DOI https://doi.org/10.30525/978-9934-26-649-2-22

ВПРОВАДЖЕННЯ СИСТЕМ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОМОНІТОРИНГУ В ПРАВООХОРОННУ ДІЯЛЬНІСТЬ УКРАЇНИ: ДОСВІД ВИСОКОТЕХНОЛОГІЧНИХ КРАЇН

Негребецький В. В.

ВСТУП

З урахування воєнного стану існуючий на сьогодні рівень забезпечення безпеки населення України від загроз життю, здоров'ю та майну не повною мірою відповідає стандартам безпеки, притаманним провідним країнам світу.

Зважаючи на складність та різноманітність факторів, що впливають на рівень забезпечення національної безпеки, стан та динаміку злочинності, ступінь захищеності населення від надзвичайних ситуацій, кардинальне поліпшення безпекової ситуації в країні може бути досягнуто лише завдяки об'єднанню зусиль та спільній скоординованій роботі сил безпеки, інших державних органів та органів місцевого самоврядування[1].

Важливим орієнтиром для України є досвід високотехнологічних країн у масштабному застосуванні технічних засобів і пристроїв, зокрема з функціями фото-, аудіо- та відеофіксації, що забезпечують можливість раннього виявлення правопорушень, ідентифікації осіб та об'єктів, а також моніторингу транспортних засобів. Нині заходи у цьому напрямі мають фрагментарний характер, що зумовлює необхідність створення комплексних систем відеомоніторингу публічної безпеки як інструменту підвищення ефективності профілактики кримінальних правопорушень, захисту населення, територій та об'єктів критичної інфраструктури держави.

Політика Східного партнерства ЄС до 2025 року окреслює стратегічні пріоритети, спрямовані на посилення стійкості, оперативне реагування на нові виклики та забезпечення комплексної цифрової трансформації. Європейська Комісія наголошує, що розвиток цифрової інфраструктури та впровадження інноваційних технологій у країнах-партнерах сприятиме сталому економічному зростанню та підвищенню кіберстійкості. У цьому контексті ЄС продовжує підтримувати розширення високотехнологічних рішень, включаючи системи відеомоніторингу, відповідно до європейських стандартів [2].

Відповідно до пропозицій Європейської Комісії щодо нових пріоритетів політики Східного Партнерства ЄС, сильна цифрова присутність в країнах-

[1] Про єдину систему відеомоніторингу стану публічної безпеки: проект Закону від 20.02.2024 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733

[2] An official website of the European Union. Joint Communication: Eastern Partnership policy beyond 2020: Reinforcing Resilience – an Eastern Partnership that delivers for all. URL: https://www.eeas.europa.eu/eeas/joint-communication-eastern-partnership-policy-beyond-2020-reinforcing-resilience-%E2%80%93-eastern_en.

сусідах ЄС сприятиме зростанню і стимулюванню сталого розвитку[3]. В цьому відношенні ЄС буде і далі вкладати кошти в цифрову трансформацію країн-партнерів відповідно до законодавства та передової практики ЄС і підтримуватиме розширення високо інноваційних цифрових технологій в регіоні. ЄС і далі надаватиме підтримку країнам-партнерам та сприятиме їх кіберстійкості.

Теоретичні та практичні проблеми правового регулювання цифрової трансформації, а також питання правового забезпечення соціальних комунікацій в умовах використання технологій Інтернету речей, штучного інтелекту, великих даних, блокчейну та інших інновацій були предметом наукових дискусій, зокрема на ІІІ Всеукраїнській науково-практичній конференції «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» (Київ, 2023). Учасники конференції підкреслили, що успіх соціальної трансформації безпосередньо залежить від масштабного впровадження цифрових технологій, а більшість держав світу вже прийняли або розглядають національні стратегії розвитку штучного інтелекту та Інтернету речей[4]. На конференції, зокрема, були розглянуті особливості правового забезпечення розвитку сучасної інформаційної інфраструктури суспільства та проблем правового регулювання суспільних відносин у сфері застосування технологій Інтернету речей. Запропоновано напрями вдосконалення законодавства з питань захисту прав людини в умовах використання цифрових технологій. В ході активного експертного обговорення вказаних питань учасники Всеукраїнської науково-практичної конференції відзначили наступне:

– світова спільнота пов'язує успіх будь-якої соціальної трансформації з проведенням широкомасштабних цифрових трансформацій на основі активного впровадження та використання досягнень Четвертої промислової революції: технологій Інтернету речей; Індустрії 4.0; штучного інтелекту; робототехніки; блокчейну; великих даних (big data); розумних контрактів; соціальних мереж та електронних комунікацій; хмарних та нано-, біотехнологій тощо;

– більшість держав світу прийняли або розглядають можливість прийняття національних стратегій впровадження технологій Інтернету речей; одночасно, близько 70 держав – національних стратегій розвитку штучного інтелекту та робототехніки, вважаючи це базовою умовою розвитку;

– актуальним є питання організації належного правового забезпечення соціальної та цифрової трансформації суспільства, а також покладання завдання щодо розробки концептуальних засад розвитку законодавства на профільні наукові установи НАН України і НАПрН України та Дослідницьку службу Верховної Ради України[5].

---

[3] An official website of the European Union. Joint Communication: Eastern Partnership: Commission proposes new policy objectives for beyond 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_452.

[4] Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали ІІІ Всеукр. наук.-практ. конф. (Київ, 23 листоп. 2023 р.). Київ, ДНУ «Інститут інформації, безпеки і права НАПрН України», 2023. 150 с.

[5] Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали ІІІ Всеукр. наук.-практ. конф. (Київ, 23 листоп. 2023 р.). Київ, ДНУ «Інститут інформації, безпеки і права НАПрН України», 2023. С.5.

Питанням застосування інформаційних технологій для попередження і розслідування кримінальних правопорушень присвятили свої наукові праці багато відомих українських науковців, зокрема Г.К. Авдєєва, В. С. Батиргареєва, В. І. Борисов, Т. Я. Гнідець, Ю. І. Дмитрик, К.В. Дубонос, Н. М. Дяченко, В. А. Журавель, В. П. Захаров, А. О. Ігнатович, Р. С. Козьяков, В.О. Коновалова, Т. М. Лемеха, А.М. Лисенко, О. С. Мельник, А. О. Мороз, І. В. Олешко, Ю. В. Осадча, О. В. Рибальський, В. І. Рудешко, В. І. Соловйов, Л. І. Сопільник, І. О. Супрун, В. В. Топчій, А. О. Фесенко, В. Г. Хахановський, Л. М. Хмельничий, Р. Ю. Царьов, В. А. Швець, В.М. Шевчук, В.Ю. Шепітько, й інші[6].

Необхідно відзначити, що в літературних джерелах в основному розглядались окремі аспекти використання технологій відеомоніторингу в діяльності органів правоохоронних органів. Разом із тим, з нашого погляду, недостатньо висвітлені були питання правового регулювання використання таких систем в Україні, позитивний досвід інших високотехнологічних країн та перспективи використання таких технологій в контексті забезпечення безпеки населення України від загроз життю, здоров'ю та майну. Тому питання дослідження можливості впровадження таких технологій в діяльність, пов'язану з розслідуванням і попередженням кримінальних правопорушень потребую подальшого розгляду. Також у зв'язку з війною в Україні вкрай актуальним становиться питання використання можливостей технологій відеомоніторингу в підвищенні ефективності розслідування воєнних злочинів та злочинів агресії в Україні.

Отже, дослідження світових тенденцій впровадження інтелектуальних систем відеомоніторингу та аналіз можливостей їх адаптації в Україні є науково обґрунтованим і практично необхідним завданням, що відповідає сучасним викликам цифрової трансформації та потребам удосконалення нормативного регулювання[7].

1. Проблеми захисту персональних даних у системах відеомоніторингу публічної безпеки та перспективи їх вирішення

Стрімкий розвиток цифрових технологій і впровадження систем відеомоніторингу публічної безпеки в Україні створюють нові можливості для забезпечення правопорядку, протидії злочинності та підвищення рівня громадської безпеки. Водночас ці процеси супроводжуються суттєвими ризиками порушення права на приватність та захист персональних даних.

Автоматизовані системи відеомоніторингу на основі біометричних технологій стали ключовими для правоохоронних органів. Вони допомагають ефективно розслідувати та попереджувати злочини, оперативно ідентифікувати підозрюваних, відстежувати їх переміщення та запобігати загрозам, підвищуючи

[6] Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 6–10. URL: https://dspace.nlu.edu.ua/bits.../123456789/18957/1/6-10.pdf

[7] Примітка. Стаття написана у межах розробки фундаментальної теми «Пріоритезація та технологізація у кримінальному провадженні у воєнний та повоєнний час», яка досліджується фахівцями НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України.

рівень громадської безпеки. Використання біометричних технологій, систем розпізнавання обличь та аналітичних алгоритмів у режимі реального часу передбачає обробку значних масивів персональної інформації, що потребує чіткого правового регулювання та ефективних механізмів контролю.

В Україні правові засади захисту персональних даних визначені Законом «Про захист персональних даних»[8], а також міжнародними актами, ратифікованими державою, зокрема Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковим протоколом до неї. Однак сучасні технологічні виклики, пов'язані з інтеграцією систем відеоспостереження у єдиний інформаційний простір, вимагають гармонізації національного законодавства з європейськими стандартами, закріпленими у Загальному регламенті захисту даних (GDPR) (Овчаренко, 2018).

В Україні захист персональних даних в системах відеомоніторингу стану публічної безпеки повинен відповідати Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних[9], Додатковому протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних[10], Загальному регламенту захисту персональних даних GDPR (General Data Protection Regulation)[11], прийнятому у державах Європейського Союзу, а також законодавству у сфері захисту інформації [10]. Для імплементації GDPR в законодавство України народними депутатами України 25.10.2022 р. було подано проект Закону України «Про захист персональних даних» (реєстр. № 8153)[12].

GDPR встановлює принципово нові правила обробки персональних даних, які мають екстратериторіальну дію. Це означає, що його положення поширюються не лише на держави-члени ЄС, а й на суб'єктів, які здійснюють діяльність на ринку ЄС або обробляють дані громадян Союзу. Для України, яка активно впроваджує цифрові сервіси та інтегрується у європейський простір, імплементація норм GDPR є не лише вимогою часу, а й умовою забезпечення конкурентоспроможності на міжнародному рівні. Відповідно до статті 3 Регламенту, обробка даних у межах моніторингу поведінки осіб, що перебувають у ЄС, підпадає під його дію, навіть якщо контролер або оператор знаходиться поза межами Союзу (GDPR, 2016).

Системи відеомоніторингу публічної безпеки, особливо ті, що використовують біометричні технології, створюють підвищені ризики порушення конфіденційності. Збирання, зберігання та аналіз відеозображень, які дозволяють ідентифікувати особу, є обробкою персональних даних у розумінні GDPR. Це вимагає дотримання принципів законності, пропорційності та

[8] Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.

[9] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Страсбург. 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

[10] Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних. Страсбург. 08.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text.

[11] Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/

[12] Про захист персональних даних : проект Закону від 25.10.2022. № 8153. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707.

мінімізації даних, а також забезпечення прав суб'єктів даних, включаючи право на доступ, виправлення та видалення інформації. Водночас українське законодавство поки що не містить комплексних механізмів контролю за використанням таких технологій у сфері публічної безпеки, що створює правові прогалини та загрози зловживань.

Вирішення проблеми захисту персональних даних у системах відеомоніторингу потребує комплексного підходу. По-перше, необхідно гармонізувати національне законодавство з положеннями GDPR, включаючи запровадження інституту незалежного контролюючого органу, який здійснюватиме нагляд за дотриманням правил обробки даних. По-друге, слід передбачити обов'язкове призначення фахівців із захисту даних у органах державної влади та приватних структурах, що експлуатують системи відеоспостереження. По-третє, важливим є впровадження технічних і організаційних заходів безпеки, таких як шифрування, анонімізація та обмеження доступу до інформації. Нарешті, необхідно встановити дієві санкції за порушення правил обробки персональних даних, що відповідатимуть європейським стандартам і забезпечуватимуть реальний превентивний ефект[13].

Імплементація GDPR в Україні має стратегічне значення не лише для захисту прав громадян, а й для розвитку цифрової економіки та інтеграції у європейський правовий простір. В умовах розбудови системи відеомоніторингу публічної безпеки це дозволить поєднати ефективність правоохоронної діяльності з гарантіями приватності, забезпечити баланс між безпекою та правами людини, а також підвищити довіру суспільства до державних інституцій.

У Верховній Раді України 20.02.2024 р. було зареєстровано законопроект «Про єдину систему відеомоніторингу стану публічної безпеки», який пропонує запровадити єдину всеукраїнську систему відеомоніторингу з використанням персональних даних громадян[14].

Представлений проект було розроблено з метою забезпечення національної та державної безпеки, підвищення загального рівня публічної безпеки і порядку, забезпечення безпеки місць проживання та перебування громадян шляхом запровадження на базі органів державної влади та органів місцевого самоврядування у відповідності з єдиними функціональними і технологічними стандартами єдиної системи відеомоніторингу стану публічної безпеки, що забезпечить моніторинг та сприятиме попередженню і ліквідації можливих загроз, а також контроль за усуненням наслідків надзвичайних ситуацій і правопорушень.

Законопроектом передбачено, що державне регулювання суспільних відносин у сфері створення та впровадження єдиної системи відеомоніторингу стану публічної безпеки ґрунтуватиметься на таких принципах:

верховенство права;

законність;

[13] Овчаренко Я.О. Регламент захисту персональних даних європейського союзу (GDPR) та можливість його застосування на території України. *Юридичний науковий електронний журнал*. 2018. № 3. С. 236–239. http://lsej.org.ua/3_2018/68.pdf

[14] Про єдину систему відеомоніторингу стану публічної безпеки : проект Закону від 20.02.2024 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733

повага і дотримання прав та свобод людини та громадянина;

відкритість та прозорість;

безперервність;

забезпечення безпеки людини, суспільства і держави при застосуванні інформаційно-комунікаційних технологій;

повага до людської гідності;

відкритість для демократичного цивільного контролю.

Для того, щоб майбутня система відеомоніторингу України запрацювала, проект Закону передбачає нормативне регулювання за наступними важливими напрямками:

– єдині функціональні та технічні вимоги до побудови та функціонування систем відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів, відомчих систем відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місцях, порядок доступу до інформації, а також складу відеоданих, метаданих, аналітичних даних, відеоархівів, сигналів тривог, що створюються ними;

– забезпечення єдиних правил інформаційного обміну на державному, регіональному та місцевому рівнях між суб'єктами єдиної системи відеомоніторингу стану публічної безпеки через єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації;

– забезпечення захисту інформації, у тому числі персональних даних у системах відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів та відомчих системах відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місцях.

За думкою авторів законопроекту, впровадження єдиної системи відеомоніторингу стану публічної безпеки відповідає і базується на таких важливих нормативно-правових актах, як Конституція України, Кодекс цивільного захисту України, закони України «Про національну безпеку України», «Про захист інформації в інформаційно – комунікаційних системах», «Про електронні комунікації», «Про критичну інфраструктуру», «Про об'єкти підвищеної небезпеки», «Про Національну поліцію».

Дійсно, Указом Президента України від 11 травня 2023 року № 273/2023 було схвалено Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки[15]. «Кожен елемент державної системи – органи правопорядку передусім – мають працювати так, щоб люди реально відчували безпеку й захищеність, щоб люди реально відчували справедливість, щоб гарантувалося на рівні інституцій, на рівні повсякденної роботи тих, по кому люди судять про державу. Довіра в державі, довіра до держави формуються з довіри до тих, хто діє від імені держави. Правоохоронці, система прокуратури – ключові в

[15] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

цьому. Звичайно, разом з усіма іншими, хто працює в державному апараті», – наголосив Президент України[16].

Документ було спільно розроблено міжвідомчою групою, до складу якої входили очільники Офісу Генпрокурора, МВС, Міністерства юстиції, СБУ, ДБР, Національної поліції, Державної прикордонної служби, БЕБ, Державної митної служби, а також представники Офісу Президента України, Кабінету Міністрів України, міжнародні експерти від Офісу Ради Європи в Україні, КМЄС, проекту ЄС «PRAVO-JUSTICE», відділу з правоохоронних питань Посольства США в Україні, Міжнародної організації права розвитку (IDLO). Основною метою розробників Плану було поставити у центр уваги сектору правопорядку, сектору безпеки і оборони людину, її життя, здоров'я, честь і гідність, права і охоронювані законом інтереси. Кожен українець має бути впевнений, що живе у безпеці, має свободу і може розраховувати на механізми справедливості.

План визначає шість стратегічних пріоритетів, які дозволять модернізувати сектор безпеки й привести у відповідність до стандартів, яких має досягти Україна на шляху до членства у ЄС, до яких належать:

1. Дієвість і ефективність органів правопорядку та прокуратури як невід'ємної складової сектору безпеки і оборони, в межах якого вони забезпечують національну безпеку України, у тому числі громадські безпеку й порядок, протидіють злочинності з урахуванням стратегічних цілей та відповідно до стандартів прав людини і основоположних свобод, у тому числі із забезпеченням гендерної рівності.

2. Послідовна кримінальна політика, пріоритетом у якій є запобігання злочинності, невідворотність відповідальності, захист особи, суспільства та держави від кримінальних правопорушень, забезпечення інтересів потерпілого.

3. Оперативність кримінального провадження з дотриманням міжнародних стандартів та принципу верховенства права.

4. Система управління, орієнтована на результат відповідно до встановлених пріоритетів.

5. Комплексна цифрова трансформація.

6. Відкритість, прозорість, підзвітність і незалежність.

Планом передбачено комплексну цифрову трансформацію, зокрема:

1. Здійснення консолідованої поетапної цифрової трансформації органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту, які відповідають найкращим практикам ЄС.

2. Подальше впровадження в діяльність органів правопорядку та прокуратури інноваційних технологічних досягнень, що забезпечують гнучкість операційних процесів, ІТ-рішення, цифрову спроможність оперативно реагувати на події та зміни й здобувати результат, орієнтований на інтереси суспільства.

3. Поетапне впровадження електронної системи управління кримінальними провадженнями шляхом комплексної заміни та модернізації обладнання, забезпечення сумісності ІТ-систем, безперебійності роботи, доступу усіх учасників кримінального провадження та інтероперабельності.

[16] Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

4. Підвищення ефективності діяльності органів правопорядку та прокуратури через забезпечення більшої доступності й повноти інформації, розроблення і впровадження сервісів на Єдиному державному вебпорталі електронних послуг.

5. Впровадження заходів безпеки і захисту персональних даних відповідно до стандартів ЄС.

6. Удосконалення та впровадження більш безпечних, гнучких, спроможних і доступних систем зв'язку між усіма органами правопорядку та іншими екстреними службами (включаючи цифрове радіо: голосовий зв'язок і широкосмугове передавання даних).

7. Запровадження в усіх органах правопорядку та прокуратури уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами. Широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.

8. Оновлення операційних процесів за допомогою ІТ-систем, придатних для обміну даними з інституціями ЄС відповідно до стандартів ЄС.

9. Надання органам правопорядку та прокуратури для забезпечення виконання покладених на них функцій права на безпосередній спільний доступ до автоматизованих інформаційних і довідкових систем, реєстрів і баз даних, держателем (адміністратором) яких є інші державні органи[17].

2. Система «Безпечне місто» – інноваційне технологічне рішення для забезпечення безпеки і покращення правоохоронної діяльності

Згідно із проектом Закону України «Про єдину систему відеомоніторингу стану публічної безпеки» (реєстр. № 11031) відеомоніторинг – це безперервний, систематичний процес збору та обробки даних про стан публічної безпеки, що здійснюється за допомогою технічних засобів, призначених для обробки інформації[18]. Це процес спостереження, що реалізується із застосуванням оптико-електронних пристроїв, призначених для візуального контролю та автоматичного аналізу[19]. Системи відеоспостереження розповсюджені й широко використовуються в різних сферах життя людини. Для контролю навколишнього середовища з метою безпеки життєдіяльності в даний час широко використовуються системи відеоспостереження – комплекс обладнання та програмного забезпечення, призначений для моніторингу поведінки, дій або інформації з метою збирання інформації, впливу, управління та координації. Завдяки автоматизації та швидкості роботи, використання біометрії для розпізнавання особи, такі

[17] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

[18] Про єдину систему відеомоніторингу стану публічної безпеки : проект Закону від 20.02.2024. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733.

[19] Рувінська В.М., Девятков В.В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні.* 2021. Том 11, № 4. С. 331–342. URL: http://immm.op.edu.ua/files/archive/n4_v11_2021/2021_4(9).pdf

технології є дуже корисними в будь-якій галузі діяльності людини, де необхідно перевірити і підтвердити особу за її біометричними характеристиками. Це може бути безпека, оборона, міграційні процеси, банківська сфера та моніторинг, та ін. Причому дати вичерпний перелік сфер застосування біометричних технологій на сьогодні вже є неможливим, оскільки сама ідея перевірки й підтвердження особи людини вже більше і більше стає привабливою і асоціюється з безпекою.

Система «Безпечне місто» в Україні розглядається як комплексне технологічне рішення, спрямоване на підвищення рівня громадської безпеки та ефективності роботи правоохоронних органів. Її основна мета полягає у створенні єдиного інтегрованого середовища, яке забезпечує оперативний моніторинг ситуації в населених пунктах, швидке реагування на інциденти та запобігання правопорушенням. В основі концепції лежить використання сучасних цифрових технологій, включаючи системи відеоспостереження, аналітичні платформи та канали обміну даними між різними службами.

За даними офіційних джерел, система «Безпечне місто» передбачає встановлення мережі камер відеоспостереження у ключових локаціях – на транспортних вузлах, у громадських місцях, на вулицях та в житлових районах. Відеопотоки з цих камер передаються до єдиного центру обробки даних, де здійснюється їх аналіз у режимі реального часу. Це дозволяє правоохоронним органам оперативне реагувати на порушення громадського порядку, дорожні інциденти та інші небезпечні ситуації. Крім того, система інтегрується з іншими інформаційними ресурсами, що дає змогу формувати комплексну картину безпеки міста та підвищувати ефективність управлінських рішень[20].

Важливим аспектом є використання аналітичних інструментів, які дозволяють не лише фіксувати події, а й здійснювати їх автоматичну класифікацію, виявляти підозрілу поведінку та прогнозувати ризики. Це значно розширює можливості правоохоронних органів у запобіганні злочинам та забезпеченні громадського порядку. Система також сприяє взаємодії між різними службами – поліцією, органами місцевого самоврядування, аварійними та комунальними службами, що забезпечує комплексний підхід до управління безпекою міського середовища (https://360view.com.ua/bezpechne-misto/).

Додатковим підтвердженням ефективності системи є її використання у діяльності державних органів, зокрема Національного агентства з питань виявлення, розшуку та управління активами (АРМА), яке отримало доступ до відеоспостереження в рамках «Безпечного міста». Це дозволяє здійснювати контроль за об'єктами, що перебувають у сфері управління агентства, та підвищує прозорість і безпеку процесів управління активами (https://arma.gov.ua/news/typical/arma-otrimalo-dostup-do-sistem-videosposterejennya-bezpechne-misto).

Розгортання системи «Безпечне місто» в Україні є не лише прикладом впровадження сучасних технологій у сфері громадської безпеки, а й важливим елементом цифрової трансформації міського управління. Ця система формує єдиний інформаційний простір, що інтегрує відеоспостереження, аналітичні сервіси та канали взаємодії між правоохоронними органами, органами місцевого

[20] Система «Безпечне місто» – інноваційні рішення, які дбають про безпеку. URL: https://i-lug.gov.ua/news/sistema_%C2%ABbezpechne_misto%C2%BB_-_innovacijni_rishennja_jaki_dbajut_pro_bezpeku.

самоврядування та іншими службами. Її функціонування забезпечує оперативний моніторинг, швидке реагування на інциденти та превентивний контроль, що відповідає ключовим принципам концепції «Smart City» – створення безпечного, технологічно розвиненого та стійкого міського середовища.

У науковій літературі концепція «Smart City» визначається як інноваційний інструмент сталого розвитку міст та їх повоєнного відновлення.

Концепція розумного міста – це система, при якій міські служби використовуються найбільш оптимальним чином і забезпечують найбільшу зручність жителям міста. Для цього необхідний тісний зв'язок між проектами розумного міста (вуличним відеоспостереженням, держпослугами, інтелектуальною транспортною системою та іншими) в масштабах міста[21].

Технології «розумних міст» поліпшать ключові показники за всіма основними напрямками: медицина та здоров'я громадян, безпека, вартість життя, зайнятість населення, соціальні зв'язки, захист навколишнього середовища.

Вуличне відеоспостереження – програмно-апаратний комплекс, що забезпечує повний моніторинг всіх відкритих просторів в будь-яких кліматичних умовах і призначений для попередження, профілактики та раннього реагування на правопорушення. До завдань зовнішнього відеоспостереження відноситься не тільки контроль периметра об'єкту, що охороняється, а й підходів до нього: огорож, стоянок і т. і. Найчастіше установку системи вуличного відеоспостереження застосовують на наступних об'єктах:

– автомобільні стоянки;
– АЗС;
– промислові зони;
– складські приміщення;
– парковки у великих торгових центрів;
– школи;
– вокзали та аеропорти і т. і.

При формуванні комплекту зовнішнього відеоспостереження в першу чергу враховуються особливості архітектури і рельєфу місцевості. Крім цілком очевидних факторів, на зразок можливості закріплення камер в обраних точках огляду і відсутності в кадрі об'єктів, що закривають значущі частини сцени – необхідно передбачити вплив регулярних природних явищ. Наприклад, кут падіння сонячного світла (в залежності від пори року і часу доби) – щоб уникнути засвічення відеозображення; або наявність в кадрі вікон, дзеркальних вітрин, поверхні води, які можуть створювати сліпучу яскравість для камери, яка працює в ІЧ-режимі.

Для організації вуличного відеоспостереження в умовах недостатньої освітленості (в нічному режимі), як правило, використовується додаткове освітлення прожекторами видимого спектру освітлення або за допомогою інфрачервоного підсвічування. Вибір між ними залежить від особливостей об'єкта, що охороняється. Ліхтарі, що працюють у видимому спектрі, зазвичай мають більше електроспоживання і можуть не відповідати вимогам міської

[21] Безпека в місті. Вуличний відеонагляд. URL: https://360view.com.ua/bezpechne-misto/.

інфраструктури (порушувати комплекс декоративного освітлення, заважати власникам житлових приміщень). Однак, в деяких випадках, необхідно саме таке освітлення. Наприклад, для ідентифікації по обличчю, яка практично не можлива при роботі камери охоронного відеоспостереження в інфрачервоному режимі. Вбудоване ІЧ-підсвічування не завжди володіє достатньою дальністю для ефективного відеоспостереження на вулиці. Тому для об'єктів зовнішнього спостереження часто застосовують системи з додатковими ІЧ-прожекторами. При монтажі такої системи вуличного спостереження, необхідно враховувати, що напрямок і кут інфрачервоного підсвічування повинні збігатися з кутом огляду і напрямком відеокамери.

Відстань точок огляду від реєстратора, не тільки може збільшувати вартість системи зовнішнього відеоспостереження за рахунок включення додаткових ретрансляторів і підсилювачів відеосигналу, а й безпосередньо впливає на кількість проводів, які необхідно захистити від впливу агресивного середовища.

Грозозахист камер зовнішнього відеоспостереження. Пристрої грозозахисту призначені для забезпечення безперебійної роботи обладнання при несприятливих погодних умовах, зокрема, для захисту елементів системи відеоспостереження від пошкодження потужними електромагнітними наведеннями, які створюються грозовими розрядами. Для захисту зовнішніх елементів системи зовнішнього спостереження від удару блискавки, як правило, використовуються спеціальні навіси або громовідводи. Однак, в разі враження блискавкою однієї з частин (або її поломки в зв'язку з несприятливими умовами навколишнього середовища), небезпеці піддається все обладнання: відеореєстратор, комп'ютер-відеосервер, камери, блоки живлення, станція спостереження (диспетчерський пункт).

Вулична камера відеоспостереження. При організації систем зовнішнього відеоспостереження обсяг і потужність відеореєстратора вибираються виходячи з кількості відеокамер, що підключаються , їх дозволу і необхідного режиму відеозапису; а тип камер – в залежності від цілей відеоспостереження і віддаленості оператора від зони, що охороняється.

Конструкція вуличних відеокамер. Конструктивно, вуличні відеокамери нічим не відрізняються від звичайних камер охоронного спостереження. Вони також можуть бути аналоговими або цифровими, безкорпусними (для установки в термокожух) або мати різні корпуси з високим класом захисту, використовувати поворотний механізм або об'єктив типу «риб'яче око» для охоплення сцени більшого розміру. Необхідно, щоб електроніка мала захист від зовнішніх впливів. Найбільшою популярністю при монтажі систем відеоспостереження, завдяки обтічному корпусу, користуються купольні камери і відеокамери типу bullet (камери зовнішнього відеоспостереження, які мають циліндричну форму і обладнані сонцезахисним козирком).Однак, вулична відеокамера є основним утворюючим елементом системи і її вибору необхідно приділити найбільшу увагу. В першу чергу, вуличні камери спостереження відрізняються від звичайних відеокамер захистом електроніки від впливу вологи, пилу, механічних пошкоджень. Як правило, корпуси таких відеокамер мають певний ступінь захисту IP і / або IK.

Діапазон робочих температур. Камери охоронного спостереження мають досить чутливу електроніку, тому для установки відеокамери на вулиці, вона повинна бути захищена від різких перепадів температури і мати можливість роботи при дуже низьких, або надто високих температурах. Вулична камера спостереження може бути закінченим рішенням «все в одному», і мати комплектацію, яка підходить для роботи поза приміщенням в широкому температурному діапазоні і в різних несприятливих умовах навколишнього середовища. Для вуличного відеоспостереження можна використовувати і стандартну за своїми характеристиками відеокамеру, помістивши її попередньо в термокожух. Вибір між вуличної камерою «все в одному» і встановленням обладнання в термокожух, як правило, обумовлений індивідуальними вимогами до характеристик системи відеоспостереження за об'єктом. Вулична відеокамера «все в одному» значно простіше в установці та налаштування, тому що являє собою комплект обладнання, збалансований по функціоналу і технічним характеристикам. При установці в термокожух слід підібрати не тільки відеокамеру, а й модулі обігріву, вентиляції тощо. – опрацювати схеми підключення, розрахувати енергоспоживання (для підключення до джерела живлення). Однак, такий підхід дозволяє отримати обладнання для вуличного відеоспостереження з нестандартними характеристиками. Наприклад: збільшити чутливість відеокамери або дальність підсвічування, створити камеру для відеоспостереження за вуличними об'єктами в умовах надвисоких або наднизьких температур.

Концепція розумного міста передбачає інтеграцію цифрових технологій у всі сфери міського життя, включаючи безпеку, транспорт, енергетику, комунальну інфраструктуру та управління ресурсами. Як зазначає Олюха В.Г., практична реалізація цієї концепції в Україні потребує нормативного врегулювання, оскільки на рівні закону вона досі не закріплена. Наявні підзаконні акти, зокрема Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки, мають декларативний характер і не містять конкретних механізмів імплементації. Тому ключовим завданням є розробка міських концептуальних проєктів Smart City, що враховують локальні потреби, джерела фінансування та можливість створення кластерів за участю комунальних підприємств, приватного бізнесу та наукових установ[22] (Олюха, 2024).

Взаємозв'язок системи «Безпечне місто» з концепцією Smart City полягає у спільній меті – формуванні цифрового міського простору, який забезпечує інтеграцію даних і сервісів для підвищення ефективності управління та безпеки. Використання аналітичних платформ, штучного інтелекту та мережевих технологій у системі «Безпечне місто» відповідає міжнародним стандартам управління міською інфраструктурою (ISO 37120, ISO 37101), що рекомендовані для впровадження у рамках цифрової трансформації. Такий підхід узгоджується з Указом Президента України № 722/2019 «Про Цілі сталого розвитку України на період до 2030 року», де розвиток міст на засадах сталості визначено пріоритетом державної політики.

[22] Олюха В.Г. Правові основи реалізації концепції «Smart City» в Україні. *Аналітично-порівняльне правознавство*. 2024. С. 339–344. URL: https://doi.org/10.24144/2788-6018.2024.06.55. URL: https://app-journal.in.ua/wp-content/uploads/2024/12/57.pdf

В рамках проекту «Безпечне місто» комунальне підприємство «Інформатіка» впроваджено новий аналітичний модуль відеоспостереження (Kyiv Smart Safe City)[23]. Унікальний модуль дозволяє шукати злочинців не тільки завдяки спеціалізованим камерам розпізнавання особи. Він фіксує зображення з будь-якої камери, установленої в рамках мережі й порівнює їх з наявною базою правопорушників. Якщо система виявляє подібність, оператор відразу одержує тривожний сигнал. Отже, правоохоронці зможуть швидше відслідковувати небезпечних злочинців. До складу нового аналітичного модуля розпізнавання осіб входить аналітична система й база даних, що полягає зі списку розшукуваних людей.

Про ефективність впровадження системи «Smart Safe City» можна деякою мірою зробити висновки, проаналізувавши показники вуличної злочинності в Україні. Так, останніми роками, у період поступового запровадження проекту (протягом 2017–2019 рр.) рівень злочинів, що вчиняються на вулицях, різко знизився. Для порівняння: якщо у 2013 р. було обліковано 66 971 кримінальних правопорушення, вчинених на вулицях, у 2014 р. – 66 255, у 2015 р. – 61 718, у 2016 р. – 62 064, то у 2017 р. кількість таких правопорушень склала 45 707, у 2018 р. – 42 465, а у 2019 р. – 38 139 кримінальних правопорушень[24].

В Україні проект Smart City активно використовується в містах: Київ, Харків, Львів, Дніпро, Вінниця, Маріуполь, Чернігів та ін. Особливим видом такого проекту є «Smart Safe City» – інформаційно-аналітична програма нового покоління, що здійснює розпізнавання потенційних небезпек, аналіз ситуації в реальному часі та передачу вже опрацьованих даних про виявлені загрози терористичного, кримінального, техногенного характеру у місцях масового перебування громадян, на об'єктах критичної інфраструктури, транспортних розв'язках, операторам екстрених служб для швидкого реагування на надзвичайні події.

Таким чином, «Безпечне місто» є не лише технологічним рішенням для підвищення рівня громадської безпеки, а й важливим компонентом стратегії цифрової трансформації України. Його інтеграція у ширшу екосистему Smart City створює передумови для комплексного розвитку міських територій, забезпечення прозорості управління та реалізації європейських стандартів сталого розвитку.

3. Впровадження систем відеомоніторингу в правоохоронну діяльність: досвід Сінгапуру та перспективи для України

Сінгапур є одним із найбезпечніших міст світу, що значною мірою пояснюється ефективним використанням системи поліцейських камер PolCam, інтегрованої у правоохоронну діяльність Сінгапурської поліції (SPF)[25].

[23] У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv/.

[24] Зменшення можливостей вчинення злочинів: стратегічний підхід : монографія / за заг. ред. В. В. Голіни. Харків : Право, 2020. С. 191. URL: https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf.

[25] PolCam: Safeguarding Our Neighbourhoods. URL: https://www.mha.gov.sg/home-team-news/story/detail/polcam-safeguarding-our-neighbourhoods/

Запроваджена у 2012 році, ця система стала ключовим інструментом у протидії злочинності, сприяючи розкриттю понад 5000 кримінальних справ та істотно скорочуючи час розслідувань: окремі провадження завершуються протягом кількох годин після реєстрації заяви. У 2016 році мережу було розширено в межах проєкту PolCam 2.0, що передбачало встановлення понад 90 000 камер у житлових масивах, комерційних зонах, багатоповерхових паркінгах та транспортних вузлах.

Традиційні методи слідства, такі як опитування потерпілих і свідків, залишаються важливими, проте PolCam значно розширила можливості поліції[26]. Система забезпечує ідентифікацію місцезнаходження та поведінки підозрюваних, використання відеоматеріалів як доказової бази в судових процесах, запобігання злочинності завдяки стратегічному розміщенню камер, оперативне реагування на інциденти через моніторинг у режимі реального часу, контроль дорожнього руху та управління транспортними потоками. Під час пандемії COVID-19 система використовувалася для контролю дотримання соціальної дистанції та маскового режиму.

Сінгапурська система громадського спостереження є складовою національної програми «Розумна нація», що передбачає використання цифрових технологій для підвищення ефективності управління. Камери оснащені функціями розпізнавання облич, номерних знаків та алгоритмами штучного інтелекту для аналізу поведінки. Важливим елементом є інтеграція з розумними світильниками (LAMPP), оснащеними сенсорами для збору даних про стан довкілля та безпеку, а також системи відеонагляду у громадському транспорті. Уряд гарантує захист даних, що використовуються виключно для дозволених цілей, із суворими протоколами запобігання зловживанням.

Фінансування системи здійснюється за рахунок державного бюджету, тому для громадян і відвідувачів відсутні прямі витрати. Непрямі витрати пов'язані зі штрафами за порушення правил, наприклад, сміттєдіяльність карається штрафом від 300 до 1000 SGD, а куріння у заборонених місцях – до 1000 SGD. Відеоматеріали використовуються як доказ у кримінальних провадженнях, а дані зберігаються обмежений час, якщо не потрібні для розслідувань. Хоча більшість громадян сприймає систему як необхідний засіб забезпечення безпеки, для відвідувачів із юрисдикцій із суворішими нормами конфіденційності вона може видаватися надмірною. Уряд наголошує на відповідальному використанні технологій.

Досвід Сінгапуру демонструє, що комплексний підхід до впровадження систем відеоспостереження, який поєднує технологічні інновації, правові механізми та соціальну відповідальність, є ефективним інструментом забезпечення правопорядку. Його результативність підтверджується низьким рівнем злочинності та високими стандартами безпеки. Для України цей досвід є релевантним з огляду на необхідність підвищення ефективності правоохоронної діяльності в умовах урбанізації та зростання загроз громадській безпеці. Впровадження аналогічних систем може сприяти оперативному

[26] Public Surveillance. An outline of Singapore's extensive CCTV network and its role in maintaining security. URL: https://citiesinsider.com/country/singapore/singapore/public-surveillance/

реагуванню на правопорушення, зниженню рівня злочинності та підвищенню довіри громадян до правоохоронних органів.

Адаптація сінгапурської моделі в Україні потребує врахування низки чинників. По-перше, слід забезпечити належну нормативно-правову базу, яка регламентуватиме використання технологій відеоспостереження та захист персональних даних. По-друге, необхідно розробити механізми фінансування, що можуть включати державні та муніципальні бюджети, а також партнерство з приватним сектором. По-третє, важливо врахувати соціально-культурні особливості та рівень готовності суспільства до прийняття системи масового спостереження. Нарешті, слід забезпечити прозорість і контроль за використанням даних, щоб уникнути ризиків зловживань та порушення прав людини.

Прогноз розвитку таких систем в Україні до 2030 року свідчить про значні перспективи[27]. Очікується, що до 2025–2027 років відбудеться розширення мережі камер у містах-мільйонниках та реалізація пілотних проєктів із використанням алгоритмів штучного інтелекту для аналітики відео. У період 2028–2030 років прогнозується повна інтеграція систем відеоспостереження з платформами «Безпечне місто» та інформаційними ресурсами МВС, впровадження предиктивної аналітики для запобігання злочинам, а також використання біометричних технологій у транспорті та громадських місцях. Масове впровадження 5G та розвиток IoT дозволять забезпечити передачу відео в реальному часі з тисяч камер без затримок, а хмарні сервіси стануть основою для обробки великих масивів даних. Очікується, що до 2030 року 90% великих міст України будуть обладнані інтелектуальними камерами з функціями AI-аналітики, а рівень злочинності у містах знизиться на 15–20% завдяки превентивним технологіям. Водночас ключовими викликами залишатимуться фінансування, кібербезпека та розробка чітких норм щодо захисту персональних даних.

Таким чином, досвід Сінгапуру може слугувати орієнтиром для України у формуванні сучасної концепції безпеки, заснованої на інтеграції інтелектуальних систем відеомоніторингу в правоохоронну діяльність. Його імплементація потребує комплексного підходу, що поєднує технологічні рішення, правові гарантії та суспільний консенсус, що дозволить досягти високих стандартів безпеки та правопорядку.

ВИСНОВКИ

Впровадження інтелектуальних систем відеомоніторингу є ключовим чинником підвищення ефективності правоохоронної діяльності та забезпечення публічної безпеки. Україна має орієнтуватися на досвід високотехнологічних країн, адаптуючи його до власних правових і соціальних реалій. Це потребує комплексного підходу, що поєднує технологічні рішення, правові гарантії та суспільний консенсус.

В Україні захист персональних даних в системах відеомоніторингу стану публічної безпеки повинен відповідати Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Додатковому протоколу

[27] Police surveillance system using video analytics to detect targets wins Home Team Achievement Award. Oct 28, 2021. URL:https://www.straitstimes.com/singapore/community/police-surveillance-system-using-video-analytics-to-detect-targets-wins-home

до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних, Загальному регламенту захисту персональних даних GDPR (General Data Protection Regulation), прийнятому у державах Європейського Союзу, а також законодавству у сфері захисту інформації. Ми повністю підтримуємо важливість проекту Закону України «Про єдину систему відеомоніторингу стану публічної безпеки» . Впровадження комплексних систем моніторингу безпеки значно підвищить ефективність профілактики зокрема корупційних правопорушень, забезпечуючи більш надійний захист громадян і суспільства в цілому. Існує необхідність імплементації в законодавство України Загального регламенту захисту персональних даних GDPR (General Data Protection Regulation).

Проведене дослідження дозволяє дійти висновку, що використання цифрових технологій і систем дозволить розширити можливості своєчасного повідомлення правоохоронців про правопорушення, розшуку і ідентифікації злочинців, оптимізувати процес розслідування кримінальних правопорушень. У разі впровадження системи відеомоніторингу стану безпеки сучасні технології відеоспостереження, інтегровані з аналітичними алгоритмами та штучним інтелектом, здатні в режимі реального часу:

– розпізнавати загрози та допомагати правоохоронцям запобігати злочинам;

– сприяти ефективному розслідуванню правопорушень;

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

– покращувати координацію між правоохоронними структурами;

– слугувати елементом швидкого реагування на надзвичайні ситуації.

Позитивним для України є досвід провідних країн Європи та Азії у провадженні систем відеомоніторингу в правоохоронну діяльність.

АНОТАЦІЯ

Стаття присвячена вивченню можливостей використання інтелектуальних технологій відеомоніторингу в діяльності правоохоронних органів України. Розглянуто актуальність впровадження систем відеомоніторингу в правоохоронну діяльність України з урахуванням досвіду високотехнологічних країн. Обґрунтовано необхідність створення комплексних систем публічної безпеки, визначено роль цифрової трансформації та міжнародних стандартів у формуванні сучасної концепції безпеки. Підкреслено важливість гармонізації національного законодавства з європейськими нормами та інтеграції інноваційних технологій у діяльність правоохоронних органів. На основі аналізу аксіологічних аспектів впровадження інформаційних технологій і систем безпеки в правоохоронну діяльність в провідних країнах світу, прикладів впровадження, результатів профільних наукових досліджень в цій галузі зроблено висновок, впровадження комплексних систем моніторингу безпеки значно підвищить ефективність профілактики зокрема корупційних правопорушень, забезпечуючи більш надійний захист громадян і суспільства в цілому. Існує необхідність імплементації в законодавство України Загального регламенту захисту персональних даних GDPR (General Data Protection Regulation).

Література

1. Про єдину систему відеомоніторингу стану публічної безпеки: проект Закону від 20.02.2024 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733.

2. An official website of the European Union. Joint Communication: Eastern Partnership policy beyond 2020: Reinforcing Resilience – an Eastern Partnership that delivers for all. URL : https://www.eeas.europa.eu/eeas/joint-communication-eastern-partnership-policy-beyond-2020-reinforcing-resilience-%E2%80%93-eastern_en.

3. An official website of the European Union. Joint Communication: Eastern Partnership: Commission proposes new policy objectives for beyond 2020. URL : https://ec.europa.eu/commission/presscorner/detail/en/IP_20_452.

4. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали III Всеукр. наук.-практ. конф. (Київ, 23 листоп. 2023 р.). Київ : ДНУ «Інститут інформації, безпеки і права НАПрН України», 2023. 150 с.

5. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків: Право, 2020. С. 6–10. URL: https://dspace.nlu.edu.ua/bits.../123456789/18957/1/6-10.pdf

6. Батиргареєва В.С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства. *Інформація і право*. 2022. № 1 (40). С. 21–34. URL: https://scholar.google.com.ua/scholar?oi=bibs&cluster=2148893118868512848&btnI=1&hl=ru

7. Shevchuk, V. (2023). Development trends in criminalistics in the era of digitalization. Scientific Collection «InterConf+», 33(155), 198–219. https://doi.org/10.51582/interconf.19-20.05.2023.019

8. Шевчук В.М. (2022). Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *Нова архітектура безпекового середовища України* : зб. тез Всеукр. наук.-практ. конф. (м. Харків, 23 грудня, 2022 р.). Харків: Юрайт, 2022. С. 146–150.

9. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. Military offences and war crimes: background, theory and practice: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2023. С. 795–823. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1.

10. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.

11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Страсбург. 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.

12. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних. Страсбург. 08.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text.

13 Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/.

14. Про захист персональних даних: проект Закону від 25.10.2022. № 8153. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707.

15. Овчаренко Я.О. Регламент захисту персональних даних європейського союзу (GDPR) та можливість його застосування на території України. *Юридичний науковий електронний журнал.* 2018. № 3. С. 236–239. http://lsej.org.ua/3_2018/68.pdf

16. Про єдину систему відеомоніторингу стану публічної безпеки : проект Закону від 20.02.2024 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733.

17. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

18. Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

19. Рувінська В.М., Девятков В.В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні.* 2021. Том 11, № 4. С. 331–342. URL: http://immm.op.edu.ua/files/archive/n4_v11_2021/2021_4(9).pdf

15. Система «Безпечне місто» – інноваційні рішення, які дбають про безпеку. URL: https://i-lug.gov.ua/news/sistema_%C2%ABbezpechne_misto%C2%BB_-_innovacijni_rishennja_jaki_dbajut_pro_bezpeku.

16. Безпека в місті. *Вуличний відеонагляд.* URL: https://360view.com.ua/bezpechne-misto/.

17. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv.

18. Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія / за заг. ред. В. В. Голіни. Харків : Право, 2020. 287 с. URL: https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf.

19. Шевчук В.М. Проблеми цифровізації криміналістики в умовах російсько-української війни. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : матеріали круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) : електрон. наук. вид.; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Від. дослідж. Проблем крим. проц. та судоустрою. Харків : Право, 2022. С. 127–140. URL: https://drive.google.com/file/d/1xeu-J0LA_70FtmwPPeqrjl8Oml6H34Ou/view.

20. PolCam: Safeguarding Our Neighbourhoods. 15 October 2021. URL: https://www.mha.gov.sg/home-team-news/story/detail/polcam-safeguarding-our-neighbourhoods/.

21. Public Surveillance. An outline of Singapore's extensive CCTV network and its role in maintaining security. URL: https://citiesinsider.com/country/singapore/singapore/public-surveillance/

22. Police surveillance system using video analytics to detect targets wins Home Team Achievement Award. Oct 28, 2021. URL:https://www.straitstimes.com/singapore/community/police-surveillance-system-using-video-analytics-to-detect-targets-wins-home

Information about the author:
Nehrebetskyi Vladyslav Valerevych,
Ph. D. in Law,
Researcher at Academician Stashis Scientific Research Institute
for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
49, Hryhoriia Skovorody str., Kharkiv, 61002, Ukraine,
Associate Professor at the Department of Criminalistics
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., Kharkiv, 61024, Ukraine