

4. Про судову експертизу : Закон України від 25.02.1994 № 4038-ХІІ. URL: <https://zakon.rada.gov.ua/go/4038-12>.

5. Постанова ККС ВС від 24.06.2025 у справі № 172/1310/23, провадження № 51-1920км25. URL: <https://reyestr.court.gov.ua/Review/128488905>

2. Вирок Луцького міськрайонного суду Волинської області від 19.11.2025 у справі № 161/4842/25. URL: <https://youcontrol.com.ua/catalog/court-document/131971280/>

3. Ухвала Святошинського районного суду м. Києва від 05.03.2026 у справі № 759/5407/26. URL: <https://kmp.ua/uk/documents/decision-of-the-svyatoshynskiyi-district-court-of-kyiv-as-of-march-05-2026-in-case-no-759-5407-26/>.

4. Ухвала Київського районного суду м. Одеси від 13.05.2025 у справі № 947/10477/25. URL: <https://youcontrol.com.ua/catalog/court-document/127482585/>.

5. Постанова ККС ВС від 21.07.2025 у справі № 201/11849/23, провадження № 51-584км25. URL: <https://reyestr.court.gov.ua/Review/129086893>.

6. Berkeley Protocol on Digital Open Source Investigations. United Nations, 2022. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

7. Federal Rules of Evidence. Rule 702. Testimony by Expert Witnesses. URL: https://www.uscourts.gov/sites/default/files/2025-02/federal-rules-of-evidence-dec-1-2024_0.pdf.

8. Strategic Analysis / Europol. URL: <https://www.europol.europa.eu/how-we-work/services-support/strategic-analysis>.

Литвин Дмитро Олександрович,
начальник Управління кримінального
аналізу Головного управління
Національної поліції в Київській області

РОЗВИТОК СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ЇХ ВИКОРИСТАННЯ

Нині в інформатизованому суспільстві для ефективної протидії злочинності правоохоронним органам уже недостатньо лише володіти інформацією, її вже потрібно вміти якісно збирати, зіставляти та інтерпретувати з метою проведення оцінювання, прогнозування, створення аналітичних висновків та

відповідних рекомендацій. Тому сьогодні основою поліцейської діяльності є застосування розвідувальної аналітики та проведення кримінального аналізу, який являє собою специфічний вид інформаційно-аналітичної діяльності [1, с. 7]. Практична потреба у професійному застосуванні методів та інструментів кримінального аналізу обумовлена попитом на сучасну технологічну і оперативну систему забезпечення діяльності підрозділів кримінальної поліції та органів досудового розслідування. Тому найбільш розповсюдженим видом кримінального аналізу є оперативний.

Оперативний кримінальний аналіз – це інформаційно-аналітична діяльність за конкретними кримінальними провадженнями стосовно інформації, що становить інтерес для кримінальної поліції або органів досудового розслідування поліції, осіб, об'єктів, організованих груп чи злочинних організацій, ознак та інших відомостей, які їх характеризують та, у подальшому, сприятимуть розслідуванню правопорушень [1, с. 31]. Під час здійснення своєї діяльності аналітик збирає та аналізує інформацію з різних джерел, відмінних за походженням та наборами інструментів роботи з ними. Окрему увагу доцільно приділити одному з таких джерел – інформації із систем відеоспостереження.

В епоху стрімкого технологічного прогресу штучний інтелект (ШІ) та машинне навчання кардинально змінюють архітектуру публічної безпеки. Одним із найважливіших елементів цього процесу є еволюція систем відеоспостереження з інструментів пасивного моніторингу в системи превентивного інтелектуального реагування [2, с. 55, 56]. Сьогодні алгоритми автоматизують найбільш трудомісткі завдання, перетворюючи розрізнені відеопотоки на структуровану й значущу оперативну інформацію. Комп'ютеризація систем відеонагляду забезпечує значне підвищення оперативної ефективності, однак водночас породжує низку правових та технічних викликів у сфері кібербезпеки та приватності [2, с. 58]. Поглиблене дослідження цих процесів є надзвичайно актуальним для розвитку всієї сучасної правоохоронної системи.

Ефективне використання таких інтелектуальних систем стало можливим завдяки створенню самостійних підрозділів кримінального аналізу в структурі Національної поліції України, що стало початком та базою для розвитку єдиного методологічного підходу до організації розвідувальної аналітики (Intelligence-Led Policing) та інформаційного забезпечення

підрозділів кримінальної поліції. За досить незначний час свого функціонування в поліції був здійснений перехід від підготовки класичних паперових звітів чи довідок до комплексної роботи з інтегрованими мультимедійними та інноваційними ІТ-платформами. Системи відеоспостереження з вбудованими аналітичними функціями займають вагоме місце під час роботи аналітиків у безпековому секторі держави.

У кримінальному аналізі центральною частиною процесу є саме аналітик та його вміння і здатність обробляти отриману інформацію та вміло користуватись інструментами її обробки. Тут варто зазначити, що час є одним із ключових ресурсів у діяльності аналітика. Тому сучасні системи відеоспостереження завдяки своєму аналітично-програмному забезпеченню виконують різні завдання. Це розпізнавання та класифікація об'єктів – розпізнавання облич людей, зчитування номерних знаків, марок, моделей та кольорів транспортних засобів; детекція небезпечних предметів чи людських взаємодій (автоматичне фіксування маркерів агресивної поведінки, бійок); аналіз маршрутів: побудова траєкторії руху осіб, автомобілів за критеріями просторового аналізу та метаданих. Такий аналітичний підхід безпосередньо спрямований на оперативну оцінку ризиків та формування обґрунтованих висновків під час розслідування злочинів.

Для об'єктивної оцінки потенціалу розвитку інфраструктури відеоспостереження в Україні доцільно звернутися до досвіду держав, які досягли значних результатів у впровадженні та використанні таких систем у сфері забезпечення публічної безпеки. Світовими лідерами за щільністю та рівнем інтеграції систем відеоспостереження є Велика Британія (за рівнем інтеграції технологій ШІ), США та ОАЕ (за щільністю розміщення камер). Велика Британія залишається найвідомішою західною країною за рівнем відеонагляду. Лондон стабільно входить до трійки світових міст за кількістю камер на 1000 осіб (близько 690 тисяч одиниць). США лідирують за абсолютними обсягами відеобладнання в обох Америках (понад 50 мільйонів камер у країні), де муніципальні мережі поєднуються з приватними мережами підприємств. За загальнодоступною інформацією, глобальний ринок обладнання, AI-аналітики та інтеграції переважно контролюється китайськими гігантами Hikvision та Dahua Technology.

На цьому тлі українська інфраструктура відеоспостереження поки що поступається провідним світовим

практикам як за кількісними показниками, так і за рівнем технологічної інтеграції, однак демонструє тенденцію до активного розвитку.

В Україні за останніми підрахунками загальна кількість камер становить приблизно 64 тисячі пристроїв, включаючи регіональні платформи на кшталт «Безпечне місто» та інші менші локальні системи відеоспостереження, що охоплюють лише невеликі населені пункти або території окремих територіальних громад. Вітчизняна інфраструктура систем відеоспостереження перебуває на етапі масштабного розширення. Це стосується як кількісного показника щодо самих пристроїв, так і збільшення аналітичних можливостей на рівні систем та пристроїв. Слід зазначити, що вже сьогодні на різні інтеграційні платформи встановлюється аналітичне забезпечення з елементами ШІ здатне об'єднувати розрізнені потоки з відеокamer різних виробників.

Окрім порівняно невеликої кількості пристроїв на території країни є й інші проблемні питання використання систем відеоспостереження. Стрімке масштабування технологій відеоспостереження в Україні спровокувало гостру суперечність із нормативним вакуумом у сфері регулювання розвитку систем відеонагляду, його використання та захисту приватності. Спробою подолати цю проблему став розроблений МВС та НПУ законопроект № 11031 «Про єдину систему відеомоніторингу стану публічної безпеки». Документ пропонував уніфікувати функціональні та технічні стандарти, визначити перелік персональних даних (ПДБ, оцифроване обличчя, номерні знаки) та встановити базові строки зберігання інформації. Законопроект передбачав створення єдиної глобальної системи відеомоніторингу трьох рівнів (центрального, регіонального та місцевого). Вона мала би об'єднати понад 64 000 державних камер, які раніше працювали розрізнено у понад 600 локальних системах на території всієї країни. Крім того вперше на законодавчому рівні пропонувалося вжити реальних заходів для захисту персональних даних в розрізі користування системами відеонагляду та обробки збереженої в них інформації [3, с. 10].

Незважаючи на прогресивні прагнення, законопроект зазнав жорсткої критики через невідповідність європейським правилам, де приватність історично постанала над безпековими ризиками. Критики законопроекту зазначали про значне розширення повноважень держави, збір біометрії та доступ правоохоронців до камер. Такий стан речей різко відрізняється від Європейського законодавства, що створює потенційні

перешкоди на шляху євроінтеграції. І тут варто згадати регіональні системи, такі як «Безпечне місто», на рівні яких спостерігається більша проблема. Наприклад, положення про інтегровану систему відеоспостереження та відеоаналітики «Безпечна Київщина» (рішення Київської обласної ради № 1719-37 VIII від 21.05.2026) яскраво демонструють загальнонаціональну тенденцію: місцеві нормативні акти є суто технічно-організаційними. Вони описують порядок закупівель, обслуговування системи, порядок надання доступів користувачам мереж, проте питання приватності громадян обмежується стандартною декларативною фразою про дотримання Закону України «Про захист персональних даних». Оскільки органи місцевого самоврядування не мають повноважень обмежувати права людини чи створювати нові правові норми, реальні механізми захисту персональних даних у цих системах практично відсутні. Саме тому кожне місто/область регулюють свої системи окремими положеннями місцевих рад.

Синергія можливостей кримінального аналізу та розвитку інтелектуального відеонагляду є невід’ємною умовою побудови безпекового середовища на рівні держави. Якнайшвидше законодавче врегулювання питання систем відеонагляду, приведення законодавства у відповідність з європейськими стандартами без урізання аналітичних інструментів та впровадження відповідного захисту систем дозволять правоохоронній системі повноцінно виконувати свою функцію.

Список використаних джерел

1. Основи кримінального аналізу : підручник / А. М. Бабенко та ін. ; за заг. ред. О. Є. Користіна. Київ, 2020. 296 с.
2. Дослідження впливу штучного інтелекту на розвиток систем відеоспостереження / Д. А. Бондаренко та ін. Зв’язок. 2025. № 1. С. 55–59.
3. Про єдину систему відеомоніторингу стану публічної безпеки : проект Закону від 20.02.2024 р. № 11031 (включено до порядку денного 11.02.2025 р. № 4229-IX).
4. Про внесення змін до обласної комплексної програми забезпечення правопорядку та публічної безпеки у Київській області на 2026–2027 роки «Безпечна Київщина» : рішення Київської обласної ради від 21.05.2026 р. № 1719-37 VIII. URL: <https://kor.gov.ua/rishennia/pro-vnesennya-zmin-do-oblasnoyi-kompleksnoyi-programy-zabezpechennya-pravoporyadku-ta-publichnoyi-bezpeky-u-kyivskij-oblasti-na-2026-2027-roky-bezpechna-kyivshhyna-3/>