандарт ONVIF (рекомендований ONVIF profile S,T) та повинна бути сумісна з існуючими системами керування відео (VMS-Milestone XProtect) та аналітичними платформами. При наявності проміжних відеореєстраторів або VMS серверів, вони мають підтримувати ONVIF profile G та приймати не більше 16 відеопотоків від камер. При цьому в разі підключення такого відеореєстратора до Milestone XProtect він буде бачити такий відеореєстратор як один пристрій з шістнадцятьма відеопотоками і використовувати одну ліцензію на пристрій. При кількості потоків більше 16 на відеореєстраторі необхідно буде використовувати «девайс» ліцензію на кожний відеопотік для підключення його до Milestone XProtect. Підтримка цих стандартів гарантує безпроблемну інтеграцію камер Vezha з різними системами керування відео, включаючи Milestone XProtect.

Захист та надійність для зовнішнього використання. Для роботи на відкритому повітрі камери повинні мати відповідний ступінь захисту: IP66 – забезпечує повну герметизацію від пилу та захист від потужних струй води; робочий діапазон температур від -30°C до +50°C** – гарантує стабільну роботу взимку та влітку

Живлення та мережеві можливості. Для стабільного функціонування системи важливими є такі можливості: підтримка PoE (Power over Ethernet), що дає змогу передавати живлення та дані одним кабелем і цим суттєво спрощує монтаж; застосування джерел безперебійного живлення на об'єктах підвищеної відповідальності, а також організація резервного енергоживлення на випадок знеструмлення. Сукупність цих характеристик гарантує надійну та ефективну роботу системи відеоспостереження за будь-яких умов експлуатації.

Процедура налаштування камер. Камери слід розміщувати на висоті 2,5 – 4 метри з оптимальним кутом нахилу для мінімізації сліпих зон. Необхідно налаштувати фокус, експозицію, баланс білого та шумопридушення. Вивід назви камери, дати та часу через OSD є обов'язковим. Визначення зон детекції, налаштування чутливості та встановлення розкладів активності покращують точність аналітики. Призначення статичних IP-адрес, налаштування QoS та синхронізація часу за NTP є обов'язковими для стабільної роботи. Використання складних паролів, Digest-аутентифікації, шифрування трафіку та регулярне оновлення прошивки забезпечують захист системи.

Інтеграція з системами керування відео (VMS). Перевірка взаємодії з VMS, налаштування подій та сповіщень є ключовими для оперативного реагування. Використання локальних носіїв (SD-картки) та мережесховищ (NAS, NVR) забезпечує надійність архівування.

Налаштування камер відеоспостереження для забезпечення ефективної роботи відеоаналітики

Коректне налаштування камер відеоспостереження є критично важливим для ефективної роботи систем відеоаналітики. Дотримання вимог до апаратних характеристик, мережесховищ, безпеки та інтеграції дозволяє забезпечити високу точність аналітичних даних, мінімізувати кількість помилкових спрацьовувань та підвищити надійність системи в цілому. Регулярне оновлення прошивок, навчання персоналу та ведення документації є невід'ємними частинами супроводу таких систем.

Вибір моделі та виробника камери відеоспостереження залежить від специфіки задач, вимог до системи та умов експлуатації. Для забезпечення коректної роботи відеоаналітики необхідно враховувати низку аспектів, що охоплюють встановлення, конфігурацію апаратного та програмного забезпечення, а також інтеграцію з іншими системами. У цій статті представлено основні вимоги та рекомендації щодо налаштування камер відеоспостереження для забезпечення оптимальної продуктивності та точності відеоаналітики.

Встановлення камери. Правильне розміщення камери є ключовим для забезпечення якісного збору даних. Камери рекомендується встановлювати на висоті 2,5 – 4 м, що забезпечує оптимальний огляд і мінімізує сліпі зони. Налаштування кута нахилу камери має гарантувати охоплення ключових зон спостереження та уникнення мертвих зон. Камера повинна розташовуватися на оптимальній відстані від об'єкта спостереження, щоб забезпечити достатній рівень деталізації зображення.

Налаштування та оптимізація зображення. Для отримання якісного відеозображення необхідно виконати наступні налаштування. Використовуйте уніфікований формат найменування камер. Назву камери слід виводити у правому верхньому куті зображення за допомогою OSD-накладання, а дату і час – у лівому верхньому куті. Налаштуйте фокус для забезпечення чіткості зображення. Відрегулюйте параметри експозиції та балансу білого для коректного відображення кольорів і освітлення в різних умовах. Активуйте функцію шумопридушення для покращення якості зображення в умовах низької освітленості.

Конфігурація відеоаналітики. Правильне налаштування відеоаналітики забезпечує ефективну обробку відеоданих, для цього: визначте та налаштуйте зони, у яких активується детекція руху або інші аналітичні функції; відрегулюйте рівень чутливості для зменшення кількості помилкових спрацьовувань; налаштуйте розклади роботи аналітики, наприклад, для активізації в нічний час.

Запропоновані кроки забезпечують ефективну роботу систем відеоспостереження та відеоаналітики, мінімізуючи ймовірність збоїв і

підвищуючи точність аналітичних даних. Дотримання цих рекомендацій дозволяє оптимізувати функціональність камер, забезпечити їх безпеку та інтеграцію з іншими системами, а також підтримувати високий рівень продуктивності в різних умовах експлуатації.

Правила найменування серверів та камер відеоспостереження в системі

Дані правила призначені для уніфікації та систематизації іменування обладнання в рамках єдиної інфраструктури відеоспостереження. Це забезпечує швидку ідентифікацію, полегшує адміністрування, пошук несправностей та інвентаризацію.

1. Правила найменування камер

Мета створення зрозумілої та інформативної назви, яка однозначно визначає місце розташування, приналежність та тип камери.

Структура формату: 3333.8383.ПППП-КККТ (Назва)

Розшифровка компонентів:

- 3333 – Код підрозділу: Унікальний номер прикордонного загону або військової частини, до якої приписана камера.

- *Призначення:* Визначає організаційну приналежність обладнання.

- 8383 – Код вузла зв'язку: Номер вузла зв'язку або комутаційного пункту, через який здійснюється підключення камери до мережі.

- *Призначення:* Вказує на мережеву інфраструктуру та полегшує вирішення проблем із зв'язком.

- ПППП – Код об'єкта: Номер прикордонного знаку, контрольно-пропускного пункту (КПП) або іншого конкретного об'єкта охорони.

- *Призначення:* Точно визначає географічне місце встановлення камери.

- *Особливість:* Якщо однойменні знаки існують у різних країнах, до коду додається літера країни (наприклад, H339U для України).

- -КККТ – Ідентифікатор камери:

- ККК – порядковий номер камери на об'єкті (від 001 до 999).

- Т – опціональний індикатор, що позначає тепловізійну камеру. Якщо камера звичайна (оптична), цей індекс відсутній.

- *Призначення:* Визначає конкретний пристрій серед інших на тому ж об'єкті та вказує на її технологічні особливості.

- (Назва) – Змістовний опис:

- *Правило:* Назва обов'язково вказується латиницею. Кирилиця заборонена для уникнення проблем із кодуванням в мережевих системах та програмному забезпеченні.

- *Призначення:* Дозволяє швидко візуально ідентифікувати камеру в списку без необхідності розшифровувати цифровий код (наприклад, "Salovka 4").

Приклад аналізу:

0094.2221.H339-001T (Salovka 4)

- 0094: Прикордонний загін №94.

- 2221: Вузол зв'язку №2221.

- Н339: Прикордонний знак №339.
- -001Т: Перша за номером камера на цьому знаку, тепловізор.
- (Salovka 4): Людсько-зрозуміла назва об'єкта.

2. Правила найменування серверів

Мета: чітка ідентифікації ролі, призначення та місця сервера в інфраструктурі.

Структура формату: 333.8383.CCC[A] (Назва)

Розшифровка компонентів:

- 333 – Код підрозділу: Скорочений номер загону (аналогічно камерам).
- 8383 – Код вузла зв'язку: Аналогічно камерам.
- CCC – Порядковий номер сервера (від 001 до 999) в межах даного вузла зв'язку.
- [A] – Ключовий індекс призначення: Літера А додається виключно для серверів, на яких працює система інтелектуальної аналітики "Vezha". Відсутність літери означає, що це інший тип сервера (наприклад, основний сервер запису Milestone).
- (Назва) – Людсько-зрозумілий опис ролі сервера (латиницею). Наприклад, MilestoneMain (основний сервер запису) або VezhaAI (сервер аналітики).

Приклади аналізу:

1. 009.2221.001 (MilestoneMain)
 - Це основний сервер управління відеоспостереженням (VMS) Milestone.
 - Розташований у загоні 009, на вузлі зв'язку 2221.
 - Перший за номером сервер.
 - Індекс А відсутній – отже, це не сервер аналітики "Vezha".
2. 009.2221.002A (VezhaAI)
 - Це сервер інтелектуальної відеоаналітики "Vezha".
 - Розташований у тому ж загоні та на тому ж вузлі зв'язку.
 - Другий за номером сервер.
 - Наявність індексу А однозначно вказує на його ключову функцію – запуск аналітичних модулів ІІІ.

Така система найменування є логічною та ієрархічною. Вона будується за принципом "від загального до приватного" (Загін -> Вузол зв'язку -> Об'єкт -> Пристрій) і містить обов'язкові індекси для позначення спеціалізації обладнання (тепловізор, сервер аналітики). Дотримання цих правил є критично важливим для підтримки порядку в великій розподіленій системі безпеки.

Налаштування відеоаналітики

У інтелектуальній системі відеоспостереження ми маємо як мінімум три рівня, де може бути реалізована аналітична оцінка відеоряду: IP-Камера; сервер відеоспостереження VMS (Milestone XProtect); спеціалізоване програмне забезпечення відеоаналітики з штучним інтелектом (Incoresoft Vezha).

Додатково між камерою та сервером відеоспостереження Milestone може бути застосований відеореєстратор.

Всі сучасні IP камери та відеореєстратори підтримують функцію детекції руху та активації певних дій по цій події – як мінімум запис фрагменту відео. Більш того сьогодні нескладні аналітичні обчислення робить процесор, вбудований у камеру або цифровий відеореєстратор. Саме такі камери та реєстратори отримали назву «старт». Приклад таких аналітик наведено нижче.

1) Затуляння об'єктива. Камера піднімає тривогу, коли зображення закрито. Приклади спрацювання: камеру намагаються закрити рукою, надіти шкарпетку, залити з балончика з фарбою.

2) Розфокусування. Так само як і попередня, містить режим тривоги у момент закриття зображення. Але тут мова не про повне зникнення картинки, лиш про часткову фіксацію картини камерою. Приклади спрацювання: камеру заклеюють скотчем, заливають будь-яким гелем тощо.

3) Вторгнення у виділену зону. Якщо ви відзначите на зображенні ділянку, то при переміщенні у неї увімкнеться тривога. У цьому випадку бувають помилкові спрацювання, наприклад, через зміну освітлення, муху, що пролітала повз та ін.

4) Перетин лінії. Схоже на вторгнення у виділену зону. Проведіть лінію на зображенні. При її перетині спрацює тривожний сигнал. Можна виставити спрацювання при односторонніх або двосторонніх перетинах.

5) Звукові зміни. Працюють лише в камерах зі звуком. Такі камери фільтрують фоновий шум для запобігання помилкових спрацювань і запускають тривогу при перевищенні порогового рівня звуку.

6) Виявлення залишених/зниклих предметів. Тривога спрацює при тривалому знаходженні нового об'єкта, або відсутності виділеного об'єкта в зоні, що охороняється. Дуже важлива функція для антитерору та боротьби з крадіжками. Налаштовується поріг спрацювання (час присутності/відсутності об'єкта до тривоги) і чутливість.

7) Підрахунок людей. Принцип роботи схожий на спрацювання при перетині лінії, але з захистом від помилкових спрацювань. Підраховує кількість людей, що увійшли (перетин в одну сторону) і вийшли (перетин в іншу сторону). У підсумку отримуємо архів з пакетом даних, які можна переглядати за періоди у день/тиждень/місяць/рік. А ще є можливість показу лічильників на OSD-меню.

8) Визначення автомобільних номерів. Камер, що підтримують цю функцію, стає все більше. Вона зазвичай дозволяє визначати й записувати в архів автономери, співвідносити їх з “чорним” і “білим” списками, віддаючи сигнали на виконавчі пристрої. Приклади використання: камери з білим списком можуть автоматично відкривати шлагбаум для зареєстрованих автомобілів.

Використання аналітичних модулів, які інтегровані у відеокамери та відеореєстратори дозволяє розвантажити канали зв'язку, сервери відеореєстрації та систему в цілому. Тому доцільно активувати аналітику, наявну в існуючому обладнанні для використання у ІСВ¹.

Для можливості інтеграції подій, які були виявлені вбудованою аналітикою обладнання у ІСВ, необхідно налаштувати їх передачу по певним правилам на сервер відеореєстрації Milestone XProtect. Зазвичай все обладнання має функцію передачі тривожних подій за різними каналами: за протоколом Onvif, e-mail, ftp сервер, тривожний вихід тощо. Відповідно з боку приймальної сторони (сервера Milestone XProtect) необхідно налаштувати правила обробки таких подій.

Для камер, які не мають навіть простої функції детекції руху, ця функція може бути реалізована безпосередньо на сервері Milestone XProtect. Більш складні функції, такі як розпізнавання розпізнавання об'єктів, виявлення зброї, розпізнавання військової техніки, номерів авто, розпізнавання обличч, тощо можуть бути реалізовані за допомогою спеціалізованого програмного забезпечення відеоаналітики з штучним інтелектом (Incoresoft Vezha)

Слід мати на увазі, що в поточній архітектурі ІСВ (рис. 5.1) та поточному сценарії її використання центром обробки подій з усіх джерел (в тому числі і від Incoresoft Vezha) є підсистема менеджера тривог сервера подій Milestone XProtect.

¹ ІСВ — це інтегрована система відеоспостереження, яка представляє собою комплекс програмно-апаратних рішень, що забезпечують збір, обробку, зберігання та аналіз відеоінформації з різних джерел. Такі системи включають часто не тільки відеокамери, але й засоби відеоаналітики, детекції руху, розпізнавання обличчя, номерних знаків, а також інтеграцію з іншими охоронними системами (контроль доступу, сигналізація) для підвищення ефективності безпеки.

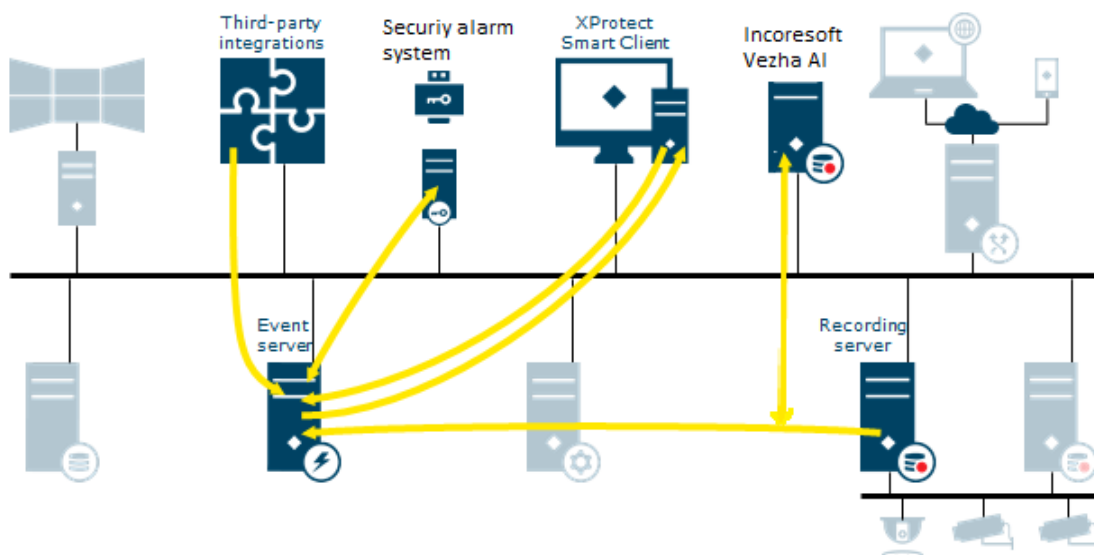


Рисунок 5.1 – Архітектура ICB

Сервер подій (рис. 5.2) отримує повідомлення від камер через серверу запису та інших зовнішніх джерел (охоронні сигналізації, спеціалізоване програмне забезпечення відеоаналітики з штучним інтелектом Incoresoft Vezha, системи контролю доступу тощо), здійснює їх обробку відповідно до правил, які описуються адміністратором в системі та відправляє дані в XProtect Smart Client для відображення в списку тривог та на мапі. Користувач XProtect Smart Client реагує на сповіщення тривоги, здійснює їх обробку та повертає дані на сервер подій.

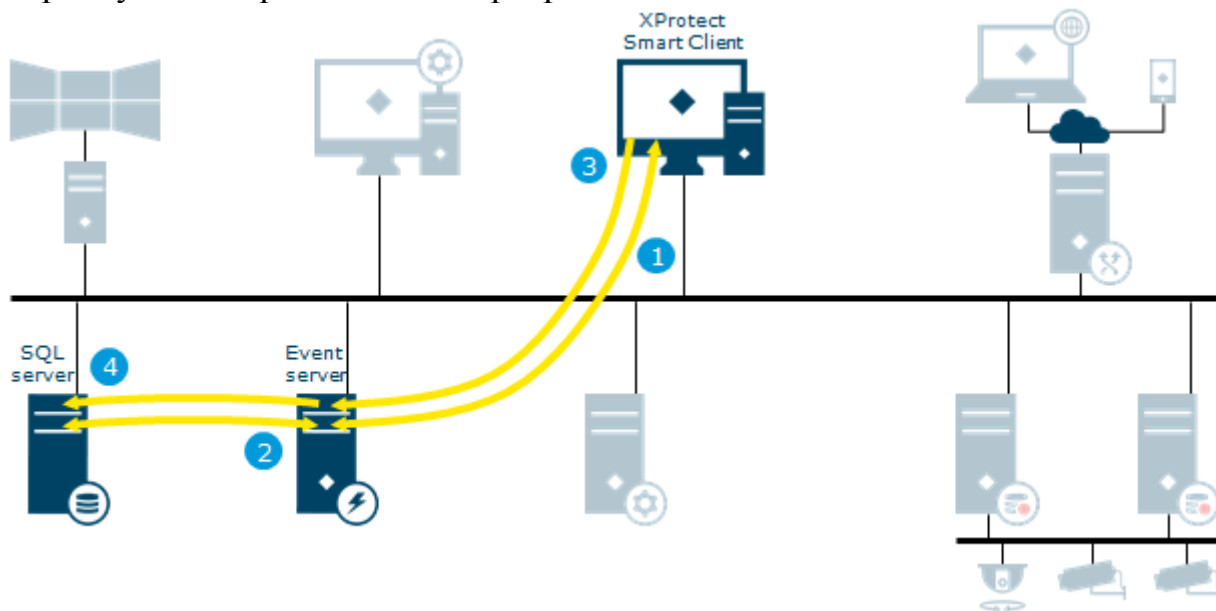


Рисунок 5.2 – Архітектура ICB (серверне обладнання)

Перегляд тривог та керування ними:

1. XProtect Smart Client опитує сервер подій щоб отримати актуальний список тривог.
2. Список тривог отримується з бази даних SQL Server і повертається до XProtect Smart Client.

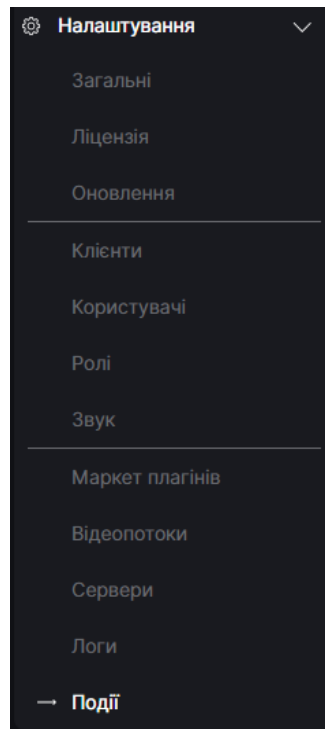
3. Тривога відображається у списку для обробки, після чого його стан, подробиці опрацьовуються оператором, додаються пояснення та коментарі.

4. Новий стан, подробиці та пояснення, зберігаються в базі даних SQL Server.

Менеджер подій (Надсилення сповіщень про події із системи аналітики до Milestone)

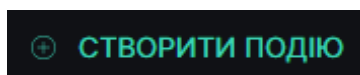
1. Відкриття розділу подій:

- У лівому меню виберіть розділ "Налаштування".
- Оберіть пункт «Події».



2. Створення події:

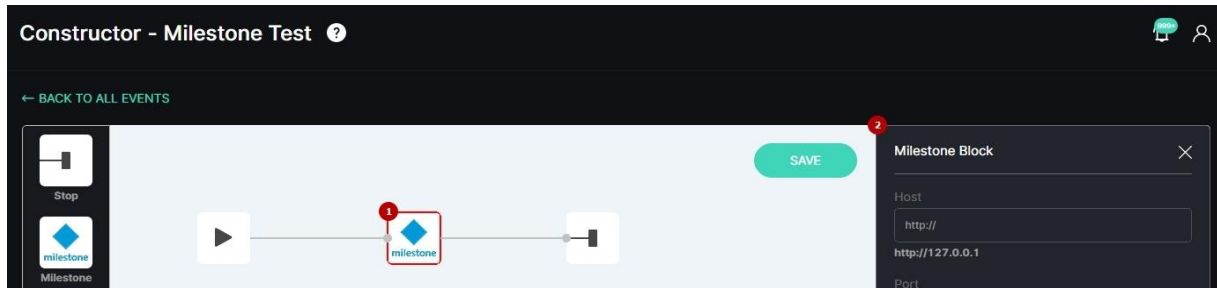
- Натисніть "Створити подію".
-



- Введіть назву події та опис, натисніть "Створити".
-

3. Огляд

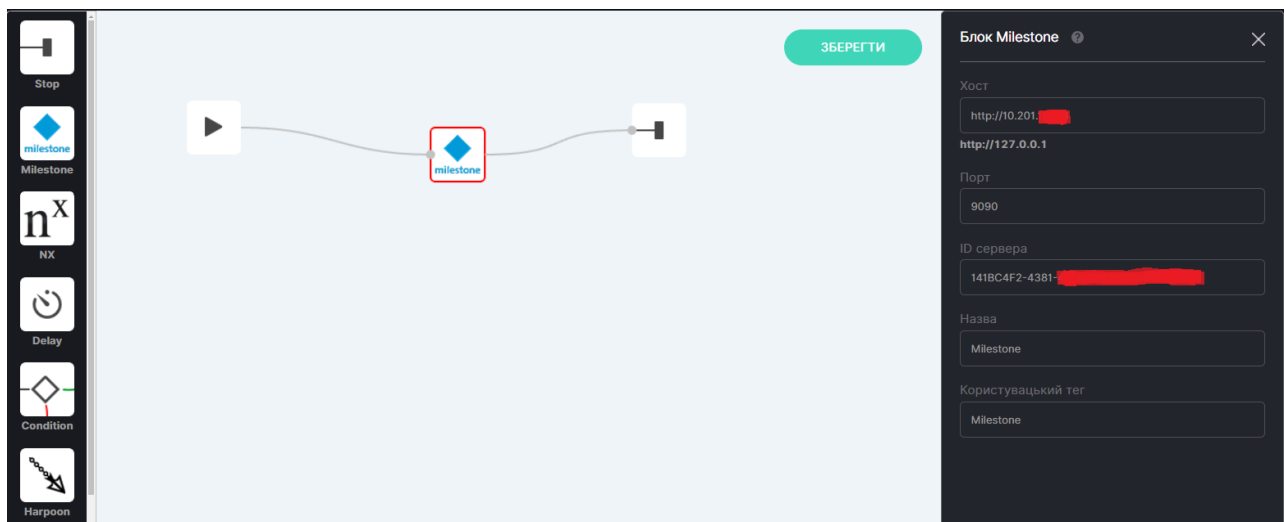
Щоб відкрити блок Milestone, у робочій області Event Manager Constructor:



- Виберіть значок блоку Milestone
- Перегляньте блок Milestone

4. Використання та функціональність

Функціональне меню блоку Milestone дозволяє:

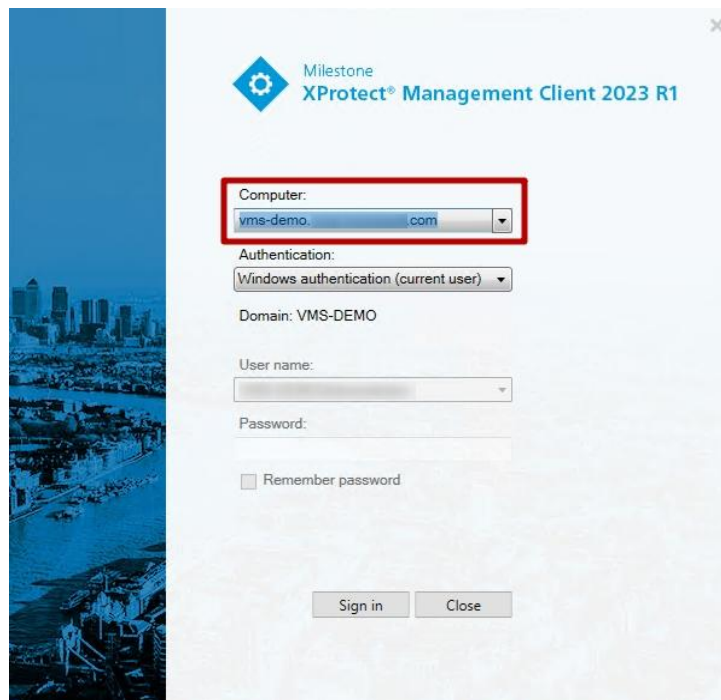


- Введіть ім'я хосту після http://
- Введіть порт
- Введіть ID сервера
- Введіть назву сповіщення про подію
- Введіть спеціальний тег

5. Визначення необхідних значень

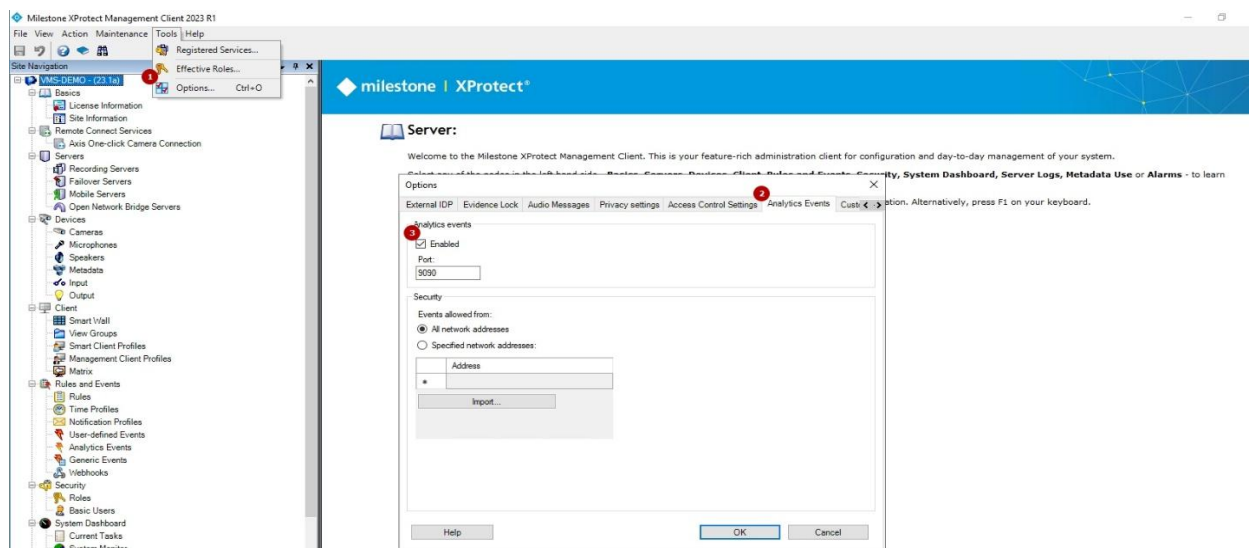
Необхідні значення для заповнення полів у блоці Milestone знаходяться в Milestone XProtect Management Client.

Щоб знайти ім'я хоста, відкрийте Milestone XProtect Management Client і скопіюйте адресу сервера з поля «Комп'ютер»:



Значення порту за замовчуванням – 9090. Однак, щоб переконатися, що доступ до сервера подій XProtect на порту 9090 дозволено, виконайте такі дії:

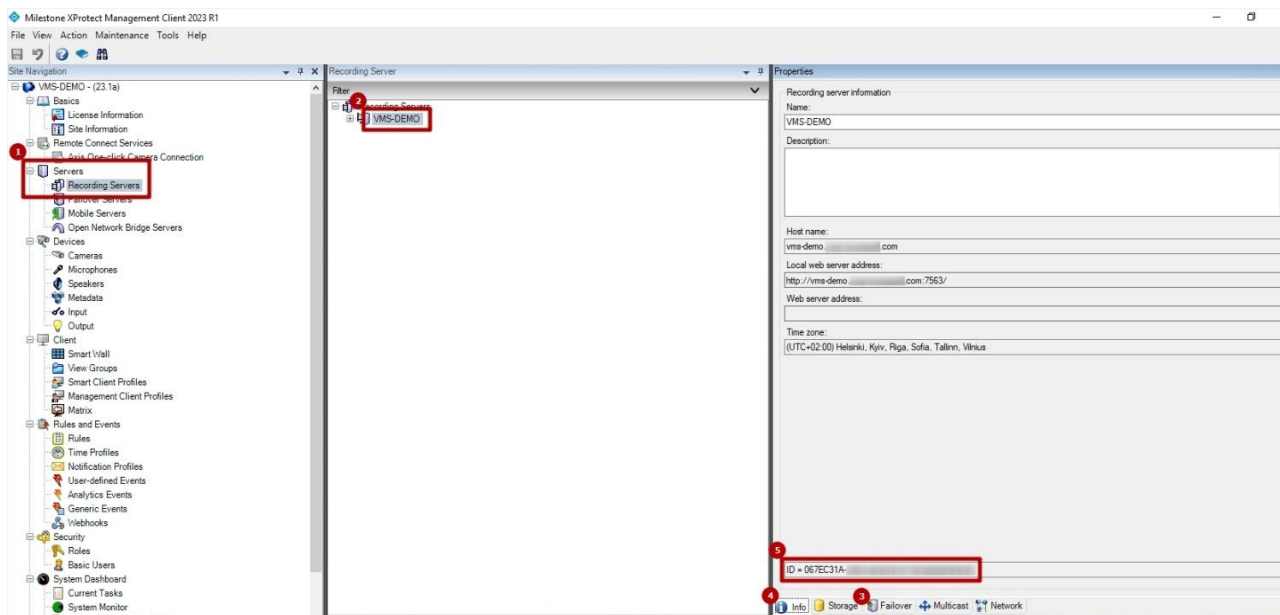
1. Відкрийте вкладку Інструменти на панелі меню та виберіть Параметри зі спадного меню (або натисніть Ctrl + O)
2. Перейдіть на вкладку Події Analytics
3. Поставте прапорець у полі «Увімкнено».



Щоб знайти ідентифікатор сервера, виконайте такі дії:

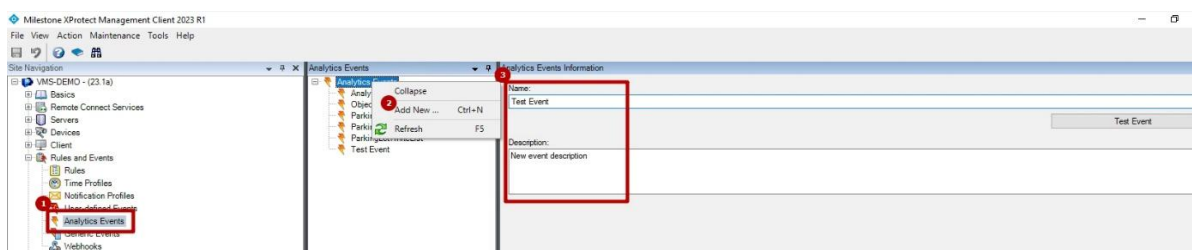
1. Відкрийте розділ Сервери і виберіть пункт Сервери запису.
2. Натисніть назву потрібного сервера запису.
3. Перейдіть на будь-яку іншу вкладку внизу вікна властивостей (наприклад, відновлення після відмови).
4. Утримуючи клавішу Ctrl, клацніть лівою кнопкою миші вкладку «Інформація».

5. Скопіюйте ідентифікатор сервера з поля, що з'явиться.



Якщо сповіщення про події ще не створено, виконайте такі дії, щоб створити нове:

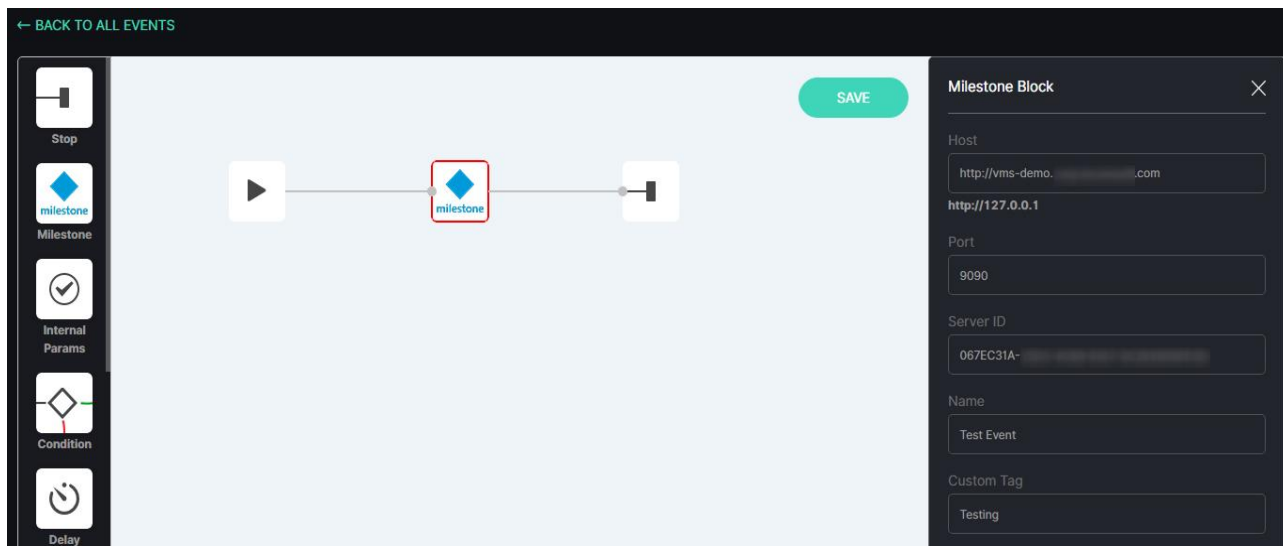
1. Відкрийте розділ «Правила та події» та виберіть пункт «Події Analytics».
2. Клацніть правою кнопкою миші Події Analytics і виберіть Додати новий у спадному меню (або натисніть Ctrl + N)
3. Введіть назву та опис події
4. Натисніть Ctrl + S, щоб зберегти зміни



Щоб отримати назву сповіщення про подію, виберіть створену аналітичну подію та скопіюйте її назву з поля Ім'я.

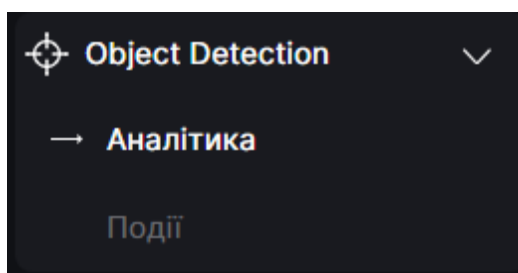
Щоб заповнити поле спеціального тегу, введіть будь-яке значущє значення, яке можна використовувати для подальших цілей.

Використовуйте зображення нижче як візуальне посилання, щоб забезпечити правильне введення значень у поля:



Приклад зі створення та налаштування аналітики розпізнавання об'єктів

Створення аналітики: перейдіть до розділу «Object Detection» у меню.

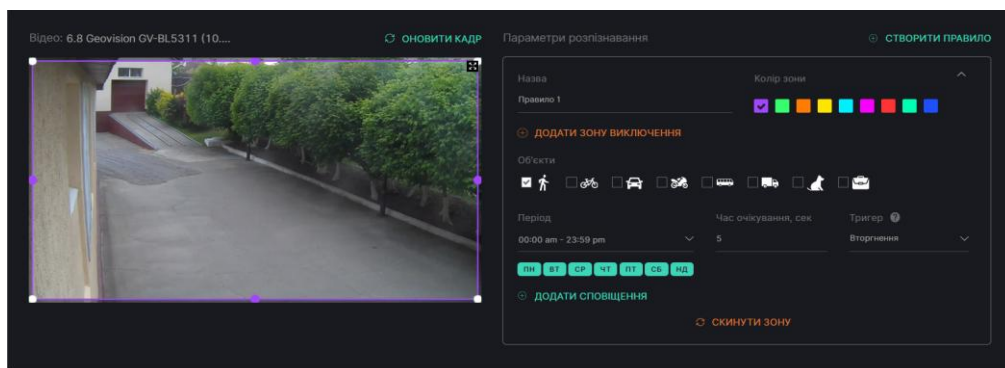


Виберіть «Аналітика» та натисніть «Створити аналітику».



Заповніть поля у вкладках:

Загальні: встановіть відеопотік, налаштуйте параметри розпізнавання.



Обладнання: виберіть апаратне прискорення (CPU/GPU) та інші параметри (для всіх аналітик, це базові налаштування!!!)

Обладнання

☐ CPU ☒ GPU

Декодування

NVDEC ☐

☒ FPS ☐ ? ☐ Ключовий кадр ☐ Раз на X секунд

15

☒ Використовувати виявлення руху для ШІ

Сповіщення: вкажіть параметри сповіщень (в параметри події вказуємо відповідну назву події, яку ми створили для надсилання спрацювань в Milestone).

☒ Системне повідомлення

☒ Відправляти події до Event Manager

Події

1

Додаткові параметри ?

Параметр	Значення
ДОДАТИ ПАРАМЕТРИ	

Дозволи: призначте права доступу ролям і користувачам.

Ролі

Додати роль

Вибрати роль

Користувачі

Додати користувача

Вибрати користувача

За замовчуванням (Активні)

За замовчуваннями	Запустити аналітику	Зупинити аналітику	Редагувати аналітику	Перегляд аналітики	Перегляд подій аналітики
За замовчуваннями	☒	☒	☒	☒	☒

Опис та рекомендації щодо використання програмних модулів відеоаналітики «Incoresoft Vezha»

Розпізнавання номерних знаків (License Plate Recognition, LPR)

Ця технологія може бути використана для відстеження транспортних засобів, автоматичного запису номерних знаків, марки, моделі, кольору, напрямку руху, та країна реєстрації.

Основні характеристики: точність розпізнавання до 99,6%, включаючи знаки низької якості, брудні, розмиті та пошкоджені; підтримка понад 100 країн; типи номерних знаків – звичайні, інверсні, спеціальні, 2- і 3-рядні; інформація про транспортний засіб (марка, модель, колір, напрямок руху, країна, швидкість); необмежена кількість списків; необмежена кількість розпізнаних номерних знаків в одному кадрі. Розмір номерного знаку для розпізнавання (Європа): мінімум 48x12 пікселів (рекомендовано 100x25 пікселів).

Рекомендації по встановленню камер. Встановіть камери з аналітикою розпізнавання номерних знаків на в'їзні та виїзні шляхи пунктів пропуску.

Позиціонування відеокамери: рекомендовано розташувати камеру на висоті 1,5 – 2 метри над дорожньою поверхнею, щоб уникнути освітлення камери сильним світлом фар; мінімізуйте кут між камерою та напрямом руху транспортного засобу, ідеально – встановити камеру над автомобілями, але не занадто високо; рекомендовано тримати загальний кут між камерою та напрямом руху транспортного засобу менше 30°. Приклад правильного встановлення показано на рис. 5.3.

Денний час: відстань до дороги: 0 м; висота камери: 1,5 м; кут 17° на 5 метрах, 8,5° на 10 метрах.





Рисунок 5.3 – Рекомендації по встановленню камер

Нічний час: відстань до дороги: 2 м; висота камери: 1,5 м; кут: 27° на 5 метрах, 14° на 10 метрах.

Таблиця: Кути камери при відстані дороги 0 м.

Висота	5 м	10 м	30 м	50 м	80 м
1,5 м	17°	8,5°	2,9°	1,7°	1,1°
3 м	31°	17°	5,7°	3,4°	2,1°
5 м	45°	27°	9,5°	5,7°	3,6°
7 м	54°	35°	13°	8,0°	5,0°
10 м	63°	45°	18°	11°	7,1°

Таблиця: Кути камери при відстані дороги 2 м

Висота	5 м	10 м	30 м	50 м	80 м
1,5 м	27°	14°	4,8°	2,9°	1,8°
3 м	36°	20°	6,9°	4,1°	2,6°
5 м	47°	28°	10°	6,1°	3,9°
7 м	56°	36°	14°	8,3°	5,2°
10 м	64°	46°	19°	12°	7,3°

Камеру слід спрямувати на дорогу так, щоб відповідні смуги руху були в центрі зображення (рис. 5.4). Це дозволить охопити потрібну кількість смуг, але не більше. Кут нахилу камери слід налаштувати так, щоб номерний знак був паралельним краям зображення.



Рисунок 5.4 – Варіанти кута нахилу камери

Аналітика розпізнавання обличчя (Face Recognition). Аналітика, спрямована на автоматизоване виявлення та ідентифікацію осіб на відеозаписах або онлайн трансляції із подальшим записом осіб у базу даних, використовуючи зображення безпосередньо з камер спостереження. Коли аналітика визначає обличчя, воно записується у базу даних. У випадку наявності у БД особи та співпадіння її фото з отриманим з камери, запису автоматично присвоюється ідентифікатор особи. У випадку відсутності збігів, оператору системи відеоспостереження пропонується ввести дані по особі, що була зафіксована системою при розпізнаванні. Потім можна відфільтрувати ці записи за допомогою фільтрації по певним ідентифікаторам та ознакам, які оператор внесе заздалегідь.

Основні характеристики:

- висока точність ідентифікації, яка досягає 99,35%;
- швидкість ідентифікації до 0,1 секунд з базою даних до 1 мільйона осіб;
- підтримка різних списків, необмежена кількість списків для осіб;
- висока якість розпізнавання (розпізнає обличчя навіть у випадку носіння окулярів, шапок, масок, бороди та помірного повороту голови);
- розпізнавання осіб по розміру – виявлення обличчя з відстанню між очима (IOD) від 10 пікселів, розпізнавання від 21 пікселя (рекомендовано 40 пікселів);
- визначення статі та віку.

Рекомендації по встановленню камер. Встановлюйте камери на висоті приблизно 2-2.5 метри для оптимального огляду обличчя. Розміщуйте камери у місцях з високою прохідністю, наприклад, на входах/виходах, у коридорах та на сходових клітках. Забезпечте достатнє освітлення в місцях встановлення камер для уникнення затемнених або пересвітлених зображень. Використовуйте камери з високою роздільною здатністю для кращої якості зображення.

Детальна інструкція по рекомендаціям для даної аналітики опублікована на порталі it.dpsu.gov.ua за [посиланням](#)

Виявлення об'єктів (Object Detection)

Аналітика відстежує та класифікує понад 50 об'єктів. Надано можливість налаштування певної зони використання аналітики на відео. Є можливість використання триггерів, такі як: кількість людей; вторгнення; контроль присутності або відсутності об'єкта в певних місцях на відео; відсутність об'єкта; присутність об'єкта; виявлення натовпу.

Рекомендації по встановленню камер. Камери слід встановлювати на висоті не менше 2,8 метра над рівнем землі для відкритих просторів або великих внутрішніх приміщень. Налаштуйте камеру під кутом до 30° від горизонталі для оптимальної класифікації об'єктів, не перевищуючи 45°. Монтувати камери на стійкій поверхні, щоб зменшити вібрацію та рух. Камери з вищою роздільною здатністю надають кращу якість зображення для виявлення об'єктів.

Розробником не рекомендується використання PTZ камер, але є можливість тонкого налаштування пресетів, для мінімізації руху камери.

Рекомендована висота установки камери:

3 метри для діапазону 10-15 метрів.

5 метрів для діапазону 15-30 метрів.

7 метрів для діапазону 30-50 метрів.

10 метрів для діапазону 50-80 метрів.

Поле зору камери повинно бути паралельним горизонту, щоб зафіксувати об'єкти в вертикальному положенні. Об'єкти, які рухаються паралельно до поля зору, дають кращі результати. Позиціонуйте камери так, щоб зафіксувати рухливі об'єкти у полі зору протягом принаймні 2 секунд. Використовуйте ширше поле зору для виявлення об'єктів що швидко рухаються для збільшення часу спостереження.

Мінімальний розмір для виявлення:

людина – мінімум 25x40 px, рекомендовано 50x125 px;

автомобіль – мінімум 25x25 px, рекомендовано 150x100 px;

велосипед – мінімум 40x70 px, рекомендовано 90x100 px;

мотоцикл – мінімум 25x30 px, рекомендовано 70x90 px;

автобус – мінімум 90x75 px, рекомендовано 200x150 px;

вантажівка – мінімум 80x70 px, рекомендовано 180x150 px;

тварина – мінімум 30x40 px, рекомендовано 120x140 px;

річ – мінімум 30x40 px, рекомендовано 100x150 px.

Детальна інструкція по рекомендаціям для данної аналітики опублікована на порталі it.dpsu.gov.ua за посиланням

Аналіз трафіку (Traffic Analytics).

Аналітика аналізу трафіку призначена для визначення інтенсивності, кількості та складу транспортного та людського руху. Відстеження потоку, ідентифікація дорожніх інцидентів в момент їх виникнення. Аналітика надає статистику руху транспорту та людей у реальному часі, що дозволяє оперативно реагувати на зміни в русі.

Основні характеристики: мінімальні розміри для виявлення: автомобіль: мінімум 20x15 пікселів, рекомендовано 150x100 пікселів (при роздільній здатності камери 2MPx); людина: мінімум 20x40 пікселів, рекомендовано 50x125 пікселів (при роздільній здатності камери 2MPx); аналітика точно підраховує кількість людей в пунктах пропуску та інших місцях скупчення. Інформаційна панель статистики дозволяє переглядати події по годинах, днях, тижнях та місяцях.

Рекомендації по встановленню камер. Вибирайте точки для встановлення камер, щоб покрити всі основні потоки руху транспорту та пішоходів. Встановлюйте камери на висоті, яка забезпечує максимальний огляд, зазвичай 3-5 метрів для пунктів пропуску та доріг. Використовуйте камери з високою роздільною здатністю (не менше 2MPx) для забезпечення

якісного зображення та коректного аналізу. Забезпечте належне освітлення зон спостереження, особливо у нічний час, для уникнення проблем із виявленням та розпізнаванням об'єктів.

Виявлення руху (Motion Detection). Аналітика надає можливість використання різних правил для виявлення рухомих об'єктів, таких як перетин лінії, мародерства, вторгнення, втрачених об'єктів і відсутніх об'єктів.

Основні можливості: забезпечує аналіз появи сторонніх осіб у визначеній зоні та допомагає запобігати небажаній або непередбачуваній активності в цьому секторі. Підтримує різні типи правил, зокрема перетин лінії, проникнення, залишений предмет чи спроби виведення камери з ладу. Застосовується в аеропортах, на автовокзалах і залізничних станціях для виявлення загублених речей і запобігання потенційним загрозам. Працює як із кольоровими, так і з тепловізійними камерами. Фіксує події з точними датами та часом виявлених порушень.

Рекомендації по встановленню камер. Рекомендуємо встановити дану аналітику по обидва фланги пункту пропуску для ефективного контролю прилеглих територій. Рекомендується встановлювати камери на висоті 3-4 метри. Така висота забезпечить оптимальний огляд території та дозволить уникнути мертвих зон, забезпечуючи максимально точно виявлення руху в зоні моніторингу. Камери слід розташувати таким чином, щоб кут нахилу був не більше 30° від горизонталі, що дозволить покращити точність виявлення руху та мінімізувати хибні спрацьовування.

Виявлення диму та вогню (Smoke & Fire Detection).

Аналітика дозволяє виявляти дим і пожежу на ранній стадії. Цей модуль може бути ефективно використаний як на камерах, встановлених на кордоні, так і на камерах в пунктах пропуску.

Технічні характеристики: мінімальний розмір диму для виявлення: 60x50 пікселів (Ширина*Висота), рекомендований: 100x60 пікселів (Ширина*Висота); мінімальний розмір вогню для виявлення: 30x40 пікселів (Ширина*Висота), рекомендований: 100x60 пікселів (Ширина*Висота).

Рекомендації по встановленню камер. Для оптимальної роботи камер з аналітикою виявлення диму та вогню рекомендується встановлювати їх на висоті 6-10 метрів. Це забезпечить широкий огляд території та дозволить виявити дим або вогонь навіть на віддалених ділянках. Камери повинні бути встановлені з кутом нахилу не більше 30° від горизонталі. Це дозволить уникнути мертвих зон та забезпечить кращий огляд території. Камери слід розміщувати в стратегічно важливих точках, таких як вхідні та вихідні зони пунктів пропуску, місця скупчення людей та транспортних засобів, а також уздовж кордону для моніторингу великих відкритих територій. Забезпечте достатнє освітлення в зоні моніторингу для покращення якості відеозаписів, особливо вночі. Використання біспектральних камер може бути корисним для виявлення диму та вогню у темний час доби.

Інтелектуальна система відстеження (Smart Tracking System)

Аналітика Smart Tracking System аналізує відео та використовує метадані для швидкого знаходження конкретної особи як у приміщенні, так і на відкритому повітрі.

Основні характеристики: відстеження особи за допомогою декількох камер; швидкий пошук потрібної особи; пошук за атрибутами (колір одягу, сумка, волосся, капелюх, стать та вік); пошук загублених дітей у торгових центрах та громадських місцях;

Рекомендації по встановленню камер. Камери слід встановлювати на висоті 2-3 метри для внутрішніх зон пункту пропуску та 3-6 метрів для зовнішніх зон. Камери повинні бути встановлені під кутом 15-30 градусів для зовнішніх камер і 30-45 градусів для внутрішніх камер відносно горизонталі. Використовуйте камери з широким кутом огляду (90-120 градусів) для загального спостереження та камери з вузьким кутом огляду (45-60 градусів) для використання аналітики в конкретних зонах. Мінімальний розмір особи для виявлення: 20x40 пікселів (ШxВ), рекомендовано: 50x125 пікселів (ШxВ) (роздільна здатність камери 2MPx).

Виявлення зброї (Gun Detection)

Аналітика Gun Detection призначена для виявлення вогнепальної зброї та ножів у реальному часі.

Основні характеристики: визначення типу зброї (пістолети, рушниці, ножі); перевірка наявності чи відсутності зброї у вказаний проміжок часу в обраній зоні; розрізнення звичайних повсякденних предметів та різних об'єктів загрози.

Рекомендації по встановленню камер.

Для ефективної роботи аналітики необхідно забезпечити наступні умови:

Мінімальний розмір об'єкта для виявлення: 20x40 пікселів (ШxВ).

Рекомендований розмір об'єкта: 50x125 пікселів (ШxВ).

Камери повинні мати роздільну здатність не менше 2 МП.

Камери слід розміщувати на висоті від 2,5 до 3 метрів, забезпечуючи оглядову зону без сліпих зон.

Виявлення військової техніки (Vezha IV - Military Detection of Military Equipment)

Аналітика призначена для виявлення та ідентифікації військової техніки в реальному часі. Цей модуль виявляє та класифікує різні типи військових транспортних засобів і техніки.

Основні характеристики. Аналітичні алгоритми дозволяють ідентифікувати широкий спектр зразків військової техніки, зокрема танки, бронетранспортери, артилерійські системи та інші типи бойових машин. Виявлення та класифікація об'єктів здійснюється в режимі реального часу, що дозволяє оперативно реагувати на загрози. Аналітика дозволяє

аналізувати не лише присутність техніки, але й її активність у визначених зонах. Аналітика здатна точно відрізняти військову техніку від цивільних транспортних засобів, мінімізуючи кількість хибних спрацьовувань.

Рекомендації по встановленню камер. Об'єкт повинен мати мінімальні розміри 30х30 пікселів для забезпечення точної ідентифікації (при роздільній здатності камери 2 МП). Для оптимального виявлення рекомендований розмір об'єкта становить від 100х100 пікселів. Камери повинні мати роздільну здатність не менше 2 МП для забезпечення високої якості зображення. Камери слід розміщувати на висоті від 5 до 10 метрів, залежно від місцевості та потреби охоплення зони спостереження. Вибирайте точки для встановлення камер, такі як дороги, пункти пропуску, прикордонна зона, в'їзди та виїзди з військових баз та інших критичних об'єктів.

Контрольні питання до розділу IV

1. Значення відеоспостереження в діяльності Національної поліції України.

2. Нормативно-правова основа застосування відеоспостереження органами та підрозділами Національної поліції України.

3. Застосування безпілотних літальних апаратів в діяльності Національної поліції України.

4. Застосування відеореєстраторів в діяльності органів та підрозділів поліції.

5. В чому виникає унікальність комплексу «ЗІР Про»?

6. Які основні компоненти входять до складу системи «ЗІР Про»?

7. Як працює система ідентифікації цілей на базі нейромереж?

8. Які переваги має використання тепловізора і оптичного зуму в комплексі?

9. Що таке біспектральні PTZ-камери і яка їхня функціональна роль?

10. Як система «ЗІР Про» використовує для протидії дронам-шахедам?

11. Які сценарії застосування комплексу з урахуванням різних погодних умов?

12. Як інтегровані рішення щодо відеоаналітики підвищують ефективність контролю кордону?

13. За якими принципами керується автоматичне виявлення порушення?

14. Які переваги модульної конструкції комплексу?

15. Які режими роботи передбачені для системи «ЗІР Про»?

16. Які рекомендації щодо використання та сервісного комплексу?

17. Як працює програмна платформа Incoresoft Vezha?

18. Що таке пропускна здатність каналів зв'язку і як її розраховувати?

19. Які основні вимоги до налаштування камери відеоспостереження?

20. Які алгоритми використовують для відеоаналізу і як вони реалізовані?

21. Які функції має модуль відеоаналітики «Incoresoft Vezha»?

22. Як забезпечити безпеку передачі та зберігання відеоінформації?

- 23. Які ризики виникають при масштабуванні системи відеоспостереження?
- 24. Як налаштувати мережеві пристрої для оптимальної роботи системи?
- 25. Що виконати при виборі та підключенні серверів і камер?
- 26. Які рекомендації щодо використання відеоаналітичних модулів у практиці?
- 27. Як реалізувати обробку подій за допомогою сервера подій?
- 28. Як використовувати систему для оперативного реагування на сигнали?

V. МІЖНАРОДНИЙ ДОСВІД ПОБУДОВИ ЦЕНТРАЛІЗОВАНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОАНАЛІТИКИ

5.1. Модель «Тотального контролю»: китайський досвід централізованого державного нагляду

В епоху цифрової трансформації держави по всьому світу активно впроваджують централізовані системи моніторингу та управління даними для підвищення національної безпеки та ефективності державного апарату. Однією з найбільш комплексних та технологічно просунутих моделей є китайська система «Тотального контролю». Ця модель характеризується безпрецедентним рівнем централізації даних під егідою держави та глибокою інтеграцією технологій штучного інтелекту для всебічного нагляду за суспільством. Ключовими елементами цієї архітектури є проекти «Золотий щит» та «Небесне око» (Tianwang або Skynet), які разом створюють єдину екосистему тотального цифрового моніторингу.

«Золотий щит» (Golden Shield Project), ініційований на початку 2000-х років, став фундаментом для створення інфраструктури цифрового контролю в Китаї. Його основною метою було створення загальнонаціональної мережі для обміну даними між правоохоронними органами та іншими державними структурами. Проект включав розробку масивних баз даних, що містять персональну інформацію про громадян, та систему фільтрації інтернет-трафіку, відому як "Великий китайський файрвол". Це дозволило уряду не лише збирати дані, але й активно контролювати інформаційний простір, блокуючи доступ до небажаних іноземних ресурсів та цензуруючи внутрішній контент.

«Небесне око» (Tianwang/Skynet) є логічним продовженням та технологічним розширенням «Золотого щита». Запущений у 2015 році, цей проект фокусується на фізичному спостереженні за допомогою найбільшої у світі мережі камер відеоспостереження. Станом на 2020-ті роки в Китаї було встановлено понад 600 мільйонів камер, інтегрованих у єдину платформу. На відміну від традиційних систем відеоспостереження, «Небесне око» активно використовує технології штучного інтелекту для аналізу відеопотоків у режимі реального часу.

Основою моделі «Тотального контролю» є кілька ключових принципів. Насамперед, це максимальна централізація під державним контролем. Усі дані, що збираються системами, акумулюються в державних дата-центрах під повним контролем Комуністичної партії Китаю. Це виключає можливість незалежного аудиту та створює асиметричну владну динаміку, де держава володіє вичерпною інформацією про своїх громадян.

Ефективність системи досягається завдяки інтеграції з іншими базами даних та перехресному аналізу даних з різних джерел. Відео з камер «Небесного ока» співставляється з базами даних соціального рейтингу, що дозволяє автоматично фіксувати порушення (наприклад, перехід дороги в недозволеному місці) і миттєво знижувати рейтинг громадянина. Дані з

транспортних систем (номери автомобілів, дані про переміщення громадським транспортом) та банківських систем (інформація про транзакції) також інтегруються в єдиний профіль, створюючи повну картину життя та поведінки людини.

Технологічний стек китайської моделі є одним з найсучасніших у світі. Система «Тотального контролю» побудована з масовим використанням AI-відеоаналітики, розпізнавання облич у реальному часі, аналізу поведінки (Behavioral Analysis) та обробки великих даних (Big Data). Системи на базі штучного інтелекту аналізують відео в реальному часі для ідентифікації нестандартної поведінки, скупчень людей або залишених предметів. Камери здатні з високою точністю (до 99.8%) ідентифікувати обличчя людей у натовпі за лічені секунди, співставляючи їх із централізованою базою даних громадян. Це дозволяє відстежувати переміщення конкретних осіб по всій країні. Алгоритми аналізують не лише обличчя, але й ходу, жести та інші поведінкові патерни для ідентифікації осіб навіть за умов поганої видимості або коли обличчя приховане. Обробка великих обсягів даних (петабайти інформації щодня) стала можливою завдяки використанню технологій великих даних. Це дозволяє виявляти неочевидні зв'язки та прогнозувати потенційні загрози на основі аналізу сукупної інформації.

Результати впровадження моделі «Тотального контролю» є вражаючими з точки зору правоохоронної діяльності. Китайські державні ЗМІ регулярно повідомляють про високі показники розкриття злочинів завдяки використанню цих систем. Здатність швидко ідентифікувати та затримувати підозрюваних, знаходити зниклих людей та припиняти правопорушення значно зросла. Система також відіграє роль потужного стримуючого фактору, оскільки громадяни усвідомлюють постійну присутність державного нагляду.

Водночас ця модель є об'єктом гострої критики з боку міжнародних правозахисних організацій та експертів з цифрових свобод. Головні ризики полягають у наступному: система фактично ліквідує поняття приватного життя, оскільки будь-яка дія людини в публічному просторі фіксується, аналізується та зберігається; модель «Тотального контролю» може використовуватись для придушення інакомислення, переслідування політичних опонентів, активістів та етнічних меншин (зокрема, уйгурів у Сіньцзяні). Можливість анонімності та свободи вираження поглядів суттєво обмежується. Інтеграція з системою соціального рейтингу перетворює нагляд на інструмент соціального контролю, заохочуючи «правильну» поведінку та караючи за відхилення від встановлених норм, що може призвести до самоцензури та конформізму в суспільстві.

Таким чином, китайська модель «Тотального контролю» демонструє парадигмальний зсув у державному управлінні, де технології стають основним інструментом забезпечення стабільності та контролю. Незважаючи на статистично високі показники ефективності у боротьбі зі злочинністю, модель породжує серйозні етичні та правові дилеми, ставлячи під загрозу основи прав людини, такі як приватність, свобода пересування та свобода

слова. Це робить її одним з найсуперечливіших явищ сучасної цифрової епохи.

5.2. Модель «Публічно-приватного партнерства» (на прикладі Великої Британії та США)

На відміну від моделі тотального державного контролю, у багатьох західних демократіях розвинувся інший підхід до побудови централізованих систем безпеки – модель публічно-приватного партнерства (ППП). Ця модель ґрунтується на співпраці між державними структурами, насамперед правоохоронними органами, та приватним сектором. Замість створення єдиної державної мережі з нуля, PPP передбачає інтеграцію вже існуючих приватних та муніципальних систем відеоспостереження в єдину аналітичну платформу.

Яскравими прикладами реалізації цієї моделі є системи безпеки у великих мегаполісах, таких як Лондон «Ring of Steel» та Чикаго «Virtual Shield».

Система «Ring of Steel» («Сталеве кільце») у Лондоні, Велика Британія, була сформована як відповідь на зростання терористичних загроз, зокрема після серії вибухів, організованих Ірландською республіканською армією у 1990-х роках. Під цією назвою розуміють розгалужену мережу камер відеоспостереження, що охоплює периметр фінансового центру міста – лондонського Сіті. На початковому етапі її головним завданням був контроль транспортних потоків на в'їздах до цього району.

Згодом система значно розширилася і сьогодні є однією з наймасштабніших у світі. Вона об'єднує камери, що належать: транспортній системі Лондона (TfL) (камери на дорогах, у метро, автобусах); муніципалітету (камери на вулицях, у парках, на громадських будівлях) та приватним компаніям (камери на офісних будівлях, у торгових центрах, магазинах).

Проект «Virtual Shield» («Віртуальний щит») у Чикаго, США, був розгорнутий після подій 11 вересня 2001 року й мав на меті інтеграцію тисяч камер, розміщених у різних частинах міста. Завдяки цій системі поліція отримала можливість у режимі реального часу переглядати відеопотоки не лише з муніципальних камер, а й із пристроїв, установлених у приватних закладах – школах, лікарнях, спортивних аренах і на підприємствах, що добровільно долучилися до програми.

Основою моделі публічно-приватного партнерства є інтеграція, а не тотальне володіння. Ключові принципи побудови системи є: добровільна співпраця; контрольований доступ; єдина мережа. Приватні власники камер (бізнеси, освітні заклади) надають доступ до своїх систем правоохоронцям на добровільній основі. Поліція не має постійного доступу до всіх приватних камер. Доступ, як правило, надається за запитом у разі виникнення інциденту або надзвичайної ситуації. Це регулюється чіткими юридичними протоколами для захисту приватності. Хоча камери належать різним

власникам, їхні відеопотоки інтегруються в єдину платформу, що дозволяє операторам у ситуаційному центрі мати цілісну картину подій.

Технологічний стек цієї моделі спрямований на інтеграцію та аналіз даних з різномірних джерел. Ключовою технологією є ANPR (Automatic Number Plate Recognition), яка використовується в «Ring of Steel». Системи автоматичного розпізнавання номерних знаків дозволяють відстежувати рух транспортних засобів, перевіряти їх за базами даних (викрадені авто, порушники) та фіксувати в'їзд/виїзд із певної зони. Технології VMS (Video Management System) та PSIM (Physical Security Information Management) є "мозком" системи. Вони дозволяють об'єднувати відеопотоки з камер різних виробників, а також інтегрувати інші датчики (сигналізації, датчики пострілів, системи контролю доступу) в єдиний інтерфейс. У спеціалізованих центрах управління (ситуаційних центрах) оператори в режимі реального часу відстежують ситуацію на моніторах, аналізують дані з різних систем та координують дії екстрених служб.

Модель публічно-приватного партнерства має свої переваги та недоліки. Систему можна легко розширювати, підключаючи нових партнерів, без значних капіталовкладень з боку держави. Використання вже існуючої приватної інфраструктури значно дешевше, ніж побудова власної мережі «з нуля». Інтеграція наявних систем дозволяє значно прискорити впровадження комплексних заходів безпеки.

До недоліків слід віднести те, що часто камери та програмне забезпечення різних виробників є несумісними. Інтеграція таких різномірних систем потребує значних зусиль та спеціалізованих програмних рішень (як-от PSIM). Виникають складні питання щодо захисту приватних даних. Необхідно розробити чіткі правові рамки, які б регулювали, хто, коли і на яких підставах може отримувати доступ до відео з приватних камер, щоб уникнути зловживань. Державні органи не можуть повністю контролювати якість та технічний стан приватних камер. Власник може вимкнути камеру або недбало ставитися до її обслуговування, що знижує загальну надійність системи.

Таким чином, модель публічно-приватного партнерства є ефективним компромісом між потребами безпеки та економічними реаліями, однак її успішна реалізація вимагає вирішення складних технологічних та юридичних завдань.

5.3. Модель «Збалансованого підходу та захисту даних» (на прикладі країн ЄС та Скандинавії)

На противагу моделі тотального державного контролю, країни Європейського Союзу, зокрема Німеччина та скандинавські держави, розвивають принципово інший підхід до побудови централізованих систем безпеки. Ця модель, яку можна умовно назвати «Збалансованим підходом», ставить за мету досягнення ефективності у правоохоронній діяльності, не жертвуючи при цьому фундаментальними правами і свободами громадян,

зокрема правом на приватність. В основі цього підходу лежить потужна законодавча база, децентралізація контролю та високий рівень громадської довіри.

Основою європейського підходу виступає Загальний регламент із захисту даних (GDPR), що набув чинності у 2018 році. Цей нормативний акт сформував глобальний орієнтир у сфері захисту персональної інформації. На відміну від китайської моделі, де контроль над даними зосереджений у держави, GDPR виходить із принципу, що персональні дані належать конкретній особі та підлягають захисту відповідно до її прав та інтересів.

Європейський підхід до захисту персональних даних базується на основних принципах GDPR – законності, справедливості та прозорості. Кожна операція з даними повинна спиратися на чітко визначену правову підставу, а громадянам мають бути відкрито повідомлені відомості про те, які саме дані збираються, з якою метою та ким. Збирання інформації допускається лише для конкретних, заздалегідь визначених і законних цілей, а використання цих даних поза межами первинної мети суворо заборонене. Так, відомості з транспортних камер не можуть автоматично застосовуватися для аналізу потенційної участі людини у мирних зібраннях. Органи влади мають право отримувати тільки той мінімальний обсяг даних, який є критично необхідним для виконання визначеної функції, – принцип «накопичувати все про всяк випадок» у цьому контексті неприйнятний. Крім того, громадяни мають право вимагати видалення своїх персональних даних у випадках, коли відсутні законні підстави для їх подальшого зберігання.

На відміну від централізованої моделі, яка функціонує в Китаї, європейські системи безпеки здебільшого мають децентралізовану структуру. Інформація, що надходить від різних суб'єктів – поліції, транспортних служб, муніципалітетів – зазвичай зберігається у відокремлених базах даних, які не мають прямого взаємозв'язку. Їх об'єднання можливе лише за умов наявності судового дозволу або іншої достатньо обґрунтованої правової підстави, що стосується конкретної справи. Такий підхід створює технічні й юридичні бар'єри, які унеможливають масове стеження.

У кожній державі-члені ЄС функціонують незалежні органи із захисту даних (Data Protection Authorities), що здійснюють контроль за дотриманням вимог GDPR. Ці установи мають широкі повноваження: вони проводять перевірки як державних, так і приватних структур, розглядають звернення громадян та можуть накладати значні фінансові санкції за порушення регламенту. Їхня незалежність від органів влади виконує роль важливого механізму запобігання зловживанням.

Використання технологій штучного інтелекту, зокрема систем розпізнавання облич у режимі реального часу в публічному просторі, стало предметом активних суспільних і політичних дискусій. У ряді країн, наприклад у Німеччині, такі технології жорстко обмежені або дозволені лише в межах антитерористичних заходів за рішенням суду. Таким чином, європейська модель тяжіє до застосування «постфактум» аналізу (наприклад,

ідентифікація підозрюваного за архівними відеозаписами), а не до превентивного масового моніторингу.

Німеччина, маючи трагічний історичний досвід тоталітарних режимів (Гестапо та Штазі), виробила одну з найсильніших у світі культур захисту приватного життя. Федеральний конституційний суд Німеччини неодноразово ухвалював рішення, що обмежували можливості держави зі збору даних, підкреслюючи «право на інформаційне самовизначення». Будь-яка ініціатива щодо посилення відеоспостереження чи збору даних нашо́вхується на потужний опір громадянського суспільства та ретельний парламентський контроль.

Скандинавські країни (Швеція, Данія, Норвегія, Фінляндія) демонструють модель, що базується на високому рівні суспільної довіри до державних інституцій. Громадяни готові надавати державі певні дані, наприклад, для ефективного функціонування цифрових державних послуг, але лише за умови абсолютної прозорості та підзвітності. Скандали, пов'язані з витоком даних або зловживанням ними, викликають значний суспільний резонанс і можуть призвести до серйозних політичних наслідків для уряду.

Сильними сторонами моделі є високий рівень захисту прав людини, прозорості та стимулювання інновацій у сфері кібербезпеки. Модель забезпечує надійний захист приватності та інших фундаментальних свобод, що є основою демократичного суспільства. Діяльність правоохоронних органів перебуває під постійним громадським та юридичним контролем, що знижує ризики корупції та зловживань. Жорсткі вимоги GDPR спонукають до розробки передових технологій захисту даних (наприклад, анонімізація, псевдонімізація, шифрування).

Серед ключових викликів і критичних зауважень щодо європейської моделі часто називають необхідність отримання численних дозволів та проходження бюрократичних процедур, що може уповільнювати хід розслідувань порівняно з системами, де доступ до даних забезпечується миттєво. Додатковою проблемою є боротьба з транскордонною злочинністю: відмінності у національних підходах до імплементації GDPR та правилах обміну інформацією між державами-членами створюють бар'єри для ефективної координації спільних поліцейських дій. Також суворі обмеження на використання технологій штучного інтелекту можуть призводити до того, що правоохоронні органи ЄС опиняються у менш вигідному технологічному становищі порівняно з відповідними структурами в авторитарних державах, де подібні технології застосовуються значно ширше.

Таким чином, «Збалансований підхід» країн ЄС є складною, багатогранною системою, яка намагається знайти компроміс між двома важливими суспільними благами – безпекою та свободою. Вона є яскравим прикладом того, як технологічний прогрес може бути інтегрований у суспільство не на шкоду демократичним цінностям.

5.4. Інноваційні моделі (на прикладі Сінгапуру та ОАЕ)

Якщо модель Китаю можна охарактеризувати як «тотальну», то підходи Сінгапуру та ОАЕ представляють собою модель «розумного» або «сервісного» спостереження. Їхня головна мета – не стільки політичний контроль, скільки підвищення ефективності управління містом (smart city), безпеки та якості життя через інноваційне використання даних. Акцент робиться на аналізі поведінки *натовпу* та *інфраструктури*, а не окремих осіб, хоча технології для індивідуального відстеження також присутні.

Сінгапур впроваджує відеоспостереження як частину глобальної програми «Smart Nation», головною моделлю якої є «Модель Розумної Держави». Ключовий проєкт «Safe City Platform» передбачає розгортання камер у громадських місцях (HDB estates, громадський транспорт). Система розрахована на запобігання інцидентам (злочинність, тероризм, порушення громадського порядку) та швидке реагування. Відеодані інтегруються з системами швидкого реагування поліції, пожежних та медиків. Замість розпізнавання окремих облич, система аналізує потоки людей, виявляючи скупчення, аномальну рухливість та потенційні небезпечні ситуації (наприклад, тисняву). Використання даних жорстко регулюється законами, зокрема Personal Data Protection Act (PDPA), що обмежує несанкціоноване використання персональної інформації.

Модель використовує такі технології: AI-відеоаналітика для моніторингу парковок, дорожнього руху та зон високого ризику; аналіз шаблонів поведінки натовпу; розпізнавання облич застосовується, але в більш обмеженому та регульованому форматі, ніж у Китаї.

Результатами впровадження моделі є те, що у Сінгапурі один з найнижчих у світі рівнів злочинності. Оптимізація дорожнього руху та розподілу ресурсів. Високий рівень довіри суспільства до дій влади, заснований на ефективності та верховенстві права.

В ОАЕ (Дубай та Абу-Дабі) використовується модель «Кібербезпечного Міста-Майбутнього».

ОАЕ, змагаючись за статус глобального хабу, роблять ставку на найновітніші технології для забезпечення безпеки як умови економічного процвітання. Ключовими проєктами є програма «Dubai Safe City» та система «Falcon Eye» в Абу-Дабі.

Система відеоспостереження використовує AI для аналізу даних із камер, соціальних мереж та історії інцидентів, щоб прогнозувати ймовірність злочинів у певних районах і в певний час. Камери інтегровані в єдину систему з розумними ліхтарями, датчиками шуму та забруднення. Тестування та впровадження технологій для міст майбутнього, таких як літальні таксі та автономний транспорт, що вимагає нових підходів до безпеки.

У системі використано технології розпізнавання облич і автомобільних номерів у реальному часі по всьому місту, прогностичні алгоритми на основі штучного інтелекту, віртуальні периметри (Geofencing). Створення віртуальних кордонів навколо критичних об'єктів, при перетині яких система

подає сигнал. Розпізнавання типів руху та поведінки, що дозволяє ідентифікувати людину навіть при відсутності чіткого зображення обличчя.

Дубай посідає одне з найвищих місць у рейтингах безпеки міст. Завдяки системам відеоспостереження відбулося різке скорочення часу реагування екстрених служб та запобігання серйозним інцидентам завдяки прогностичним моделям.

Однак, подібно до Китаю, існують занепокоєння щодо відсутності прозорих механізмів контролю за цими системами та потенційного використання їх для політичного нагляду.

Таблиця 2.1

Порівняльний аналіз сучасних систем відеоспостереження

Критерій	Модель "Тотального контролю" (Китай)	"Розумна" модель (Сінгапур)	"Кібербезпечна" модель (ОАЕ)
Головна мета	Соціально-політична стабільність, контроль	Ефективність управління, якість життя	Економічна безпека, глобальна конкурентоспроможність
Фокус аналізу	Окремі особи (цифровий двійник)	Поведінка натовпу, потоки, інфраструктура	Прогнозування подій, інтеграція інфраструктурою
Правове середовище	Слабкий захист приватності, підпорядкованість державі	Сильне законодавство про захист даних (PDPA)	Змішана ситуація: передові технології при авторитарному правлінні
Соціальний ефект	Ефект страху, самоцензура	Ефект безпеки, довіра	Ефект технологічності, забезпечення комфорту

Таким чином інноваційні моделі Сінгапуру та ОАЕ (табл. 2.1) демонструють еволюцію відеоспостереження від пасивного фіксатора подій до активного, інтелектуального інструменту управління містом. Головна відмінність від китайської моделі полягає в акценті на аналізі агрегованих даних та сервісній складовій, спрямованій на підвищення комфорту та безпеки всіх мешканців, а не на цільовому контролі за окремими громадянами. Однак, навіть у цих моделях залишаються виклики, пов'язані з балансуванням між безпекою, приватністю та свободою в епоху розумних міст.

Контрольні питання до розділу V

1. Що розуміється під терміном «відеоспостереження» (CCTV) згідно з визначенням у посібнику?
2. Які державні стандарти України регламентують застосування систем відеоспостереження охоронного призначення?
3. Перелічіть основні компоненти системи відеоспостереження за пропонованою класифікацією.
4. Які головні завдання сучасних систем відеоспостереження?
5. Опишіть першу задокументовану промислову систему CCTV та її призначення (1942 рік).
6. Яка комерційна система CCTV з'явилася в США у 1949 році та для яких об'єктів вона призначалася?
7. Які ключові інновації з'явилися в системах відеоспостереження у 1960–1970-х роках?
8. Як вплинуло впровадження ПЗС-матриць на розвиток систем відеоспостереження наприкінці 1980-х років?
9. Які основні зміни відбулися в системах відеоспостереження у 1980–1990-х роках (перехід до цифрових технологій)?
10. Опишіть ключові особливості IP-відеоспостереження у 2000-х роках.
11. Які тенденції розвитку інтелектуальних систем відеоспостереження характерні для 2010-х років і сьогодення?
12. Перелічіть основні тенденції майбутнього розвитку систем відеоспостереження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kubaienko A., Okhrimenko I., Kryzhanovska O. Modernization of the law enforcement system at the current stage of digital transformation. *Journal of Law and Political Sciences*, 2022. P. 386.
2. Калугін В. Ю., Форос Г. В. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України : науково-практичні рекомендації. Одеса : ОДУВС, 2025. 84 с.
3. Кириченко О. В., Хмеленко В. В. Принципи оперативно-розшукового запобігання злочинам. Монографія / О. В. Кириченко, В. В. Хмеленко. Київ: Центр учбової літератури, 2020. 160 с.
4. Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) від 04.11.1950 р. № 995_004. (Ратифіковано Законом № 475/97-ВР від 17.07.97). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
5. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <http://zakon.rada.gov.ua/laws/show/254к/96-ВР>
6. Крижановська О. В. Взаємодія Національної поліції з силами безпеки та оборони як основа правопорядку в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2025. № 7. С. 402.
7. Порядок проведення масових заходів на території Київської області в умовах правового режиму воєнного стану. URL: <https://koda.gov.ua/wp-content/uploads/2022/07/poryadok-provedennya-masovyh-zahodiv-na-terytorii-kyivskoї-oblas.pdf>
8. Притула А. М. Оперативно-розшукові відділи Державної прикордонної служби України : сутність та призначення. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 21. С. 95.
9. Про державну прикордонну службу України : Закон України від 03.04.2003 р. № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15#Text>
10. Про доступ до публічної інформації : Закон України від 13.01.2011р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
11. Про затвердження Інструкції з організації діяльності дільничних офіцерів поліції та поліцейських офіцерів громад : Наказ МВС України від 28.07.2017 р. № 650. URL: <https://zakon.rada.gov.ua/laws/show/z1041-17#Text>.
12. Про затвердження Інструкції з організації роботи підрозділів Національної поліції України із забезпечення безпечного освітнього середовища в закладах загальної середньої освіти : Наказ МВС України від 01.10.2024 р. № 663. URL: <https://zakon.rada.gov.ua/laws/show/z1590-24#Text>
13. Про затвердження Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України : Наказ МВС України від 19.12.2017 р. № 1044. URL: <https://zakon.rada.gov.ua/laws/show/z0686-18#Text>
14. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають

функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : Наказ МВС України від 18.12.2018 р. № 1026. URL: <https://zakon.rada.gov.ua/laws/show/z0028-19#Text>

15. Про затвердження Інструкції про порядок використання автоматичної фото- і відеотехніки під час виконання службових обов'язків посадовими і службовими особами Державної прикордонної служби України : Наказ МВС України від 04.04.2019 р. № 244 (Зареєстровано в Міністерстві юстиції України 22 квітня 2019 р. за № 419/33390). URL: <https://zakon.rada.gov.ua/laws/show/z0419-19#Text>

16. Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах : Постанова Кабінету міністрів України від 21.11.2018 р. № 975. URL: <https://zakon.rada.gov.ua/laws/show/975-2018-%D0%BF#n15>

17. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України : Наказ Адміністрації ДПСУ від 30.09.2008 р. № 810 із змінами, внесеними згідно з Наказом Адміністрації Державної прикордонної служби № 750 (z0959-10) від 05.10.2010. URL: <https://zakon.rada.gov.ua/laws/show/z1086-08#Text>

18. Про затвердження Положення про підрозділи поліції особливого призначення : Наказ МВС України від 04.12.2017 р. № 987. URL: <https://zakon.rada.gov.ua/laws/show/z1565-17#Text>

19. Про затвердження Порядку забезпечення охорони об'єктів органами поліції охорони на договірних засадах : Наказ МВС України від 14.12.2022 р. № 816. URL: <https://zakon.rada.gov.ua/laws/show/z0126-23#Text>

20. Про затвердження Порядку організації взаємодії Національної гвардії України та Національної поліції України під час забезпечення (охорони) публічної (громадської) безпеки і порядку : Наказ МВС України від 10.08.2016 р. № 773. URL: <https://zakon.rada.gov.ua/laws/show/z1223-16#Text>

21. Про затвердження Порядку проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ : Постанова Кабінету Міністрів України від 22.05.2019 р. № 507. URL: <https://zakon.rada.gov.ua/laws/show/507-2019-%D0%BF#Text>

22. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

23. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

24. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

25. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

26. Про Національну гвардію України : Закон України від 13.03.2014 р. № 876-VII. URL: <https://zakon.rada.gov.ua/laws/show/876-18#Text>

27. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: <http://zakon3.rada.gov.ua/laws/show/580-19>

28. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

29. Про організацію службової діяльності поліції охорони з питань забезпечення фізичної охорони об'єктів : Наказ МВС України від 07.07.2017р. № 577. Дата оновлення: 27.11.2018. URL: <https://zakon.rada.gov.ua/laws/show/z0989-17#n21>

30. Про особливості забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольних матчів: Закон України від 08.07.2011 р. № 3673-VI. URL: <https://zakon.rada.gov.ua/laws/show/3673-17#Text>

31. Про правовий режим воєнного стану : Закон України від 12.05.2015р. № 389-VIII. URL : <https://zakon.rada.gov.ua/laws/show/389-19#Text>

32. Про практику розгляду судами клопотань про визнання й виконання рішень іноземних судів та арбітражів і про скасування рішень, постановлених у порядку міжнародного комерційного арбітражу на території України: Постанова Пленуму Верховного Суду України від 24.12.1999 р. URL: <https://zakon.rada.gov.ua/laws/show/v0012700-99#Text>.

33. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : Розпорядження Кабінету міністрів України від 24.07.2019 р. № 687-р. URL: <https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text>

34. Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 р. № 1835-III. URL: <https://zakon.rada.gov.ua/laws/show/1835-14#Text>

35. Радченя Наталія. Європейські стандарти професійної підготовки прикордонників. *Visegrad Journal on Human Rights*. 2020. № 4. С. 104.

36. Трофименко О. В., Ляшук Р. М., Вичавка В. І. Правове регулювання взаємодії Державної прикордонної служби України та суб'єктів сектору безпеки і оборони. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2024. № 70. С. 51.

37. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

АВТОРСЬКИЙ КОЛЕКТИВ (за алфавітом)

Бабарика Анатолій Олександрович – заступник начальника кафедри (завідувача кафедри) зв'язку та інформаційних систем Державної прикордонної служби України імені Богдана Хмельницького, доктор філософії

Денисова Аліна Володимирівна – завідувач кафедри адміністративного права та адміністративного процесу факультету підготовки фахівців для підрозділів превентивної діяльності Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

Калугін Володимир Юрійович – професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Катеринчук Іван Степанович – професор кафедри зв'язку та інформаційних систем Державної прикордонної служби України імені Богдана Хмельницького, доктор технічних наук, професор

Крижановська Олена Володимирівна – доцент кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Меликов Руслан Гюндуз огли – т.в.о. завідувача науково-дослідної лабораторії з актуальних питань кримінального аналізу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ, доктор філософії

Пилипенко Євгенія Олексіївна – старший науковий співробітник науково-дослідної лабораторії з актуальних питань кримінального аналізу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ, кандидат юридичних наук, старший дослідник

Пишна Алла Георгіївна – завідувач кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Прокопенко Євгеній Володимирович – начальник кафедри (завідувач кафедри) зв'язку та інформаційних систем Національної академії Державної прикордонної служби України імені Богдана Хмельницького, кандидат технічних наук, доцент

Наукове видання

Бабарика Анатолій Олександрович
Денисова Аліна Володимирівна
Калугін Володимир Юрійович
Катеринчук Іван Степанович
Крижановська Олена Володимирівна
Меликов Руслан Гюндуз огли
Пилипенко Євгенія Олексіївна
Пишина Алла Георгіївна
Прокопенко Євгеній Володимирович

**Аналіз побудови централізованих систем відеоспостереження та
відеоаналітики в частині забезпечення публічного
(громадського) порядку
(міжнародний досвід створення таких систем,
здіянні технології та виробники)**

Навчальний посібник

Підписано до друку 25.11.2025. .Формат 60х84/16 Папір офсетний.
Гарн. «Times New Roman». Друк цифровий.
Ум. друк .арк. 9,76. Обл.вид.арк 8,08.
Надруковано з готового оригінал-макета.
Наклад 10 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.