МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗВО «ВІДКРИТИЙ МІЖНАРОДНИЙ УНІВЕРСИТЕТ РОЗВИТКУ ЛЮДИНИ «УКРАЇНА»

Кваліфікаційна наукова
праця на правах рукопису

ПУСТОВІТ ОЛЕКСІЙ БОРИСОВИЧ

351.86:352:004.9](477)

ДИСЕРТАЦІЯ

ОБГРУНТУВАННЯ ЗАПРОВАДЖЕННЯ ПРОЄКТІВ «БЕЗПЕЧНЕ МІСТО» НА ДЕРЖАВНОМУ РІВНІ В УКРАЇНІ

281 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **О.Б. Пустовіт**

Науковий керівник
ФЕДОРЕНКО ТЕТЯНА ВІКТОРІВНА,
кандидат юридичних наук,
доцент

Київ – 2026

АНОТАЦІЯ

Пустовіт О.Б. Обгрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії в галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». ЗВО «Відкритий міжнародний університет розвитку людини «Україна». Київ, 2026.

Дисертацію присвячено розробленню та обґрунтуванню теоретико-методичних положень та практичних рекомендацій щодо запровадження проєктів «Безпечне місто» на державному рівні в Україні.

Запровадження концепції та проєктів «Безпечне місто» на державному рівні в Україні обґрунтовується потребою у створенні цілісної, цифрової та адаптивної системи публічної безпеки, особливо в умовах воєнного стану та повоєнної відбудови.

Цифрові технології (відеоспостереження, аналітика великих даних, геоінформаційні системи) перетворюють міську інфраструктуру з потенційної мішені на стійку систему, здатну протистояти воєнним загрозам і кібератакам. Концепція розглядається як стратегічний інструмент публічного управління для моніторингу простору, раннього виявлення загроз та швидкого реагування на небезпечні ситуації.

Проєкти «Безпечне місто» реалізуються переважно на рівні окремих міст, що призводить до різного рівня технічного оснащення, несумісності баз даних і стандартів. Державний рівень дозволяє створити єдиний технічний та правовий стандарт. Централізоване фінансування та координація між МВС, СБУ, ДСНС і місцевою владою оптимізують витрати на закупівлю обладнання та програмного забезпечення.

Проєкт є каталізатором впровадження штучного інтелекту та інтернету речей в роботу правоохоронних органів та служб надзвичайних ситуацій.

Автоматизована фіксація правопорушень, розпізнавання облич та номерних знаків значно знижують рівень злочинності та прискорюють розкриття злочинів.

Науковці та практики визначають «Безпечне місто» не просто як сукупність камер спостереження, а як новий стандарт державного управління, що поєднує безпеку громадян із дотриманням принципів захисту персональних даних.

Під час дослідження наукових інформаційних джерел виявлено, що категоріальна сутність проєктів «Безпечне місто» полягає в тому, що вони є комплексними організаційно-правовими та програмно-технічними системами. Ці системи об'єднують відеоспостереження, аналітику даних та взаємодію громад із поліцією задля захисту мешканців, контролю трафіку та оперативного реагування на надзвичайні події в реальному часі.

Введення військового стану докорінно змінило порядок реалізації проєктів «Безпечне місто», змістивши фокус із загальної протидії злочинності на оперативні завдання національної безпеки та оборони. Раніше такі програми координувалися переважно органами місцевого самоврядування, але тепер їхнє впровадження регулюється у тісній взаємодії з військовими адміністраціями, Силами оборони та правоохоронними органами. Головні зміни у функціонуванні та реалізації проєктів охоплюють зміну пріоритетів моніторингу, кібербезпеку, інтеграцію інтелектуальних функцій та питання фінансування.

Замість фіксації переважно дрібних правопорушень та контролю дорожнього руху, системи відеоспостереження тепер критично важливі для відстеження пересування ворожої техніки, диверсійно-розвідувальних груп, коригувальників вогню, а також для контролю за дотриманням комендантської години. Посилилися вимоги до захисту каналів зв'язку та збереження даних. Доступ до інтегрованих платформ «Безпечне місто» суворо обмежено – повний контроль мають співробітники СБУ, Національної поліції та військові. Закриваються будь-які публічні трансляції з міських камер, щоб ворог не міг оцінювати наслідки ракетних чи дронових ударів.

Обгрунтовано, що проєкти «Безпечне місто» є базовим елементом концепції «розумне місто» (Smart City), спрямованим на створення комфортного та захищеного середовища для мешканців українських міст.

Висвітлено, що людиноцентричність і партисипативність перетворюють систему «Безпечне місто» з технічного нагляду на функціонуючий простір спільної безпеки. Людиноцентричність у концепції «Безпечне місто» орієнтована на захист прав, доступність та якість життя громадян українських міст. Партисипативність як залучення громадян до управління міста охоплює такі напрями, як участь жителів міст у обговоренні розташування камер чи освітлення, локальні ініціативи для покращення безпеки районів міст, використання цифрових сервісів та додатків для швидкого реагування на проблеми та комунікації з комунальними службами.

Досліджено, що проблеми впровадження європейської моделі світового досвіду запровадження проєктів «Безпечне місто» в Україні полягають у залежності від окремих масових закордонних виробників апаратного забезпечення, недостатньому обсязі фінансування на рівні окремих міст в умовах воєнного стану, ризики порушення прав громадян на приватність через недосконалість законодавчого поля щодо регулювання біометричних даних.

Доведено, що впровадження концепції «Безпечне місто» в Україні спирається на передовий світовий досвід. Воно передбачає створення інтегрованих систем відеоспостереження з аналітикою, авторозпізнаванням номерів, сенсорами моніторингу довкілля та єдиними операційними центрами реагування для таких міст як Київ, Дніпро, Харків та Одеса.

Обґрунтовано, що для реалізації проєктів «Безпечне місто» в Україні доцільно вивчити західну та східну (азійську) моделі. В рамках західної моделі (досвід ЄС та США) фокусуються на балансі безпеки та захисту приватного життя, використанні європейського/американського обладнання та залученні громадськості через прозорі муніципальні платформи. Азійська/східна модель (досвід Сінгапуру, Китаю) характеризується тотальною цифровізацією, штучним інтелектом, прогнозна аналітика та глибока інтеграція біометричних даних.

Східна (азійська) модель проєкту «Безпечне місто» базується на жорсткій державній координації, масовому впровадженні штучного інтелекту, систем розпізнавання облич, Інтернету речей (IoT) та об'єднанні всіх комунальних і правоохоронних служб у єдині централізовані ситуаційні центри реагування в реальному часі. Ключовою рисою східної (азійської) моделі є домінування централізованого державного управління та єдиних вертикальних протоколів замість ініціатив представників місцевих органів влади. Активне застосування дронів-безпілотників із панорамними камерами для ліквідації простіру навколо автомобілів, які водій не може бачити через вікна чи джерела з огляду (стандартні дзеркала заднього виду) та моніторингу масових скупчень людей з повітря. Прямі канали зв'язку забезпечують миттєву передачу зашифрованого відеопотоку на планшети патрульних поліцейських ще до їх прибуття на місце події.

Сформульовано критерії оцінки ефективності вітчизняних програмних рішень із зарубіжними аналогами. Вітчизняні рішення найчастіше виграють за критеріями економічної доцільності, адаптивності до локального законодавства та безпеки, тоді як глобальні зарубіжні аналоги мають перевагу в масштабності системи, передових технологічних стандартах та готовій експертизі.

Доведено, що інтелектуальні системи інтеграції відеоданих відіграють критичну роль у сучасній координації служб порятунку, забезпечуючи перехід від пасивного спостереження до проактивного реагування в режимі реального часу. Вони об'єднують потоки з тисяч камер (міських, автомобільних, камер на тілі, дронів) в єдине цифрове середовище для прийняття рішень.

Зазначено, що формування міської координаційної ради з питань проєкту «Безпечне місто» здійснюється шляхом реалізації відповідного рішення виконавчого комітету міської ради або розпорядження міського голови. Цей орган створюється як консультативно-дорадчий для узгодження дій влади, правоохоронців, комунальних служб та громадськості у сфері розбудови інтелектуального відеоспостереження та безпекового простору.

Встановлено, що децентралізація міських вузлів – це стратегія сучасного містобудування, яка передбачає відмову від класичної моделі міста з одним домінуючим центром (моноцентризм) на користь створення мережі автономних, багатофункціональних районів (поліцентризм).

Запропоновано етапи розвитку джентрифікації в українських містах. Перетворення занепалих чи промислових районів на більш престижні та дорогі) зазвичай відбувається не за класичною західною схемою (де спочатку селяться мітці та студенти), а через капіталістичну ініціативу забудовника та точкову реконструкцію.

Виділено, що традиційна моноцентрична та поліцентрична моделі міст представляють два принципово різні підходи до організації міського простору, економіки та логістики. Якщо перша фокусується навколо єдиного історичного чи ділового центру, то друга розподіляє міські функції між кількома рівнозначними вузлами. У сучасному урбанізмі більшість мегаполісів світу намагаються трансформуватися з моноцентричної моделі у поліцентричну, оскільки це єдиний спосіб забезпечити екологічну та транспортну стійкість міста в умовах перенаселення.

Доведено, що впровадження поліцентричної міської структури в містах України є одним із ключових завдань сучасного вітчизняного містобудування. Перехід від моноцентричної моделі (де всі адміністративні, культурні та бізнесові функції зосереджені в одному історичному осередку) до поліцентричної (де створюється кілька самодостатніх підцентрів) дозволяє знизити навантаження на транспортну систему, покращити екологію та забезпечити концепцію «15-хвилинного міста». Впровадження поліцентричності в Україні є безальтернативним шляхом розвитку для подолання інфраструктурної кризи великих міст, особливо в процесах повоєнного відновлення та модернізації постраждалих регіонів.

Обґрунтовано, що ключові елементи безпекової інфраструктури формують стійкість українських міст в умовах сучасних викликів, охоплюють комплекс інженерних, цифрових, організаційних та соціальних рішень. Вони спрямовані

на захист населення, збереження критичних послуг та швидке відновлення після кризових ситуацій.

Визначено, що легітимність використання відкритих даних визначається правовими, етичними та технічними нормами, які забезпечують законність, безпеку та справедливість обробки інформації. Головний принцип полягає в тому, що дані мають бути не просто доступними, а їх використання не повинно порушувати права інших осіб чи державні інтереси.

Доведено, що розвиток безпекового простору в українських містах сьогодні базується на комплексній системі цивільного захисту, національної стійкості та концепції безбар'єрності й доступності середовища. Створення систем екстреного оповіщення з дублюванням інформації (звукові сигнали, текстові табло, жестова мова), забезпечення доступності цифрових платформ і додатків (наприклад, мапи укриттів) для людей з порушеннями зору чи слуху.

Використання хмарних технологій дозволяє відійти від застарілих локальних серверів на користь централізованих, масштабованих та захищених систем. Резервне копіювання всіх критичних даних життєзабезпечення міста у розподілені хмарні платформи (зокрема за межами України) для захисту від фізичних та кібератак. Хмарні системи аналізують дані з камер спостереження та навігаторів для динамічного регулювання світлофорів, зменшення заторів та пріоритезації громадського транспорту. Перенесення аналітики відеопотоків на хмарні платформи для використання алгоритмів штучного інтелекту дозволяє автоматично розпізнавати обличчя, автомобільні номери, виявляти залишені предмети або фіксувати ДТП.

Обґрунтовано вимоги до проєктування систем «Безпечне місто», що випливають із європейського правового регулювання та судової практики, конкретизовано зміст трьох рівнів управління (початкового, аналітичного, інтегрованого), запропоновано мінімальний безпековий пакет для громад із низькою спроможністю, визначено запобіжники для вразливих груп у соціально орієнтованих проєктах і завдання державного рівня: єдині вимоги до кожного рівня, кадрові нормативи, співфінансування та державний моніторинг.

Сформовано методичні вимоги до запровадження систем «Безпечне місто» за етапами – від діагностики безпекової ситуації та обґрунтування мети до оцінки впливу на приватність, правил функціонування, прозорості, щорічного оцінювання результативності та фінансування.

Ключові слова: безпека, безпечне місто, проєкт «Безпечне місто» державне управління, правоохоронні органи, інфраструктура, публічне управління, національна безпека, держава, хмарні технології, цифровізація, відеоспостереження, безпекові програми, соціальна політика міста, соціальний розвиток міста.

ANNOTATION

Pustovit O.B. Justification for the Implementation of "Safe City" Projects at the State Level in Ukraine. Scientific qualification work (manuscript).

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 28 "Public Management and Administration," specialty 281 "Public Management and Administration." Higher Education Institution "Open International University of Human Development 'Ukraine'." Kyiv, 2026.

The dissertation is dedicated to the development and substantiation of theoretical and methodological principles and practical recommendations regarding the implementation of "Safe City" projects at the state level in Ukraine

The implementation of the "Safe City" concept and projects at the national level in Ukraine is driven by the need to create an integrated, digital, and adaptive public safety system–particularly given the context of martial law and post-war reconstruction.

Digital technologies–such as video surveillance, big data analytics, and geoinformation systems–transform urban infrastructure from a potential target into a resilient system capable of withstanding military threats and cyberattacks. This concept serves as a strategic public management tool for monitoring urban spaces, detecting threats early, and enabling rapid responses to dangerous situations.

Currently, "Safe City" projects are primarily implemented at the individual city level, resulting in disparities in technical equipment, as well as incompatible databases and standards. A national-level approach allows for the establishment of unified technical and legal standards. Furthermore, centralized funding and coordination among the Ministry of Internal Affairs, the Security Service of Ukraine (SBU), the State Emergency Service, and local authorities help optimize expenditures on equipment and software procurement.

The initiative acts as a catalyst for integrating artificial intelligence and the Internet of Things (IoT) into the operations of law enforcement agencies and emergency services. Automated detection of offenses, along with facial and license

plate recognition, significantly reduces crime rates and accelerates the resolution of criminal cases. Scholars and practitioners define the "Safe City" concept not merely as a collection of surveillance cameras, but as a new standard of public administration that balances citizen safety with the principles of personal data protection.

An analysis of academic and informational sources reveals that "Safe City" projects are, in essence, comprehensive systems comprising organizational, legal, software, and technical components. These systems integrate video surveillance, data analytics, and community-police interaction to protect residents, manage traffic, and facilitate real-time responses to emergencies.

The imposition of martial law has fundamentally altered the implementation of "Safe City" projects, shifting the focus from general crime prevention to operational tasks related to national security and defense. While such programs were previously coordinated primarily by local self-government bodies, their implementation is now managed in close cooperation with military administrations, the Defense Forces, and law enforcement agencies. Key changes in the operation and execution of these projects concern monitoring priorities, cybersecurity, the integration of intelligent functions, and funding.

Rather than focusing primarily on minor offenses and traffic control, video surveillance systems have become critical for tracking the movement of enemy equipment, sabotage and reconnaissance groups, and fire-spotters, as well as for enforcing the curfew. Furthermore, requirements for securing communication channels and preserving data have been strengthened. Access to integrated "Safe City" platforms is strictly restricted; full control lies with the SBU (Security Service of Ukraine), the National Police, and the military. Public live streams from city cameras are disabled to prevent the enemy from assessing the aftermath of missile or drone strikes.

It is established that "Safe City" projects serve as a foundational element of the "Smart City" concept, aimed at creating a comfortable and secure environment for the residents of Ukrainian cities.

The analysis highlights that a human-centric approach and civic participation transform the "Safe City" system from a mere tool for technical surveillance into a

functional space for collective security. Within the "Safe City" framework, a human-centric focus prioritizes the protection of rights, accessibility, and the quality of life for citizens. Civic participation-involving residents in city governance-encompasses areas such as public consultation on the placement of cameras or street lighting, local initiatives to enhance neighborhood safety, and the use of digital services and applications to facilitate rapid responses to issues and communication with municipal utility services.

The study identifies several challenges in implementing the European model of "Safe City" projects in Ukraine. These include a reliance on specific large-scale foreign hardware manufacturers, insufficient funding at the municipal level under martial law, and the risk of infringing upon citizens' privacy rights due to an inadequate legislative framework regarding the regulation of biometric data. It has been established that the implementation of the "Safe City" concept in Ukraine draws upon advanced global practices. This involves establishing integrated video surveillance systems-featuring analytics, automatic license plate recognition, and environmental monitoring sensors-alongside centralized operational response centers in cities such as Kyiv, Dnipro, Kharkiv, and Odesa.

It is argued that, for the implementation of "Safe City" projects in Ukraine, it is advisable to examine both Western and Eastern (Asian) models. The Western model-drawing on the experience of the EU and the US-focuses on balancing security with the protection of privacy, utilizing European or American equipment, and engaging the public through transparent municipal platforms. The Eastern (Asian) model-exemplified by Singapore and China-is characterized by comprehensive digitalization, the use of artificial intelligence and predictive analytics, and the deep integration of biometric data.

The Eastern (Asian) "Safe City" model relies on strict state coordination, the large-scale deployment of artificial intelligence, facial recognition systems, and the Internet of Things (IoT), as well as the integration of all municipal and law enforcement services into unified, centralized real-time response centers. A key feature of this model is the dominance of centralized state governance and standardized vertical protocols,

rather than initiatives driven by local authorities. It involves the active use of drones equipped with panoramic cameras-which eliminate blind spots around vehicles (areas not visible through windows or standard rearview mirrors)-and the aerial monitoring of large crowds. Direct communication channels enable the instant transmission of encrypted video feeds to the tablets of police officers, even before they arrive at the scene. Criteria have been formulated for evaluating the effectiveness of domestic software solutions in comparison with their foreign counterparts. Domestic solutions typically excel in terms of economic viability, adaptability to local legislation, and security, whereas global foreign alternatives offer advantages regarding system scalability, advanced technological standards, and established expertise.

It has been demonstrated that intelligent video data integration systems play a critical role in the modern coordination of emergency services, facilitating a shift from passive surveillance to proactive, real-time response. These systems aggregate feeds from thousands of sources-including urban, vehicle-mounted, and body-worn cameras, as well as drones-nto a unified digital environment for decision-making.

It is noted that the establishment of a municipal coordination council for the «Safe City» project is effected through a resolution by the city council's executive committee or an order issued by the mayor. This body serves an advisory function, coordinating the efforts of government authorities, law enforcement, municipal services, and the public in the development of intelligent video surveillance and a secure urban environment.

It has been established that the decentralization of urban hubs is a modern urban planning strategy that entails moving away from the traditional monocentric city model-characterized by a single dominant center-toward a polycentric model, which consists of a network of autonomous, multifunctional districts.

Stages for the development of gentrification in Ukrainian cities have been proposed. The transformation of dilapidated or industrial districts into more prestigious and expensive areas typically does not follow the classic Western pattern-where artists and students move in first-but rather occurs through capitalist developer initiatives and targeted, site-specific redevelopment.

It is noted that traditional monocentric and polycentric urban models represent two fundamentally different approaches to organizing urban space, the economy, and logistics. While the former focuses on a single historical or business center, the latter distributes urban functions across several equivalent hubs. In contemporary urbanism, many of the world's major metropolises are seeking to transition from a monocentric to a polycentric model, as this is the only way to ensure environmental and transport sustainability in the face of overpopulation.

It has been established that implementing a polycentric urban structure is a key objective for modern urban planning in Ukraine. Shifting from a monocentric model-where all administrative, cultural, and business functions are concentrated in a single historical center-to a polycentric one-characterized by the creation of several self-sufficient sub-centers-helps reduce the strain on transport systems, improves environmental conditions, and facilitates the realization of the «15-minute city» concept. Adopting a polycentric approach is an essential development path for Ukraine to overcome the infrastructure crisis in its large cities, particularly within the context of post-war reconstruction and the modernization of affected regions. It is established that the key elements of security infrastructure-comprising a complex of engineering, digital, organizational, and social solutions-foster the resilience of Ukrainian cities in the face of modern challenges. These elements are aimed at protecting the population, maintaining critical services, and ensuring rapid recovery following crisis situations.

It is determined that the legitimacy of using open data is governed by legal, ethical, and technical standards that ensure the lawfulness, security, and fairness of information processing. The core principle is that data must not merely be accessible; its use must not infringe upon the rights of others or compromise state interests.

It has been established that the development of a secure environment in Ukrainian cities today relies on a comprehensive system encompassing civil protection, national resilience, and the concepts of a barrier-free, accessible environment. This includes the creation of emergency alert systems that utilize redundant communication channels (auditory signals, text displays, and sign language), as well as ensuring that

digital platforms and applications-such as maps of shelters-are accessible to individuals with visual or hearing impairments.

The adoption of cloud technology enables a transition away from outdated local servers toward centralized, scalable, and secure systems. Critical data essential for the city's life-support functions is backed up to distributed cloud platforms-including those located outside of Ukraine-to safeguard against physical and cyberattacks. Cloud-based systems analyze data from surveillance cameras and navigation tools to dynamically adjust traffic lights, alleviate congestion, and prioritize public transport. Furthermore, migrating video stream analytics to cloud platforms allows for the application of artificial intelligence algorithms, enabling the automated recognition of faces and license plates, the detection of unattended objects, and the identification of traffic accidents.

The study substantiates design requirements for "Safe City" systems derived from European legal regulation and case law, specifies the content of three management levels (initial, analytical and integrated), proposes a minimum security package for communities with limited capacity, and identifies safeguards for vulnerable groups in socially oriented projects together with state-level tasks: unified requirements for each level, staffing standards, co-financing and state monitoring. Methodological requirements for the implementation of "Safe City" systems are formulated by stages, from the diagnosis of the security situation and the justification of the purpose to the privacy impact assessment, operating rules, transparency, annual performance evaluation and financing.

Key words: security, safe city, Safe City Project, state administration, law enforcement agencies, infrastructure, public administration, national security, state, cloud technologies, digitalization, video surveillance, security programs, urban social policy, urban social development.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

1. **Пустовіт О. Б.,** Крилова І. І. Обґрунтування запровадження проектів «Безпечне місто» на державному рівні в Україні. *Інвестиції: практика та досвід.* 2023. № 11. С. 126-131. DOI: https://doi.org/10.32702/2306-6814.2023.11.126 *(Крилова І. І. – здійснено систематизацію вітчизняного та зарубіжного досвіду цифрової трансформації муніципальної інфраструктури й виокремлено організаційно-правові передумови централізації безпекових проєктів. Пустовіт О. Б. – обґрунтовано необхідність переходу від локальних ініціатив до загальнодержавного рівня задля цифрової трансформації публічного адміністрування).*

2. **Пустовіт О. Б.,** Крилова І. І. Управління ефективністю існуючих заходів забезпечення безпеки міст. *Науковий журнал «Успіхи та досягнення в науці».* 2024. № 1 (1). С. 258-266. DOI: https://doi.org/10.52058/3041-1254-2024-1(1)-258-266. (*Крилова І. І. – розроблено аналітичний підхід до оцінювання результативності превентивних заходів та структуровано взаємодію екстрених служб у єдиному інформаційному просторі міст. Пустовіт О. Б. – розкрито аналіз наявних інструментів забезпечення публічного порядку й безпеки життєдіяльності в містах України зокрема в умовах воєнного стану та адаптації до повоєнного відновлення).*

3. **Пустовіт О. Б.,** Крилова І. І. Оцінка ефективності існуючих заходів забезпечення безпеки міст. *Науковий журнал «Успіхи та досягнення в науці».* 2024. № 2 (2). С. DOI: https://doi.org/10.52058/3041-1254-2024-2(2)-196-204 *(Крилова І. І. – описано методології оцінювання того, як органи публічної влади керують безпековими ризиками, координують дії екстрених служб і впроваджують превентивні заходи. Пустовіт О .Б. – описано методології оцінювання того, як органи публічної влади керують безпековими ризиками,*

координують дії екстрених служб і впроваджують превентивні заходи)

4. Пустовіт О. Б. Передумови та цілі впровадження проєктів «Безпечне місто» на державному рівні. *Актуальні проблеми інноваційної економіки та права.* 2026. №3. С. 187-191. DOI: https://doi.org/10.36887/2524-0455-2026-3-35 .

5. Пустовіт О. Б. Проєкт «Безпечне місто» як інструмент державного управління у сфері забезпечення національної безпеки України. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С. 389-397. DOI: https://doi.org/10.31891/2307-5740-2026-356-52.

Тези наукових доповідей

6. Пустовіт О. Б. Проекти «Безпечне місто»: запровадження на державному рівні в Україні. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : матеріали І Міжнар. наук.-практ. конф. (2 черв. 2023 р.) / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 220-223.

7. Пустовіт О. Б. Значення проектів «Безпечне місто» на державному рівні в Україні. *Складові національної безпеки в умовах воєнного стану* : матеріали наук.-практ. конф. з міжнар. участю (м. Київ, 09-11 серп. 2023 р.) / за заг. ред. З. В. Гбур. Кам'янець-Подільський : Друкарня Рута, 2023. С. 413-418.

8. Пустовіт О. Б. Обгрунтування запровадження проектів «Безпечне місто». *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : матеріали ІІ Міжнар. наук.-практ. конф. (27 жовт. 2023 р.) / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 188–191.

9. Пустовіт О. Б. Потенціал впровадження проектів «Безпечне місто в Україні». *Національна безпека України в умовах воєнного стану* : матеріали І наук.-практ. конф. з міжнар. участю (м. Чернігів, 06-08 берез. 2024 р.) / за заг. ред. З. В. Гбур. Чернігів : ІПТ, 2024. С. 208-211.

10. Пустовіт О. Б. Оцінка ефективності існуючих заходів забезпечення безпеки міст. *Тренди сталого розвитку для України* : зб. тез І наук.-практ. конф. за міжнар. участю (м. Чернігів – м. Київ, 10 лип. 2024 р.). Чернігів : УТМ, 2024. С. 77–80.

11. Пустовіт О. Б. Державне управління процесом реалізації програми «Безпечне місто» в умовах цифрової трансформації. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : зб. наук. пр. з матеріалами VII Міжнар. наук. конф. (м. Харків, 31 лип. 2026 р.) / Міжнар. центр наук. досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 59–61.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI / ШІ – Artificial Intelligence – штучний інтелект;

ANPR – Automatic Number Plate Recognition – автоматичне розпізнавання автомобільних номерних знаків;

Big Data – технології та масиви обробки великих даних;

CDTO – Chief Digital Transformation Officer – керівник цифрової трансформації;

GDPR – General Data Protection Regulation – Загальний регламент про захист даних;

ГІС – геоінформаційні системи;

ДСНС – Державна служба з надзвичайних ситуацій України;

ДТП – дорожньо-транспортна пригода;

ДТП – дорожньо-транспортна пригода;

ЄС – Європейський Союз;

ЄСПЛ – Європейський суд з прав людини;

IoT – Internet of Things – Інтернет речей;

ISO – International Organization for Standardization – Міжнародна організація зі стандартизації;

МВС – Міністерство внутрішніх справ України;

ООН – Організація Об’єднаних Націй;

ПДР – Правила дорожнього руху;

РНБО – Рада національної безпеки і оборони України;

СБУ – Служба безпеки України;

UNFPA – United Nations Population Fund – Фонд ООН у галузі народонаселення;

UN – Habitat – Програма ООН з населених пунктів;

ЦНАП – Центр надання адміністративних послуг;

ЦСР – Цілі сталого розвитку;

ВПО – внутрішньо переміщені особи;

КМУ – Кабінет Міністрів України;

IP – Internet Protocol – інтернет-протокол.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 18

ВСТУП 21

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ КОНЦЕПЦІЇ ПРОЄКТІВ «БЕЗПЕЧНЕ МІСТО» НА ДЕРЖАВНОМУ РІВНІ В УКРАЇНІ 31

1.1. Категоріальна сутність поняття проєкт «Безпечне місто» 31

1.2. Різновиди сучасних проєктів «Безпечне місто» 43

1.3. Методичні основи запровадження системи «Безпечне місто» 54

Висновки до розділу 1. 66

РОЗДІЛ 2. ОСОБЛИВОСТІ ФУНКЦІОНУВАНЯ СИСТЕМ «БЕЗПЕЧНЕ МІСТО» В УКРАЇНСЬКИХ РЕАЛІЯХ 71

2.1. Впровадження моделей світового досвіду в Україні 71

2.2. Розвиток соціальної політики держави у проєктах «Безпечне місто» 95

2.3. Характеристика рівня управління українськими населеними пунктами при реалізації проєктів «Безпечне місто» 116

Висновки до розділу 2 135

РОЗДІЛ 3. ЗАПРОВАДЖЕННЯ СИСТЕМ «БЕЗПЕЧНЕ МІСТО» НА РІВНІ УКРАЇНСЬКОЇ ДЕРЖАВИ 144

3.1. Концепція стратегічного розвитку систем «Безпечне місто» на території України 144

3.2. Використання хмарних технологій в рамках підвищення рівня безпеки в містах України 153

3.3. Напрями підвищення ефективності процесу управління українськими населеними пунктами із застосуванням системи «Безпечне місто» 172

Висновки до розділу 3. 188

ВИСНОВКИ 193

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 201

ДОДАТКИ 233

ВСТУП

Актуальність теми. Запровадження проєктів «Безпечне місто» на державному рівні в Україні визначається сучасними викликами у сфері публічного управління, національної безпеки та цифрової трансформації. Зростання ризиків терористичних актів, диверсій, ракетних обстрілів та необхідність оперативного реагування на надзвичайні ситуації вимагають централізованої системи відеомоніторингу й аналітики.

За сучасних умов проєкти «Безпечне місто» реалізуються переважно локально (на рівні окремих громад чи міст), що створює різний рівень технологічного оснащення, проблеми з сумісністю даних і відсутність загальнодержавної координації. Інтеграція систем відеоспостереження з розпізнаванням облич, номерних знаків авто та аналітикою великих даних (Big Data) дозволяє підвищити розкриття злочинів і загальний рівень правопорядку.

Концепція «Безпечне місто» є базовим компонентом розвитку сучасних «розумних міст», що оптимізує роботу транспортних мереж, ЖКГ, екологічного моніторингу та екстрених служб (ДСНС, поліція, медицина катастроф). Централізований підхід дозволяє раціонально використовувати державний бюджет, залучати міжнародні інвестиції та забезпечити прозорість процесів безпеки.

В Україні запровадження проєктів «Безпечне місто» на державному рівні перебувають на етапі інтеграції локальних систем у єдину загальнодержавну платформу- Єдину систему відеомоніторингу стану публічної безпеки під егідою Міністерства внутрішніх справ (МВС) та Національної поліції [103]. Цей процес супроводжується двома ключовими процесами: законодавчим врегулюванням та технологічним об’єднанням. Триває опрацювання законопроєкту «Про єдину систему відеомоніторингу стану публічної безпеки». Він має закріпити єдині стандарти для встановлення й адміністрування камер, а також захисту персональних даних. Паралельно відбувається поетапна трансформація від

локальних рішень (індивідуальних для кожного міста) до трирівневої архітектури. Камери місцевих систем «Безпечне місто», відеокамери на дорогах державного значення та об'єктах інфраструктури інтегруються до єдиного аналітичного контуру на базі МВС із використанням інструментів штучного інтелекту та розпізнавання облич.

У дослідженнях О. Коробка та А. Ткача обґрунтовано еволюцію концепції «Безпечне місто» від інструменту локального захисту публічного порядку до фундаменту національної безпеки. Науковці доводять необхідність інтеграції цих систем у загальний контур оборони держави для захисту її суверенітету від традиційних та асиметричних загроз в умовах військового стану.

У свох працях В. Мороз фокусується на імплементації світового досвіду автоматизації публічного управління та цивільного захисту, аналізуючи фінансові інвестиції громад і розбудову інтелектуальних безпекових мереж.

Науковець О. Руденко детально аналізує теоретичні та державно-управлінські засади проєкту «Безпечне місто» як інтегрованого механізму державного управління. Автор наголошує на трансформації систем відеоспостереження у комплексні цифрові платформи для міжвідомчої координації (МВС, ДСНС, СБУ) та інформаційного забезпечення прийняття рішень на державному рівні.

Дослідники Ю. Тимошенко і Д. Кисленко вивчають цифровізацію правоохоронної системи та правове регулювання використання систем штучного інтелекту, біометричного розпізнавання Big Data в межах проєктів «Безпечне місто» [115].

Отже, дослідження лежать у площині державного управління, національної безпеки та адміністративного права [170; 198]. Вони доводять, що концепція «Безпечне місто» в Україні вже переросло рівень звичайного встановлення камер комунальними службами та має регулюватися єдиною державною стратегією.

Для повноцінного наукового та прикладного обґрунтування системи «Безпечне місто» на державному рівні необхідно розробити цілісну трирівневу

модель, яка б об’єднувалатакі складові: безпеку окремої людини (захист прав та персональних даних); безпеку міст (цифровізацію локальної інфраструктури, контроль трафіку та публічного простору) та національну безпеку держави (інтеграцію систем у загальний контур стійкості проти внутрішніх та зовнішніх загроз). Доцільною є чітке закріплення нормативно-правового статусу та дефініції самого поняття «Безпечне місто». Сучасні проєкти «Безпечне місто» впроваджуються фрагментарно, переважно на основі локальних актів органів місцевого самоврядування (наприклад, положень міських рад), що ускладнює загальнодержавну сертифікацію. захистом персональних даних, приватністю й дотриманням прав людини**.** Відсутність чітких законодавчих меж використання штучного інтелекту у моніторингу публічного простору періодично призводить до судових розбіжностей щодо законності доступу до таких баз.

Дисертація спрямована на вирішення науково-прикладної проблеми щодо запровадження проєктів «Безпечне місто» на державному рівні в Україні, що й обумовило вибір теми дослідження, його мету, структуру та завдання.

Зв’язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження відповідає проблематиці науково-дослідної роботи кафедри міжнародних відносин та політичного консалтингу Інституту права та суспільних відносин ЗВО «Відкритий міжнародний університет розвитку людини «Україна» за темою «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322) (довідка від 02.10.2026 р. № 13/23-271), де автором проаналізовано інституційне забезпечення державного регулювання інформаційної безпеки в системі національної безпеки України, зокрема: теоретико-методичні засади запровадження проєктів «Безпечне місто» на державному рівні; особливості функціонування та трансформації систем відеоспостереження й аналітики в умовах воєнного стану; рівні управління та організаційні засади взаємодії суб’єктів публічного управління, правоохоронних органів і Сил оборони; а також стан дотримання прав, свобод і законних інтересів людини і громадянина, забезпечення кіберзахисту та захисту персональних

даних при інтеграції локальних рішень у єдиний інформаційно-комунікаційний простір національної безпеки.

Мета і завдання дослідження. Метою дослідження виступає обґрунтування теоретичних і прикладних засад, а також практичних рекомендацій щодо запровадження проєктів «Безпечне місто» на державному рівні в Україні.

Досягнення поставленої мети зумовило визначення та вирішення наведених дослідницьких **завдань**:

- аналіз теоретичних засад запровадження проєктів «Безпечне місто» на державному рівні в Україні;
- класифікація різновидів сучасних проєктів «Безпечне місто» у контексті українських реалій сьогодення;
- формулювання методичних основ запровадження та реалізації системи «Безпечне місто»;
- аналіз світових моделей впровадження проєктів «Безпечне місто» для адаптації в Україні;
- виявлення соціально-орієнтованого підходу до реалізації проєктів «Безпечне місто»;
- визначення рівня управління українськими населеними пунктами при реалізації проєктів «Безпечне місто»;
- формулювання концепції стратегічного розвитку систем «Безпечне місто» на території України;
- вивчення можливостей хмарних технологій в рамках підвищення рівня безпеки в містах України;
- підвищення ефективності процесу управління українськими населеними пунктами із застосуванням системи «Безпечне місто».

Об'єкт дослідження – процес запровадження проєктів «Безпечне місто» на державному рівні в Україні.

Предмет дослідження – сукупність теоретичних, методологічних та прикладних засад формування, запровадження й розвитку процесу управління

національною безпекою України за допомогою інструментів, які застосовуються в рамках проєктів «Безпечне місто».

Методи дослідження. Теоретичною і методологічною базою дослідження є наукові розробки вітчизняних і зарубіжних вчених щодо обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні. У процесі обґрунтування теоретичних та практичних питань дослідження використовувалися такі наукові методи: аналізу та синтезу, моделювання та формалізації – для дослідження теоретичних підходів та концептуальної сутності поняття «Безпечне місто»; упорядкування та узагальнення понятійного апарату проєкту «Безпечне місто»; системний та процесний метод – для формування концептуальних засад оцінки цільових програм «Безпечне місто»; статистичного аналізу, економіко-порівняльного аналізу, імовірнісного – для рекомендації вимірювальних блоків єдиного Індексу безпеки українських міст та критеріїв легітимності використання відкритих даних; експертних оцінок, групування – для здійснення експертної оцінки впливу основних критеріїв оцінки ефективності вітчизняних програмних рішень та із зарубіжними аналогами; функціональний – для визначення рівня впровадження поліцентричної міської структури в містах України; графічні–для побудови рисунків і таблиць, з метою візуалізації результатів дослідження; системного підходу – для комплексного та взаємопов'язаного врахування економічних, екологічних, правових та соціальних аспектів порівняння локальної інфраструктури та хмарних технологій у проєктах «Безпечне місто»; моделювання і формалізації – для розробки етапів розвитку джентрифікації в українських містах; абстрактно-логічний – для узагальнення теоретико-методичних засад та формулювання висновків дослідження.

Дослідження базуються на таких джерелах первинної та вторинної інформації:

1. Нормативно-правових актах України (Конституція України [1], Цивільний кодекс України [6], Цивільний процесуальний кодекс України [7], Господарський кодекс України [2], Кодекс адміністративного судочинства

України [4], Закон України «Про місцеве самоврядування в Україні» [19], Закон України «Про адміністративні послуги», Закон України «Про національну безпеку України» [20], Закон України «Про Національну програму інформатизації» [22], Закон України «Про звернення громадян» [17], Закон України «Про службу в органах місцевого самоврядування», Закон України «Про основні засади забезпечення кібербезпеки України» [23], Закон України «Про хмарні послуги» [30], Закон України «Про державну службу спеціального зв'язку та захисту інформації» [13], Закон України «Про державну службу» [12], Закон України «Про державне прогнозування та розроблення програм економічного і соціального розвитку України» [9], Закон України «Про державну підтримку інвестиційних проектів із значними інвестиціями в Україні» [11], Постанови та розпорядження Кабінету Міністрів, зокрема «Про схвалення Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року» [38] та «Про затвердження плану заходів на 2025-2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року» [35], а також «Про схвалення Концепції Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року» [37]). Нормативно-правові акти, що втратили чинність після початку дослідження (2023 р.), наведено в редакціях, чинних на час їх аналізу, для збереження спадковості висновків і моделювання.

2. Стратегії реформування державного управління України на 2026-2030 роки [134].

3. Постановах Пленуму Верховного Суду України, Рішеннях Конституційного Суду України, Роз'ясненнях Вищого арбітражного суду України.

4. Статистичні дані Державної служби статистики України та звіти КМУ.

5. Вітчизняних та зарубіжних наукових публікацій та аналітичних досліджень.

6. Результатах соціологічних опитувань та експертного середовища.

Наукова новизна отриманих результатів полягає у тому, що дисертаційне дослідження є одним із перших комплексних досліджень державного управління національною безпекою, у якому системно поєднано теоретико-правовий аналіз із практико-орієнтованими підходами до запровадження проєктів «Безпечне місто» на території України. У межах проведеного дослідження сформульовано такі положення наукової новизни:

вперше:

- розроблено цілісну концепцію державного управління інтеграцією локальних систем «Безпечне місто» в єдиний інформаційно-комунікаційний простір національної безпеки, що передбачає трансформування розрізнених муніципальних проєктів на елемент загальнодержавної системи стійкості України;

удосконалено:

- категоріальну сутність проєктів «Безпечне місто», яка полягає в тому, що вони є комплексними організаційно-правовими та програмно-технічними системами, які об’єднують відеоспостереження, аналітику даних та взаємодію громадян із представниками поліції, контролю трафіку та оперативного реагування на надзвичайні події в реальному часі;
- наукові підходи моделі проєктів «Безпечне місто» базується на жорсткій державній координації, масовому впровадженні штучного інтелекту, систем розпізнавання облич, Інтернету речей та об’єднанні всіх комунальних і правоохоронних служб у єдині централізовані ситуаційні осередки реагування в реальному часі;
- механізм перенесення аналітики відеопотоків у хмарні платформи з використанням алгоритмів штучного інтелекту, що дозволяє автоматично розпізнавати обличчя, автомобільні номери, виявляти залишені предмети або фіксувати ДТП.
- класифікацію рівнів управління проєктами «Безпечне місто» (початковий, аналітичний, інтегрований), доповнену мінімальними правовими,

кадровими, технічними та кібербезпековими вимогами до кожного рівня і мінімальним безпековим пакетом для громад із низькою спроможністю;

набули подальшого розвитку:

- система показників оцінки ефективності міської програми «Безпечне місто» за рахунок порівняння витрачених коштів із реальними результатами (кількістю розкритих злочинів за допомогою камер, зменшенням рівня злочинності на вулицях, станом дорожнього руху та відгуками жителів українських міст).
- соціально-орієнтований підхід до реалізації проєктів «Безпечне місто», що передбачає використанні штучного інтелекту та відеоаналітики для формування системи прогнозованих випереджувальних заходів, спрямованих на запобігання правопорушенням до того, як вони настануть.
- система управлінських вимог до проєктування систем «Безпечне місто», сформована на основі узагальнення європейського правового регулювання та практики Європейського суду з прав людини і національних судів (законне визначення підстав і меж застосування біометричних та аналітичних функцій, попередня оцінка впливу, нормативні строки зберігання, журналювання доступу, незалежний аудит);
- положення щодо електронних запобіжних пристроїв для вразливих груп у соціально орієнтованих проєктах «Безпечне місто» (мінімізація даних під час поєднання безпекових і соціальних систем, оцінка впливу на рівність до запровадження аналітичних функцій, збереження нецифрових каналів звернення по допомогу) та щодо вимірювання їх результативності на основі індикатора 11.7.2 Цілей сталого розвитку.

Практичне значення отриманих результатів отриманих результатів полягає в розробленні науково-практичних положень і рекомендацій щодо запровадження проєктів «Безпечне місто» на державному рівні в Україні, удосконалення інформаційно-аналітичного забезпечення публічного управління, розвитку цифрових інструментів оброблення інформації та підвищення ефективності міжвідомчої інформаційної взаємодії. Практична

цінність результатів дисертаційного дослідження підтверджується їх використанням у діяльності державних органів та освітньому процесі, зокрема:

- результати дисертаційного дослідження впроваджено в освітній процес ЗВО «Відкритий міжнародний університет розвитку людини «Україна» та використано під час розроблення робочих програм, силабусів і викладання навчальних дисциплін «Громадські об'єднання в Україні» для здобувачів першого (бакалаврського) рівня вищої освіти та «Міжнародна та національна безпека» для здобувачів другого (магістерського) рівня вищої освіти (довідка про впровадження № 13/23-270 від 02.10.2026 р.);
- науково-практичні положення та рекомендації щодо використання хмарних технологій, інтелектуальної аналітики даних, інтеграції інформаційних систем, стандартизації цифрових рішень і забезпечення захищеного інформаційного обміну використано в діяльності Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, з метою вдосконалення інформаційно-аналітичного забезпечення, підвищення ефективності міжвідомчої інформаційної взаємодії та розвитку цифрових інструментів підтримки управлінських рішень (довідка про впровадження № 02-34/2026 від 21.09.2026 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею, у якій викладено авторський підхід до розробки методико-прикладних положень щодо визначення положень запровадження. Наукові результати, представлені в дисертації, розроблено автором особисто. З наукових публікацій, виданих у співавторстві, у роботі використано лише ті положення, які становлять особистий внесок авторки, про що зазначено в переліку публікацій.

Апробація матеріалів дисертації. Основні науково-теоретичні та практичні результати дисертації були оприлюднені на: IV Всеукраїнській науково-практичній конференції молодих вчених та студентів «Трансформаційні процеси соціально-економічної системи в умовах сучасних викликів»

(Університет Григорія Сковороди в Переяславі, м. Переяслав, 27 листопада 2025 р.); ІІ науково-практичній конференції за міжнародною участю «Проблеми управління суспільним розвитком в умовах криз та післякризового відновлення» (Національний університет охорони здоров'я України імені П.Л. Шупика, м. Київ, 4 грудня 2025 р.); Міжнародній науково-практичній конференції «Перспективи та інновації сучасної науки: теорія, практика та глобальні виклики» (м. Ізмаїл, 17 квітня 2026 р.); XIX Міжнародній науково-практичній конференції «Умови економічного зростання в країнах з ринковою економікою» (м. Переяслав, 23–24 квітня 2026 р.).

Публікації. Основні положення дисертаційного дослідження викладено у 11 наукових працях, з яких 5 статей у наукових фахових виданнях України, 6 тез наукових доповідей.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи становить 245 сторінок. Дисертація містить 20 таблицю, 8 рисунків та 3 додатки. Список використаних джерел містить 259 найменувань.

РОЗДІЛ І
ТЕОРЕТИЧНІ ОСНОВИ КОНЦЕПЦІЇ ПРОЄКТІВ «БЕЗПЕЧНЕ МІСТО» НА ДЕРЖАВНОМУ РІВНІ В УКРАЇНІ

1.1. Категоріальна сутність поняття проєкт «Безпечне місто»

Необхідність запровадження проєктів «Безпечне місто» зумовлена потребою забезпечити захист громадян України та їх майна на державному рівні, послуговуючись виконанням відповідних функцій на місцях. Такі проєкти представлені функціонуванням інтелектуальних відеокамер, датчиків та зв'язку в рамках єдиної мережі. Головне призначення комплексних проєктів «Безпечне місто» полягає в координації роботи екстрених служб (поліція, ДСНС), управління дорожнім рухом, моніторинг інфраструктури та забезпечення громадської безпеки в режимі реального часу. Такі проєкти допомагають представникам поліції та Державної служби з надзвичайних ситуацій швидко ловити злочинців, стежити за дорогами та допомагати громадянам під час аварій або небезпеки [99].

Камери спостереження сприяють зниженню рівня злочинності у людних місцях та вулицях українських міст. Завдяки цьому системи фіксують порушення правил, зменшуючи кількість аварій на дорогах. Екстрені служби бачать проблеми одразу і швидше реагують на виклик. Камери розпізнають обличчя та номери машин для швидкого пошуку зниклих. Так, запровадження проєктів «Безпечне місто» забезпечує зменшення кількості злочинів на вулицях і дворах, швидке реагування на надзвичайні ситуації, створюючи умови для спокійного життя усіх мешканців українських міст.

Основні функції за призначенням системи комплексних проєктів «Безпечне місто» представлені в таблиці 1.1.

Таблиця 1.1

Основні функції проєктів «Безпечне місто»

№ п\п	Функція	Сутність
1.	Громадська безпека та правопорядок	Цілодобовий відеомоніторинг вулиць з автоматичним розпізнаванням номерних знаків, облич та порушень Правил дорожнього руху для оперативного реагування на злочини та збереження доказів (відеозаписи слугують доказом у суді або для пошуку автомобілів та громадян)
2.	Управління дорожнім рухом	Автоматична фіксація порушень правил дорожнього руху (швидкість, перетин смуг), моніторинг трафіку та дистанційне керування світлофорами для запобігання заторам
3.	Контроль комунальних служб та інфраструктури	Координація роботи служб благоустрою, контроль за прибиранням снігу, вивезенням сміття та станом дорожнього покриття.
4.	Кризовий менеджмент	Миттєве оповіщення про надзвичайні ситуації (аварії, пожежі, стихійні лиха) та координація евакуації чи рятувальних операцій
5.	Аналітика даних	Збирання, обробка та архівація масивів даних, які дозволяють створювати теплові карти, оптимізувати маршрути громадського транспорту та планувати розвиток громади

Джерело: складено автором на основі проведених досліджень

Отже, основні функції проєктів «Безпечне місто» охоплюють цілодобовий відеомоніторинг вулиць, розпізнавання автомобільних номерів, облич та об’єктів, контроль за станом комунальної інфраструктури, а також оперативну координацію дій екстрених служб та поліції для запобігання правопорушенням. Превентивна та правоохоронна функція передбачає дію, спрямовану на попередження, уникнення або заздалегідь підготовлену протидію можливій загрозі, небезпеці чи проблемній ситуації. Управлінська функція проєктів «Безпечне місто» розкривається в контролі функціонування комунальних служб, оптимізації транспортних потоків та координація роботи екстрених служб у реальному часі. Соціальна спрямованість проєктів «Безпечне місто» забезпечує формування безпечного середовища для життя мешканців українських міст та комфорту їх гостей.

Визначення концепції «Безпечне місто» еволюціонувало від класичного захисту від злочинності до комплексних систем. Воно об’єднує технології,

інфраструктуру та суспільну взаємодію задля безпеки громадян українських міст. У наукових і практичних джерелах виділяють кілька підходів до визначення категорії проєктів «Безпечне місто» (табл. 1.2).

Таблиця 1.2

Підходи до визначення категорії проєктів «Безпечне місто»

№ п\п	Підхід	Автори	Визначення
1.	Техноцентричний та охоронний	Н. Медведенко, С. Медведенко (дослідники безпеки дорожнього руху та інфраструктури); І. Дрок (дослідник контролю за законодавством)	Програмно-технічний комплекс, що базується на хмарних технологіях та об'єднує системи відеоспостереження (з інтелектуальною відеоаналітикою), контролю трафіку, виявлення надзвичайних подій і комунікаційні мережі в єдиний системний інформаційний простір
2.	Соціально-урбаністичний (якість міського життя та середовище)	Співробітники економічного розвідувального підрозділу; дослідники урбаністики Айша Наджма Ікбал та Сану К. Теккат	Частина ширшої концепції «міста, зручного для життя» (livable city), де технології слугують інструментом для урядів та громад для зменшення рівня злочинності, зниження ризиків тероризму та забезпечення комфортного, здорового середовища.
3.	Багатовимірний (для кризового менеджменту)	Йозеф Ріствєй та Марош Лацінак (співробітники Університету у Жиліні, Словаччина)	Стан, коли всі ключові міські структури (поліція, рятувальні служби, органи влади та комунальні підприємства) взаємодіють для попередження загроз, прогнозування надзвичайних ситуацій та оперативного реагування.
4.	Правовий та просторово-гендерний (український контекст)	Г. Фесенко, Т. Фесенко (дослідники просторового розвитку міста Харкова за допомогою ГІС-технологій – сучасних комп'ютерних системи для збору, обробки, аналізу та візуалізації просторових даних і карток)	Інноваційна взаємодія поліції та громади (Community Policing), об'єднання міських програм задля оперативного реагування на надзвичайні події та забезпечення інклюзивного простору (наприклад, врахування гендерних аспектів безпеки, безбар'єрності, створення зручної інфраструктури).

Джерело: складено автором на основі проведених досліджень

Концепцію «Безпечне місто» та її зв'язок із цифровою трансформацією, міською безпекою й управлінням досліджували аналітичні центри, урбаністи та правознавці, зокрема фахівці аналітичного центру Cedos, аналітик Сергій Баглай, а також ті, хто долучився до таких ініціатив, як Kyiv Smart City [74].

Основні напрями досліджень концепції «Безпечне місто» стосуються питань урбаністика та соціальний контроль, а також локальні інфраструктурні рішення [225; 226]. Дослідники вивчають баланс між покращенням добробуту громадян, приватністю та посиленням присутності представників національної поліції [74]. Вони аналізують, як діяльність поліції впливає на життя людей, шукають межі допустимого втручання в особисте життя та оцінюють ефективність заходів безпеки для українських міст [104].

Науковці у сфері державного управління аналізують системи відеоспостереження, кібербезпеки та автоматизації моніторингу подій в правовому та публічному аспекті [93]. Аналогічні дослідження у безпековому аспекті здійснюють фахівці у галузях права та інформаційних технологій. Узагальнення цих праць дає автору підстави виокремити серед них представників сектору безпеки і науково-дослідних установ, які аналізують інтеграцію платформ і захист даних. Дослідження правових режимів забезпечення захисту критичної інфраструктури та аналіз стійкості систем кіберпростору здійснюють дослідники публічного управління, зокрема С. Демедюк [82].

На оперативно-розшукове та превентивне застосування відеоспостереження дійснюють вплив новітні технології, штучний інтелект та відеофіксація на запобігання правопорушенням у публічних місцях. Цей напрям вивчають Р. І. Благута та А. В. Мовчан.

Експерти аналітичних та громадських центрів (зокрема, Cedos, Українська Гельсінська спілка з прав людини) оцінюють ефективність цільових програм «Безпечне місто» у різних регіонах України (рис. 1.1). Вона безпосередньо залежить від рівня антикризового управління, наявності чітких індикаторів результативності та інтеграції громадян у бюджетний процес [251, с. 17, 21].

Рис. 1.1. Етапи проведення аналізу ефективності міської програми «Безпечне місто»

Джерело: складено автором на основі проведених досліджень

Оцінити ефективність міської програми «Безпечне місто» можна через порівняння витрачених коштів із реальними результатами: кількістю розкритих злочинів за допомогою камер, зменшенням рівня злочинності на вулицях, станом дорожнього руху та відгуками жителів українських міст (табл. 1.3) [251, с. 21].

Узагальнення проаналізованих джерел дає змогу автору виокремити кілька ключових чинників, які визначають успішність реалізації таких програм у регіонах: якість управлінських рішень, подолання формального підходу, баланс між відновленням і розвитком, громадський контроль і прозорість.

Найвищу ефективність демонструють програми, інтегровані в довгострокові Стратегії розвитку міст, а не розроблені як відокремлені документи. Поширеним недоліком у багатьох українських містах залишається відсутність вимірюваних індикаторів ефективності, через що моніторинг часто зводиться до оцінки простого освоєння бюджетних коштів, а не реальних якісних

змін для мешканців міст. Аналіз регіональних програм показує, що значна частина фінансування спрямовується на інфраструктурні об’єкти. На думку автора, що ґрунтується на сукупному аналізі регіональних програм, інвестиції у відновлення людського капіталу часто ігноруються або фінансуються за залишковим принципом, хоча саме проєкти, які проходять публічне обговорення із залученням інститутів громадянського суспільства, мають значно вищий рівень довіри та реальної результативності.

Рис. 1.2. Ключові критерії та їх показники щодо оцінки цільових програм «Безпечне місто»

Джерело: складено автором на основі проведених досліджень

У великих обласних центрах та столиці України міські цільові програми (наприклад, у сфері енергоефективності, ЖКГ чи підтримки підприємництва) мають системний характер і затверджуються на середньострокові періоди (наприклад, 2024–2028 або 2026–2028 роки). Проте, аудит таких програм часто виявляє прогалини у виконанні окремих соціальних заходів через дефіцит бюджетного покриття чи зміну пріоритетів в умовах воєнного стану.

Проєкти «Безпечне місто» – це комплексні системи міської безпеки, що об'єднують відеоспостереження, аналітику та комунікації. Вони створюють єдиний інформаційний простір для цілодобового моніторингу, оперативного реагування на надзвичайні ситуації, розшуку злочинців та управління інфраструктурою [174]. Як окрема категорія, проєкти «Безпечне місто» базуються на кількох фундаментальних складових:

- аналітика та відеоспостереження (встановлення смарт-камер розпізнавання облич, автомобільних номерів, фіксація швидкості);
- функціонування єдиного ситуаційного центру для збору, обробки та координації даних між представниками поліції, муніципальної варти та рятувальних служб;
- управління трафіком шляхом оптимізації дорожнього руху та автоматизованого виявлення ДТП;
- громадська безпека, а саме контроль за місцями масового скупчення громадян та комунікація з ними (наприклад, тривожні кнопки) [100].

Відеоспостереження та аналітика є основою концепції «Безпечне місто». Вони автоматизують моніторинг, допомагають швидко реагувати на загрози, розшукувати автомобілі та громадян за допомогою камер з вмонтованим штучним інтелектом та об'єднують велику кількість пристроїв в управлінські центри.

Управління трафіком та оптимізація дорожнього руху базуються на інтелектуальних транспортних системах, які використовують сенсори Інтернет речей, комп'ютерний зір та алгоритми глибокого навчання. Вони в реальному

часі регулюють функціонування світлофорів та забезпечують автоматизоване виявлення ДТП для оперативного реагування екстрених служб [99].

Оптимізація дорожнього руху в українських містах охоплює:

- адаптивні світлофори, які змінюють тривалість зеленого та червоного світла залежно від довжини черг та кількості автомобілів на перехресті;
- алгоритми прогнозують затори та перенаправляють транспортний потік для розвантаження міських доріг;
- збір даних за допомогою інструментів Інтернет речей. Сенсори та камери передають інформацію про швидкість та потік автомобілів до автоматизованої системи регулювання дорожнього руху в реальному часі.

В рамках концепції «Безпечне місто» автоматизоване виявлення ДТП здійснюються за таким алгоритмом:

1. Комп'ютерні камери спостереження сканують дорогу та миттєво фіксують зіткнення автомобілів чи падіння об'єктів.

2. Мережі відрізняють аварійну зупинку від реальної дорожньо-транспортної пригоди.

3. Система надсилає сигнал оповіщення до патрульної поліції та швидкої допомоги без дзвінка свідків.

Концепція «Безпечне місто» охоплює комплекс інноваційних цифрових та організаційних рішень, спрямованих на захист мешканців, запобігання правопорушенням та оперативного реагування на надзвичайні ситуації за допомогою централізованого моніторингу, відеоаналітики й координації дій екстрених служб.

Для українських міст системи «Безпечне місто» є критичним інструментом для зниження рівня злочинності та підвищення комфорту життя. Запровадження проєктів «Безпечне місто» вважається актуальним для підвищення рівня громадської безпеки, оперативного реагування на надзвичайні ситуації та оптимізації управління інфраструктурою. На думку автора, що ґрунтується на сукупному аналізі джерел, проєкти «Безпечне місто» дозволяють ефективніше

запобігати правопорушенням і швидко розкривати злочини завдяки сучасним технологіям моніторингу.

Проєкти «Безпечне місто» є базовим елементом концепції «Розумне місто» (Smart City), спрямованим на створення комфортного та захищеного середовища для мешканців українських міст [72; 117]. Проєкти «Безпечне місто» охоплюють комплексні системи відеоспостереження, аналітики та реагування [98; 190]. Вони необхідні для захисту громадян, оперативного розкриття злочинів, контролю дорожнього руху та координації екстрених служб. Це не тотальне стеження, а інструмент безпеки та швидкого реагування. Необхідність впровадження систем «Безпечне місто», в основному, обумовлюється виконанням таких завдань [75]:

- зниження рівня злочинності та вандалізму через наявність камер на вулицях, перехрестях та в громадських місцях.
- допомога представникам правоохоронних органів оперативно знаходити зловмисників, викрадені автомобілі або розшукувати зниклих людей.
- безпека дорожнього руху шляхом фіксації порушень ПДР (швидкість, проїзд на червоне світло) зменшує кількість аварій та дисциплінує водіїв.
- координація служб дозволяє диспетчерам, співробітникам поліції, швидкої допомоги та ДСНС відслідковувати ситуацію в реальному часі та миттєво реагувати на надзвичайні події;
- забезпечення цілодобового моніторингу критично важливих об’єктів (мостів, котелень, лікарень) охоронною інфраструктурою.

Категоріальна сутність проєктів «Безпечне місто» полягає у створенні єдиної інтегрованої системи, яка поєднує інноваційні технології, відеоаналітику та партнерство громади українських міст задля підвищення рівня безпеки, управління міською інфраструктурою та оперативного реагування на надзвичайні ситуації.

Людиноцентричність і партисипативність перетворюють систему «Безпечне місто» з технічного нагляду на функціонуючий простір спільної безпеки. Людиноцентричність передбачає те, що мешканець міста та його

комфорт знаходиться у центрі рішень. Партисипативність означає те, що громадяни самі беруть участь в управлінні, планують та контролюють безпеку в місті разом із міською владою.

Людиноцентричність у концепції «Безпечне місто» орієнтована на захист прав, доступніть та якість життя громадян українських міст. Забезпечується фокусування на безпеці людини, а не лише на збереженні майна чи інфраструктури міста. Здійснюється формування інклюзивного середовища для всіх груп населення, враховуючи маломобільні. Оцінка безпеки здійснюється через визначення рівня тривожності, довіри до співробітників національної поліції та комфорту на вулицях міст.

Партисипативність як залучення громадян до управління міста охоплює такі напрями:

- участь жителів міст в обговоренні розташування камер чи освітлення;
- локальні ініціативи для покращення безпеки районів міст;
- використання цифрових сервісів та додатків для швидкого реагування на проблеми та зв'язок з комунальними службами.

Перевага спільного підходу полягає у високій довірі громадян міст за рахунок кращого розуміння рішень влади, запропонованих ними. Залученість громадян міста до виявлення небезпеки раніше, ніж автоматизовані датчики. Стійкість міста означає його згуртованість та готовність до кризових обставин.

Основні напрями подальшого розвитку понять і категорій концепції «Безпечне місто»:

- Розширення меж безпеки. Перехід від фізичного правопорядку до комплексного захисту, що охоплює техногенну, екологічну, інформаційну та економічну безпеку жителів.
- Цифрова трансформація. Наповнення категорії «безпека» новими атрибутами на базі штучного інтелекту, інтернету речей, предиктивної аналітики та великих даних.

- Стійкість та адаптивність. Уведення категорій здатності міської системи прогнозувати, протистояти та швидко відновлюватися в умовах воєнного стану.

Людиноцентричність і парсипативність передбачає акцентування на відчутті захищеності громадян, залученні до управління ризиками через е-демократію та відкритість даних.

Розширення меж безпеки в концепції «Безпечне місто» означає перехід від базового поліцейського нагляду до комплексної життєстійкості урбанізованого середовища. Сучасний підхід охоплює захист від воєнних загроз, кібератак, техногенних аварій та природних стихій через об'єднання цифрових сенсорів, фізичних укриттів та аналітики даних у єдину систему [86, с. 69].

Напрями розширення меж захисту охоплюють фізичну інтеграцію стійких інженерних споруд та укриттів безпосередньо в міську інфраструктуру, захист баз даних критичних комунальних мереж від ворожих цифрових втручань та масове впровадження камер із розпізнаванням облич та аналітикою поведінки [86, с. 69; 94, с. 199].

Інструменти інтеграції стійких інженерних споруд та укриттів безпосередньо в міську інфраструктуру стосуються збору інформації з усіх міських датчиків в єдиному координаційному центрі, автоматичного виявлення загроз за допомогою штучного інтелекту та швидкого інформування жителів про небезпеку через цифрові та мобільні канали сповіщення.

Концепція «Безпечне місто» поєднує нові цифрові технології, штучний інтелект та міське управління. Вона перетворює звичайні послуги на розумні системи. Це допомагає швидко знаходити загрози, захищати жителів та контролювати порядок на вулицях за допомогою єдиної мережі датчиків і камер.

Стійкість та адаптивність у концепції «Безпечне місто» – це здатність міської цифрової та фізичної інфраструктури протистояти кризам, прогнозувати загрози, оперативно реагувати на надзвичайні ситуації та швидко відновлювати роботу критичних сервісів за допомогою інтегрованих платформ, відеоаналітики

та координації служб [86, с. 69–70]. Основні принципи стійкості в рамках концепції «Безпечне місто»:

- Кіберзахист серверів, мереж передачі даних та датчиків від цифрових атак для забезпечення безперервності процесів.
- Резервування та дублювання каналів зв'язку та баз даних на випадок відключення основного обладнання чи живлення.
- Безперервна робота муніципальних систем навіть у ході масштабних криз чи техногенних аварій.

Компоненти адаптивності системи «Безпечне місто» охоплює динамічний моніторинг та збір інформації про вуличний трафік, натовпи та стан комунікацій в реальному часі. Автоматизоване швидке перерозподілення ресурсів поліції, ДСНС та комунальних служб здійснюється залежно від поточних ризиків. Існує можливість додавати нові датчики, камери та аналітичні модулі без зупинки всієї системи [182].

Основними складовими впровадження систем «Безпечне місто» визначено:

- Відеоспостереження з аналітикою. Використання камер із функціями розпізнавання облич, номерних знаків та силуетів значно прискорює пошук зниклих осіб та правопорушників.
- Екстрене реагування. Координація дій поліції, рятувальників та медиків у режимі реального часу.
- Контроль трафіку та безпека дорожнього руху. Автоматизована фіксація порушень правил дорожнього руху (ПДР) та управління транспортними потоками для зменшення кількості заторів.
- Моніторинг стану міста, що допомагає вчасно реагувати на аварії, пошкодження інфраструктури, координування та управління діяльністю комунальних служб [182].

Розвиток категоріального базису концепції «Безпечне місто» спрямований на перехід від чисто техноцентричного підходу (відеоспостереження та охорони) до людиноцентричної парадигми, яка охоплює кібербезпеку, стійкість до криз,

екологічну безпеку, цифрову інклюзію та інтеграцію муніципальних даних у реальному часі.

Змістовні аспекти еволюції термінології передбачають синтез понять Smart City та «Безпечне місто» у єдиний комплексний контур функціонування урбанізованих систем [90; 200; 202]. Формування чітких критеріїв оцінки ефективності муніципальних цифрових платформ безпеки та стандартів захисту персональних даних.

Категоріальна сутність проєктів «Безпечне місто» полягає в тому, що вони є комплексними організаційно-правовими та програмно-технічними системами. Ці системи об'єднують відеоспостереження, аналітику даних та взаємодію громад із поліцією задля захисту мешканців, контролю трафіку та оперативного реагування на надзвичайні події в реальному часі.

1.2. Різновиди сучасних проєктів «Безпечне місто»

Проєкти «Безпечне місто» призначенні для захисту громадян, контролю правопорядку та управління інфраструктурою українських міст, використовуючи інструменти відеоспостереження, інтелектуальну аналітику та комунікаційні мережі в єдиному інформаційному просторі.

Сучасні проєкти «Безпечне місто» вважаються комплексні апаратно-програмні рішення з відеоспостереженням, відеоаналітикою та датчиками для контролю правопорядку, дорожнього руху та роботи комунальних служб. Вони класифікуються за функціоналом та призначенням, масштабом та архітектурою (табл. 1.3) [125].

Таблиця 1.3

Основні різновиди проєктів «Безпечне місто»

Класифікаційна ознака	Роз'яснення
За призначенням	
Транспортні та дорожні системи	Фокусуються на фіксації порушень ПДР, розпізнаванні автомобільних номерів, керуванні світлофорами та моніторингу трафіку
Громадська безпека та охорона правопорядку	Забезпечують відеонагляд у людних місцях, розпізнавання облич, оперативного реагування поліції через кнопки екстреного виклику
Екологічний та комунальний моніторинг	Виявленням стихійних сміттєзвалищ, контролем роботи комунальної техніки та пожежної безпеки
Інфраструктурна та цивільний захист	Інтегрують системи оповіщення населення, моніторинг критичної інфраструктури та укриттів
Архітектурні та масштабні рішення	
Локальні (об'єктні)	Охоплюють окремі житлові комплекси, підприємства чи навчальні заклади з локальним сервером
Міські та регіональні	Масштабні платформи, що об'єднують тисячі камер усього населеного пункту або області в єдиний аналітичний центр для поліції та ДСНС
Хмарні рішення	віддалений доступ до сервісів відеоспостереження без потреби купувати потужні власні сервери
За функціоналом	
Відеоспостереження та аналітика	Охоплює мережі IP-камер, що автоматично розпізнають обличчя, автомобільні номери, порушення правил дорожнього руху або залишені без нагляду предмети
Безпека дорожнього руху	Інтегровані системи автофіксації, які відстежують перевищення швидкості, проїзд на червоне світло та координують роботу «розумних» світлофорів
Оперативне реагування	Об'єднання в єдину мережу поліції, ДСНС та комунальних служб. Передбачає встановлення кнопок екстреного виклику «громадянин-поліція» у людних місцях
Моніторинг критичної інфраструктури	Захист об'єктів енергетики, водопостачання та транспортних вузлів із можливістю оперативного оповіщення населення

Джерело: складено автором на основі проведених досліджень

Наведена в табл. 1.3 класифікація проєктів «Безпечне місто» відображає передусім технічні та функціональні ознаки. Для цілей публічного управління її доцільно доповнити ознаками, що характеризують зміст безпеки, на яку спрямований проєкт «Безпечне міто». Розрізнення вимірів безпеки закріплене в Настановах системи ООН щодо безпечніших міст і населених пунктів, ухвалених 31 травня 2019 р. Асамблеєю ООН-Хабітат (вищим керівним органом Програми ООН з населених пунктів). Фактично воно відображає субєктивний ризик стати

жертвою правопорушення, що відображає сприйняття небезпеки крізь призму страху і тривоги [251, с. 9]. Відповідно, деякі проєкти спрямовані переважно на зменшення кількості правопорушень, інші – на відновлення відчуття захищеності, що і обумовлює використання різних показників результативності.

Відповідно до настанов системи ООН щодо безпечніших міст і населених пунктів міські стратегії безпеки поєднують три типи профілактики:

- соціальну, що охоплює цільові соціальні та освітні заходи для вразливих груп;
- ситуаційну, спрямовану на зменшення можливостей для вчинення правопорушень, зокрема через стандарти проєктування середовища;
- громадську, яка змінює умови життя в містах, опираючись на досвід їхніх мешканців [251, с. 19].

Більшість українських проєктів «Безпечне місто» характеризуються ситуаційною профілактикою. Настановами ООН найефективнішими визнаються підходи, що поєднують соціальні й технологічні заходи [251, с. 9–10]. Показово й те, що безпеку міста в документі визначено як «суспільне благо, що є результатом динамічної взаємодії чинників ризику та стійкості» і відмежовано від національної та публічної безпеки, що належать до функцій держави [251, с. 27].

Вітчизняні дослідники пропонують і структурну типологізацію. Т. Кадлубович і В. Дабіжа розглядають інформаційно-аналітичний комплекс «Безпечне місто» як систему взаємопов’язаних підсистем безпеки, автоматизації, координації та взаємодії, а також екологічної підсистеми [86, с. 67–68]. Спираючись на підхід Д. Сергенюка [109], автори виокремлюють три рівні архітектури системи безпеки: рівень моніторингу (камери відеоспостереження, комплекси екстреного зв’язку, інформаційні системи); рівень доставки, накопичення, зберігання та обробки інформації; рівень управління, аналізу та прийняття рішень, до якого належать ситуаційні центри, диспетчерські служби та локальні центри моніторингу [86, с. 68]. За цією моделлю проєкти різняться

тим, які рівні в них реалізовано: частина невеликих громад обмежується першим, повноцінні ситуаційні центри формують третій.

А. Некряч пропонує типологізацію за вимірами сталого розвитку: соціальним (зменшення злочинності, координація екстрених служб, безбар'єрність, що відповідають 11 і 16 цілям стралого розвитку), екологічним (моніторинг повітря, води, радіаційного фону, раннє виявлення пожеж і підтоплень, що визначено 3 і 13 Цілями сталого розвитку) та економічним (оптимізація бюджетних витрат через смарт-освітлення й облік енергоносіїв – 9 Ціль сталого розвитку) [95, с. 292]. Окремий різновид становлять спеціалізовані модулі «Безпечна школа» і «Безпечний двір», які разом утворюють «цілісний контур кримінологічного моніторингу» [95, с. 295].

Відеоаналітика – це технологія штучного інтелекту, яка перетворює звичайний відеонагляд на систему збору даних. Вона автоматично розпізнає обличчя, номери авто, залишені речі та порушення. Замість ручного перегляду, система миттєво сповіщає про тривогу та надає статистику.

Аналіз ринку рішень для інтелектуального відеоспостереження дає змогу автору дійти висновку, що вітчизняні розробники пропонують платформи, які інтегрують відеонагляд із системами контролю доступу, протипожежного захисту та кібербезпеки, що дає змогу автоматизувати процеси, оптимізувати витрати й оперативно реагувати на події в реальному часі.

Сучасні системи відеоспостереження виконують низку ключових завдань за допомогою інтелектуальних модулів:

- Розпізнавання осіб та ідентифікація номерних знаків транспортних засобів з бази даних.
- Виявлення або фіксація руху та вторгнень (сповіщення про перетин лінії, проникнення в охоронну зону або появу людини в заборонений час [93].

Використання інтелектуальних рішень дозволяє представникам поліції переходити від пасивного контролю до превентивної безпеки та оптимізації процесів [98].

Безпека дорожнього руху – це стан процесу руху, який відображає рівень захищеності його учасників від дорожньо-транспортних пригод (ДТП) та їхніх наслідків. Гарантування безпеки є спільною відповідальністю водіїв, пішоходів і пасажирів, а її правові основи в Україні регулюються Законом України «Про дорожній рух» [14].

Елементами інфраструктури безпеки є дорожні знаки та розмітка для швидкої орієнтації, світлофори та регулювальники для розподілу транспортних потоків, камери автофіксації порушень для контролю за дотриманням правил, освітлення та бар'єри для зменшення аварійності в темну пору доби та на перехрестях [14].

Система оперативного реагування та ситуаційні центри в Україні координуються через головний Ситуаційний центр Міністерства внутрішніх справ (МВС України), Службу порятунку 112 [26], а також Національну поліцію, що здійснює цілодобовий моніторинг ситуації Ситуаційний центр Національної поліції України. На рівні держави реагування та збір даних забезпечує Головний ситуаційний центр при РНБО.

Ситуаційний центр МВС України – це ключовий аналітичний підрозділ кризового менеджменту, який забезпечує безперервний збір, обробку та аналіз інформації про безпекову ситуацію в країні. Центр розташований у будівлі МВС України.

Інформацію про роботу Служби 112 МВС оприлюднює в окремому спецпроєкті: службу запроваджено в липні 2023 р. за принципом системи екстреної допомоги за єдиним номером, за 2,5 року її оператори опрацювали понад 10,5 млн викликів, а у 2025 р. МВС запустило мобільний застосунок «112 Ukraine» [175].

Національна поліція України – це центральний орган виконавчої влади, який забезпечує охорону прав і свобод людини, протидіє злочинності та підтримує публічну безпеку й порядок. Діяльність відомства координується Кабінетом Міністрів через Міністерство внутрішніх справ. Головним

нормативним документом, що регулює її роботу, є Закон України «Про Національну поліцію» [21].

Ситуаційний центр Національної поліції України є головним координаційним підрозділом, який цілодобово збирає, аналізує та опрацьовує інформацію про криміногенну ситуацію, правопорушення, воєнні загрози та надзвичайні події в усій країні. На основі отриманих даних центр формує оперативні зведення, моделює розвиток подій і допомагає керівництву приймати термінові управлінські рішення для захисту громадян українських міст [168]. Функціонування ситуаційного центру в кожному українському місті спрямоване на:

- цілодобовий моніторинг оперативної обстановки в реальному часі;
- накопичення інформаційних даних про рівень, структуру та динаміку злочинності в областях;
- аналітика та прогнозування: оцінка ризиків та моделювання ускладнення ситуації в країні;
- координація поліцейських підрозділів під час ліквідації кризових ситуацій;
- фіксації наслідків обстрілів, воєнних злочинів та взаємодії із силами оборони [113, с. 133–134].

На думку автора, що ґрунтується на аналізі нормативних актів і наукових праць, діяльність центру визначається Законом України «Про Національну поліцію» та відомчими нормативними актами, які встановлюють його завдання і порядок взаємодії з іншими службами [21]. Підрозділ тісно взаємодіє із Ситуаційним центром МВС України для швидкого обміну інформацією між різними службами, такими як Державна служба з надзвичайних ситуацій або Державна прикордонна служба України. Регіональні ситуаційні центри розгорнуті в усіх Головних управліннях Національної поліції в областях України. Основні завдання регіональних ситуаційних центрів полягають в:

- охороні прав, захисті свобод людини, інтересів суспільства та держави;
- протидії злочинності шляхом запобігання, виявлення та розкриття правопорушень.

- підтриманні порядку громадської безпеки на вулицях та в публічних місцях українських міст;
- надання допомоги особам, які опинилися в надзвичайних чи скрутних ситуаціях.

Відповідно до Закону України «Про Національну поліцію» до складу єдиної системи входять центральний апарат та територіальні органи. У структурі функціонують такі підрозділи: кримінальна поліція, патрульна поліція, органи досудового розслідування, поліція охорони, спеціальна поліція та поліція особливого призначення [21].

Головний ситуаційний центр України – це ключовий державний програмно-апаратний комплекс, який функціонує при Раді національної безпеки і оборони України (РНБО) і забезпечує збір, накопичення та аналіз інформації для ухвалення стратегічних рішень у сфері національної безпеки [33; 123]. Головний ситуаційний центр України створено відповідно до Указу Президента України від 28.02.2015 № 115/2015 [32]. Узагальнення джерел дає змогу автору стверджувати, що центр технічно оснащений для обробки великих масивів даних з державних і недержавних баз, а Державне космічне агентство України забезпечує його обробленою інформацією високої та надвисокої розрізненості з космічних платформ [159].

Головні завдання головного ситуаційного центру України полягають у:

- Безперервному моніторингу загроз: геополітичній, військовій, інформаційній та економічній ситуацій в країні.
- Оперативна аналітика, оцінювання та прогнозування рівня небезпеки з метою розробки сценаріїв локалізації криз.
- Забезпечення Президента та Секретаря Ради національної безпеки і оборони України верифікованими даними під час кризових ситуацій для прийняття відповідних рішень [123].

Головний ситуаційний центр інтегрує в єдину мережу ситуаційні центри України. До цієї системи також інтегровані: Урядовий ситуаційний центр, Центри сектору безпеки і оборони (наприклад, Ситуаційний центр Міністерства

оборони України), ситуаційні центри центральних органів влади та обласних державних адміністрацій та резервні та рухомі (мобільні) пункти управління [33]. Центр працює в цілодобовому штатному режимі під надійною охороною для гарантування стабільного управління державою у сфері оборони.

Єдиний ситуаційний центр – це інтегрована інформаційно-аналітична та командна платформа, створена для цілодобового моніторингу безпеки, оперативної обробки екстрених сповіщень та координації дій між Національною поліцією, Муніципальною вартою та Державною службою з надзвичайних ситуацій (ДСНС) [94, с. 199]. Такі центри ефективно функціонують у багатьох містах України. Наприклад, ефективну міжвідомчої співпраці демонструє Ситуаційний центр міста Вінниці, а також сучасні системи моніторингу в містах Київ, Львів, Дніпро та Ірпінь. На загальнодержавному рівні ця система тісно пов’язана з формуванням Єдиної служби екстреної допомоги 112 [26].

Основні функції ситуаційного центру в будь-якому місті України передбачають:

- Автоматичний збір інформаційних даних з камер відеоспостереження (включаючи системи розпізнавання облич і автомобільних номерів), датчиків моніторингу довкілля та звернень громадян на гарячі лінії [203].
- Використання штучного інтелекту та аналітичної обробки для виявлення правопорушень, ДТП, пожеж, підозрілих предметів або заторів у реальному часі.
- Миттєву координацію при одночасному сповіщенні та диспетчеризація екіпажів патрульної поліції, патрулів муніципальної варти та рятувальних підрозділів ДСНС на місце інциденту за допомогою єдиної цифрової радіомережі.

В рамках дисертаційного дослідження під центром обробки даних (дата-центром) автор розуміє спеціальну будівлю чи приміщення для безпечного зберігання, обробки та передачі великих обсягів інформації, у якому розміщують сервери та мережеве обладнання, підключені до швидкісних каналів зв’язку й забезпечені безперебійним живленням і охолодженням. До його основних

компонентів автор відносить серверні стійки, системи резервного живлення (акумулятори та генератори), прецизійні кондиціонери та захищені канали зв’язку.

Узагальнення технічних джерел дає змогу автору віднести до головних функцій центру обробки даних розміщення та зберігання баз даних, сайтів і хмарних сховищ, виконання складних обчислень за допомогою інструментів штучного інтелекту, забезпечення стабільної роботи та захист від збоїв чи зламу.

Аналізом систем відеоспостереження, кібербезпеки та автоматизованого моніторингу подій у правовому та публічному аспекті займаються профільні державні відомства (РНБО, Державна служба спеціального зв’язку та захисту інформації України [13], Департамент кіберполіції Національної поліції), науково-дослідні інститути системи МВС та Міністерства освіти та науки, а також незалежні громадські та аналітичні центри, що досліджують права людини і прозорість влади [94, с. 198].

Рада національної безпеки і оборони України (РНБО) координує стратегічний аналіз стану кібербезпеки та захисту критичної інфраструктури на державному рівні. Державна служба спеціального зв’язку та захисту інформації України здійснює технічний та регуляторний аналіз інцидентів, розробляє стандарти кіберзахисту [23; 94, с. 198].

Моніторинг критичної інфраструктури – це система постійного контролю за станом таких стратегічних об’єктів, як енергетика, транспорт, зв’язок та комунальне господарство. В Україні він регламентується Законом «Про критичну інфраструктуру» та має на меті оцінку захищеності, запобігання аваріям та забезпечення стійкості [18].

Державний нагляд і контроль критичної інфраструктури охоплює такі основні напрями:

- Законодавча відповідність. Секторальні органи кожні 3 роки проводять планові оцінки стану безпеки та контролюють достовірність існуючих даних.

- Контроль за спорудженням захисних інженерних конструкцій, фізичним станом обладнання та охороною територій.
- Кібербезпека. Постійний моніторинг інформаційно-комунікаційних систем, що захищають роботу ключових галузей, для недопущення втручань [23].

Співробітники Державної служби спеціального зв'язку та захисту інформації України здійснюють реєстр об'єктів критичної інфраструктури та координує дії для мінімізації наслідків надзвичайних ситуацій. Також сучасні підходи часто охоплюють високоточний супутниковий моніторинг для раннього виявлення змін та контролю території України [18; 159].

Введення військового стану при звело до виокремлення ще одного різновиду функціонального призначення проєктів «Безпечне місто» – оборонного або подвійного використання. К. Споришев і О. Бондаренко пов'язують обороноздатний потенціал проєкту з трьома функціями: оптимізації ситуаційної обізнаності органів військового управління та правоохоронних органів щодо обстановки в тилу; превентивної сек'юритизації тилу через створення цифрового «щита», який ускладнює функціонування агентурних мереж противника і диверсійно-розвідувальних груп; інфраструктурної стійкості, тобто фіксації й оперативного оцінювання наслідків уражень об'єктів критичної інфраструктури для координації сил цивільного захисту [113, с. 133]. За висновком авторів, в умовах воєнного стану проєкт «Безпечне місто» трансформується з локального інструменту громадського порядку та міського врядування у стратегічний ресурс сектору безпеки й оборони [113, с. 134].

А. Некряч, аналізуючи проєкт крізь призму трирівневої концепції безпеки Б. Бузана [208], показує, що він діє на рівні індивіда, де поряд із захистом виникають ризики для приватності, на рівні держави і на рівні міжнародної системи, зокрема через взаємодію з базами даних Інтерполу (Міжнародної організації кримінальної поліції) та безпекових структур ЄС [94, с. 199–200]. Принципово важливо, що в умовах воєнного стану система «не замінює собою військові засоби оборони, а виконує допоміжну (інфраструктурно-

інформаційну) функцію» [94, с. 199]. А. Некряч також пропонує розрізняти режими функціонування публічного адміністрування – мирного часу, підвищеної готовності, надзвичайного та воєнного станів [94, с. 198]. А. Некряч також фіксує етапи становлення таких проєктів в Україні. Перший етап стосується їх використання як інструменту публічного управління розпочалося до 2014 р. Другий етап припадає на схвалення Концепції першочергових заходів реформування системи МВС 22 жовтня 2014 року [36], яким задекларовано застосування сучасних автоматизованих і телекомунікаційних систем. Системне впровадження проєктів «Безпечне місто» відбулося в 2015–2016 рр. на основі рішень міських рад. З 2024 р. розпочалося об'єднання міських проєктів відеоспостереження та аналітики в єдину державну систему [94, с. 198–199]. З огляду на це Т. Кадлубович і В. Дабіжа пропонують розглядати вкладення в системи «Безпечне місто» як «інвестиції подвійного призначення, що одночасно відповідають на актуальні воєнні виклики» і водночас створюють технологічний фундамент для повоєнного розвитку [86, с. 69].

Отже, класифікація, наведену в табл. 1.4, має враховувати три ознаки: вимір безпеки (фактична або суб'єктивна), тип профілактики (ситуаційна, соціальна, громадська) і режим функціонування (мирний час, підвищена готовність, надзвичайний або воєнний стан). Від них залежать склад даних, які збирає система, коло їх користувачів і електронні запобіжні пристрої для захисту прав мешканців українських міст.

Сучасні проєкти «Безпечне місто» – це комплексні апаратно-програмні рішення з відеоспостереженням, відеоаналітикою та датчиками для контролю правопорядку, дорожнього руху та роботи комунальних служб. Вони класифікуються за функціоналом, масштабом та архітектурою.

Проєкти «Безпечне місто» еволюціонують від простих систем локального відеонагляду до інтелектуальних екосистем міської безпеки. На думку автора, що ґрунтується на сукупному аналізі джерел, головними напрямами їх розвитку є впровадження штучного інтелекту й аналітики даних, інтеграція з державними цифровими сервісами, розширення транспортної тематики та перехід до

концепції стійкості перед новими викликами. Ключові напрями розвитку проєктів «Безпечне місто» базуються на таких інструментах:

- Штучний інтелект та аналітика. Використання комп'ютерного зору для розпізнавання облич, детекції залишених предметів, аналізу скупчень людей та прогнозування надзвичайних ситуацій.
- Цифрова інтеграція. Об'єднання локальних платформ із державними сервісами (зокрема інтеграція з додатком Дія та загальнонаціональними базами даних).
- Ефективний трафік та мобільність. Автоматизований контроль за допомогою інтелектуальних систем фіксації порушень Правил дорожнього руху, аналіз транспортних потоків та управління громадським транспортом в українських містах [84].

Проєкти «Безпечне місто» використовують штучний інтелект та інтелектуальну відеоаналітику для автоматичної обробки даних з тисяч камер, розпізнавання облич, ідентифікації автомобільних номерів, аналізу транспортних потоків та оперативного реагування на надзвичайні події в реальному часі [122]. Датчики інфраструктурного контролю здійснюють моніторинг за станом комунальних мереж та роботою міських служб. Досягнення енергонезалежності реалізується переходом обладнання на автономні джерела живлення, захист дата-центрів та каналів зв'язку від кібератак і радіоелектронного впливу.

1.3. Методичні основи запровадження системи «Безпечне місто»

Методичні основи запровадження системи «Безпечне місто» базуються на створенні єдиного інформаційного простору. На думку автора, що ґрунтується на сукупному аналізі джерел, цей комплекс об'єднує відеофіксацію, аналітику трафіку та координацію служб (національної поліції, ДСНС, комунальників) через програмно-апаратні засоби, спираючись на місцеві програми розвитку, законодавство про захист інформації та аналіз ризиків будь-якого українського міста (рис. 1.3).

Методичні основи системи «Безпечне місто» необхідні для створення єдиного, захищеного та стандартизованого середовища. Вони запобігають хаотичному встановленню камер, забезпечують сумісність технологій та ефективне управління безпекою будь-якого українського міста [251, с. 13; 182].

Міжнародні настанови ООН-Хабітат (Програми ООН з населених пунктів) розглядають запровадження таких систем як процес, що ґрунтується на знаннях і починається з діагностики. Настанови системи ООН щодо безпечніших міст і населених пунктів передбачають, що предстаники місцевої влади у співпраці з національними органами складає карту відповідних суб'єктів і ресурсів міста, періодично оцінюючи ефективність програмної політики і збирає дані для регулярної загальноміської оцінки безпеки [251, с. 16]. Такі оцінювання мають спиратися на дезагреговані за територією, статтю та віком дані поліції й закладів охорони здоров'я, геоприв'язаний аналіз злочинності на рівні найменшої адміністративної одиниці, якісні дані про сприйняття безпеки мешканцями та відповідальне використання нових технологій. Завершальним етапом є визначення системи моніторингу та переліку показників [251, с. 16–17]. Для реалізації рішень рекомендовано створювати міськукоординаційну раду з питань проєкту «Безпечне місто», здатну оцінювати людський, територіальний і технологічний виміри безпеки [251, с. 18].

Кодекс практики щодо камер спостереження, чинний в Англії та Уельсі (редакція 2021 р.), визнає застосування відкритих систем відеоспостереження в публічних місцях виправданим, якщо воно переслідує законну мету, є необхідним для задоволення нагальної потреби, пропорційним, ефективним і відповідає правовим зобов'язанням [245, с. 6]. Потенційно втручальною у кодексі практики щодо камер спостереження не саму технологію, а спосіб її використання, тому рішення про розгортання має бути задокументоване, а технічне рішення – «пропорційним заявленій меті, а не визначатися наявністю фінансування чи технологічними новаціями» [245, с. 6]. На думку автора, для українських громад ця вимога має особливе методичне значення: спершу

визначаються проблема, мета та показники результативності, і лише потім – технічний склад системи.

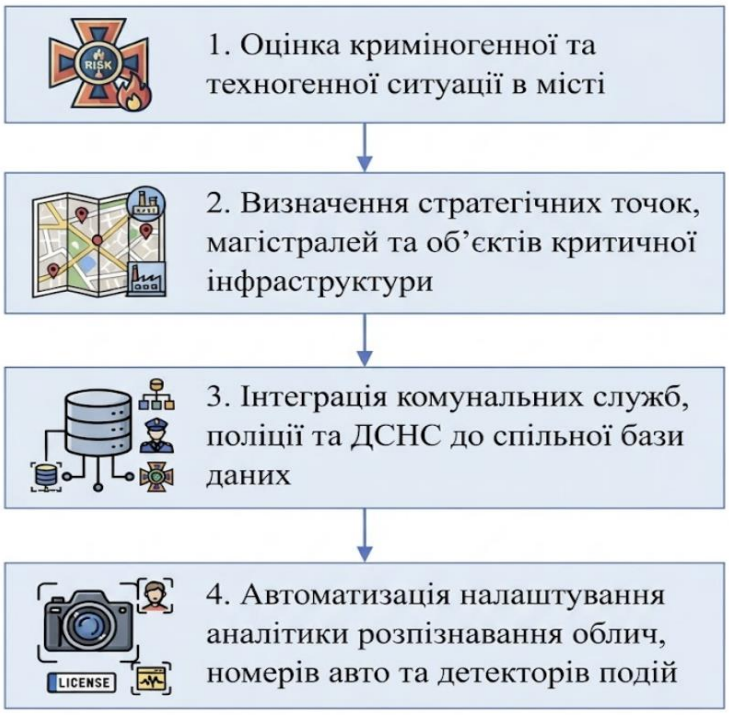

Рис. 1.3. Методичні етапи проєктування та впровадження апаратно-програмного комплексу «Безпечне місто»

Джерело: складено автором на основі проведених досліджень [103]

Запровадження апаратно-програмного комплексу «Безпечне місто» базується на принципах системності, комплексності, законності та централізованого управління, об'єднуючи відеоспостереження, аналітику трафіку та координацію екстрених служб задля безпеки будь-якого українського міста [251, с. 11–13]. Основні принципи побудови апаратно-програмного комплексу «Безпечне місто» охоплюють:

- розгляд міського середовища як єдиного системного об'єкта захисту з взаємопов'язаними підсистемами;
- комплексне поєднання технічних засобів (камер, датчиків, серверів) та організаційних заходів;
- збір та обробка даних в єдиному централізованому Ситуаційному центрі для швидкого реагування.
- діяльність у межах законодавства з дотриманням прав на приватність та захист інформації;

- масштабування, яке передбачає можливість поступового додавання нових камер, модулів штучного інтелекту та сервісів [182].

Пріоритетні завдання методичних основ запровадження системи «Безпечне місто» (табл. 1.4) охоплюють створення єдиного інформаційного середовища, розгортання мережі інтелектуального відеоспостереження, інтеграцію комунікаційних каналів, забезпечення кіберзахисту даних та організацію взаємодії між органами місцевого самоврядування і правоохоронними структурами [251, с. 16–18].

Таблиця 1.4

Завдання при формулюванні методичних основ запровадження системи «Безпечне місто»

№п\п	Напрями завдань	Сутність
1.	Архітектура та інфраструктура	• Визначення єдиних технічних стандартів для обладнання (камер, серверів, сенсорів). • Проєктування захищених волоконно-оптичних ліній зв'язку. • Створення централізованих пунктів збору, обробки та зберігання даних (ЦОД). • Проектування єдиної мережі «Безпечне місто» відеоспостереження та сенсорів [182]. • Забезпечення зв'язку із диспетчерськими центрами.
2.	Аналітика та інтеграція	• Впровадження модулів розпізнавання автомобільних номерів, облич та аналізу поведінки. • Інтеграція наявних підсистем (транспортних мереж, ЖКГ, систем оповіщення) у єдиний комплекс. • Автоматизація реагування на надзвичайні події в режимі реального часу.
3.	Організаційно-правові засади	• Розробка регламентів доступу до відеоархівів та персональних даних для служб. • Нормативно-правове закріплення повноважень суб'єктів управління системою. • Забезпечення фінансового планування та поетапного моніторингу реалізації програми.
4.	Аналіз та оцінка	• Визначити поточні безпекові загрози, ризики та потреби міської інфраструктури. • Дослідити наявний ресурс комунікацій і технічних мереж.

Джерело: складено автором на основі проведених досліджень

Формулювання методичних основ запровадження системи «Безпечне місто» передбачає визначення концептуальних підходів, нормативно-правової

бази, архітектури та алгоритмів взаємодії комунальних і правоохоронних служб задля гарантування публічної безпеки. Основні цілі: запровадження методичних основ системи «Безпечне місто» зводяться до запобігання фрагментації, захисту даних та кібербезпека.

Запобігання фрагментації вимагає комплексу дій для оптимізації зберігання даних або пам'яті, що передбачає регулярну дефрагментацію жорстких дисків, виділення однакових блоків пам'яті в програмуванні та уникнення надмірного розбиття файлів. Це забезпечує швидкий доступ до інформації та запобігає збоям системи. Об'єднання розрізнених камер і датчиків у єдину аналітичну мережу для миттєвого реагування співробітників поліції та ДСНС.

Кібербезпека та захист даних потребує формування комплексу процесів, технологій і практик, спрямованих на захист комп'ютерних систем, мереж, програм та інформації від цифрових атак, несанкціонованого доступу, крадіжки або пошкодження. У сучасному цифровому світі забезпечення конфіденційності, цілісності та доступності даних є критично важливим як для окремих користувачів, так і для державних чи комерційних організацій. Встановлення жорстких правил доступу до персональних даних громадян та алгоритмів запобігання витокам інформації Стандартизація обладнання передбачає визначення чітких вимог до роздільної здатності, функцій (розпізнавання облич, автомобільних номерів) та надійності техніки.

Стандартизація обладнання означає процес встановлення єдиних технічних норм, параметрів і вимог до матеріалів, машин та систем. Вона забезпечує взаємозамінність деталей, полегшує обслуговування та гарантує, що пристрої від різних виробників працюватимуть спільно [28; 114, с. 12]. Основні переваги стандартизації обладнання, задіяного в проєках «Безпечне місто»:

- уніфіковані вузли та деталі дозволяють швидко замінити зламану частину, не купуючи весь новий механізм;
- серійне виробництво стандартизованих елементів зменшує собівартість виготовлення та ремонту;

- масштабування спрощує процеси розширення бізнесу, відкриття нових філій або складів завдяки ідентичним вимогам до інфраструктури;
- фіксовані технічні регламенти гарантуючи, що продукція відповідає нормам безпеки та якості [114, с. 13].

До методів стандартизації відноситься уніфікація (зменшення кількості різновидів деталей до оптимального мінімуму), агрегатування (створення складного обладнання з готових стандартних універсальних блоків та вузлів і розробка типових технологічних процесів та конструкцій для однотипних видів обладнання) [114, с. 15–16].

Юридичні основи стандартизації в Україні регулюються профільним Законом України «Про стандартизацію» [28], який визначає об'єкти та процедури оцінки відповідності. Також велика увага приділяється міжнародній гармонізації, а саме впровадженню вимог ISO Міжнародної організації зі стандартизації, що дозволить здійснювати експорт обладнання.

Основні цифрові загрози для безпеки даних постійно змінюються, набуваючи нових форм:

- фішинг (листи або повідомлення, що маскуються під надійні джерела для викрадення паролів та платіжних даних).
- програми-вимагачі шифрують файли на пристрої та вимагає викуп за відновлення доступу.
- шкідливе програмне забезпечення (віруси, трояни та шпигунські програми, які непомітно пошкоджують систему або збирають інформацію);
- маніпулювання з метою примушення добровільно розкрити конфіденційні дані [80].
- Захист інформації є основою функціонування концерції «Безпечне місто». Для цього необхідно забезпечувати:
- обмеження та контроль прав доступу користувачів за принципом найменших привілеїв;
- шифрування даних під час зберігання та передачі інформації по мережі;

- регулярний інструктаж персоналу щодо виявлення фішингу та інших кібератак;
- суворе дотримання законодавчих вимог захисту персональних даних відповідно до національного законодавства та міжнародних стандартів, таких як GDPR (Загальний регламент про захист даних – це головний закон Європейського Союзу про захист приватних даних, що діє з 2018 року) [67; 213].

Впровадження системи «Безпечне місто» базується на державно-муніципальному партнерстві. Воно передбачає створення єдиного інформаційного простору, який об'єднує відеоспостереження, аналітику трафіку та координацію служб. Мета впровадження системи «Безпечне місто» полягає у профілактиці правопорушень та оперативному реагуванні на надзвичайні ситуації [94, с. 199; 100]. Методологічні та організаційні засади реалізації проєктів «Безпечне місто» охоплюють кілька основних напрямів, представлених в рис. 1.4.

Рис. 1.4. Методологічні засади реалізації проєктів «Безпечне місто»

Джерело: складено автором на основі проведених досліджень

Центри безпеки в містах – це об’єкти інфраструктури, що об’єднують пожежно-рятувальні підрозділи (ДСНС або місцеву пожежну охорону), поліцейські станції та пункти екстреної медичної допомоги. В основному, їх призначення полягає у скороченні часу прибуття на виклик і наближення публічних послуг до мешканців. Основні рекомендації щодо створення Центру безпеки в будь-якому українському місті передбачають:

1. Аналіз території та ризиків. Визначення оптимального розташування, радіус обслуговування (зазвичай до 20 км), чисельність населення та кількість об’єктів підвищеної небезпеки.

2. Архітектурні вимоги до приміщень для чергової зміни, гаража для спецтехніки (пожежні автомобілі, поліцейські авто), диспетчерського пункту, тренувальної бази та побутових кімнат.

3. Комплектація служб. Організація постійної або мобільної присутності пожежників-рятувальників, поліцейських офіцерів громади та фельдшерів.

4. Матеріально-технічне забезпечення. Закупівля спеціалізованого обладнання, засобів зв’язку та транспорту.

Для практичної реалізації цих вимог Кодекс практики щодо камер спостереження встановлює такі основні принципи:

- визначена мета;
- урахування впливу на приватність із регулярним переглядом;
- прозорість і контакти для скарг;
- чітка відповідальність;
- правила і процедури до початку роботи;
- зберігання лише потрібних даних і їх видалення після досягнення мети;
- обмежений доступ; дотримання стандартів;
- захист від несанкціонованого доступу;
- перегляд і аудит з оприлюдненням звітів;
- отримання зображень доказового значення;
- точність довідкових баз даних [245, с. 9].

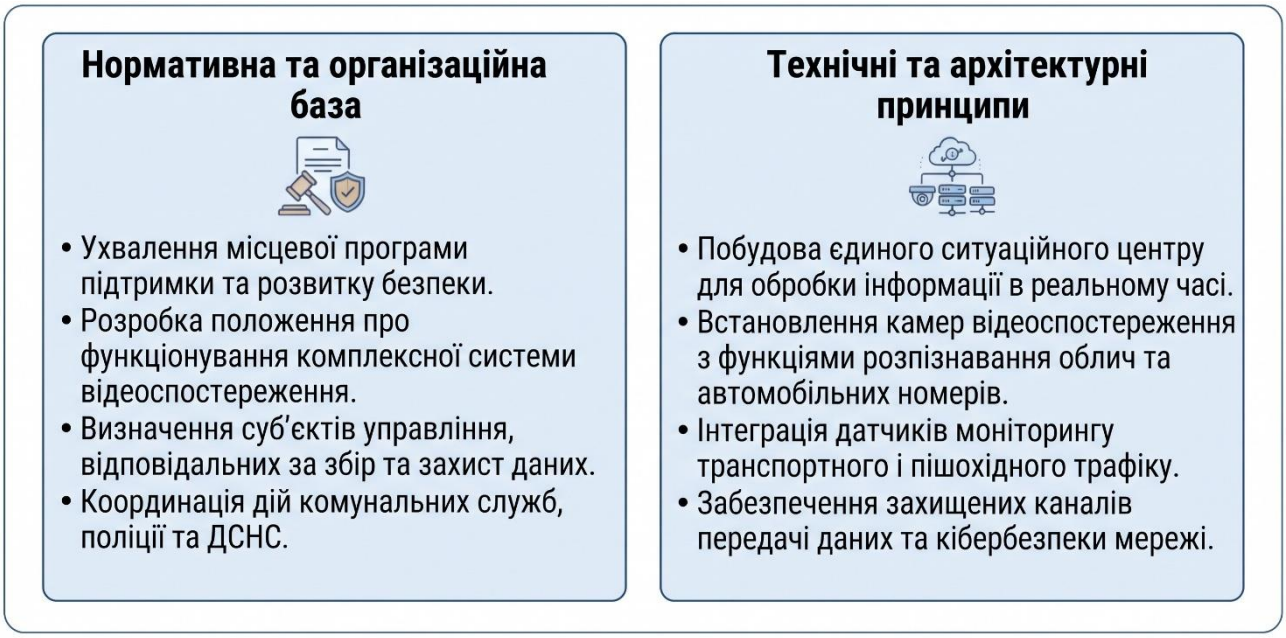

Рис. 1.5. Методичні рекомендації щодо запровадження систем «Безпечне місто» відповідно до основних напрямів

Джерело: складено автором на основі проведених досліджень

Окремо Кодекс вимагає проводити оцінку впливу на захист даних щоразу, коли розглядається створення або перегляд системи, а застосування розпізнавання облич – чітко обґрунтовувати, перевіряти та передбачати втручання людини до ухвалення рішень, що негативно впливають на особу [245, с. 11].

Настанови ООН-Хабітат (Програми ООН з населених пунктів) доповнюють ці вимоги на рівні нормативного регулювання: місцеві акти мають належно врегульовувати використання технологій, що порушують право на приватність, зокрема доступ до персональних даних, строки їх зберігання, засоби правового захисту та алгоритмічну прозорість, а також передбачати звітування про витрати на безпеку в розрахунку на одного мешканця й післязаконодавчий контроль [251, с. 21]. А. Некряч застерігає, що без належного правового регулювання інтелектуального відеоспостереження цифровий захист особи може перетворитися на інструмент несанкціонованого втручання в її приватне життя [94, с. 199].

На думку автора, масштабування систем відеоаналітики потребує електронних запобіжних принципів, передбачених принципами Кодексу

практики щодо спостереження: визначеної мети, оцінки впливу на приватність, обмеження доступу та незалежного аудиту. Узагальнені методичні вимоги до запровадження систем «Безпечне місто» за етапами наведено в табл. 1.5.

Таблиця 1.5

Методичні вимоги до запровадження систем «Безпечне місто» за етапами

Етап	Методична вимога	Завдання для міста
Діагностика	Регулярне загальноміське оцінювання безпеки за даними поліції, закладів охорони здоров'я та опитувань мешканців [251, с. 16–17]	Аудит безпеки міста до закупівлі обладнання
Обґрунтування мети	Законна мета, нагальна потреба, пропорційність, ефективність [245, с. 6, 9]	Мета, завдання й показники в цільовій програмі
Оцінка впливу	Оцінка впливу на захист даних; консультації з мешканцями [245, с. 11]	Публічне обговорення до розгортання системи
Правила функціонування	Правила до початку роботи; обмежений доступ; строки зберігання за метою [245, с. 9, 14]	Регламент доступу, зберігання та розкриття даних
Прозорість і підзвітність	Оприлюднення процедур, оцінок впливу, статистики роботи та скарг [245, с. 12]	Щорічний публічний звіт, контакти для звернень
Оцінювання	Щорічний перегляд; порівняння з менш втручальними альтернативами; витрати на утримання [245, с. 16–17]	Оцінювання за показниками, перегляд розміщення камер
Фінансування	Муніципальне фінансування, бюджет участі, партнерство з бізнесом, аналіз витрат і вигод [251, с. 21]	Обґрунтування бюджету з урахуванням утримання

Джерело: складено автором на основі [251; 245]

Методичні основи запровадження системи «Безпечне місто» базуються на створенні єдиного інформаційного простору. Вони включають нормативно-правове регулювання безпеки в українських містах, розробку комплексних міських програм, інтеграцію аналітичних та апаратних рішень відеофіксації, а також взаємодію органів місцевого самоврядування з правоохоронними структурами.

Рис. 1.6. Етапи впровадження методичних основ запровадження системи «Безпечне місто»

Джерело: складено автором на основі проведених досліджень

Подальші напрями розвитку методичних основ запровадження системи «Безпечне місто» охоплюють:

- Інтеграцію з цифровими системами, а саме об'єднання можливостей платформи «Дія» з міськими базами даних для ідентифікації та оперативного реагування.
- Запровадження нових методів транспортної аналітики, а саме обробки даних про трафік, інтеграцію з системою електронного квитка та контролю пасажиропотоків.
- Удосконалення відеонагляду: розширення мережі камер із функцією розпізнавання облич, номерів автомобілів та автоматичної фіксації порушень.
- Розробку спільних методичних алгоритмів взаємодії поліції, рятувальників та комунальників у реальному часі.
- Захист інформації, а саме вдосконалення стандартів кібербезпеки та збереження персональних даних під час обробки відеопотоків.

Отже, основні напрями розвитку методичних основ системи «Безпечне місто» охоплюють інтеграцію з державними цифровими платформами (зокрема «Дія»), впровадження систем електронного квитка та транспортного аналізу, посилення відеомоніторингу й автоматичної фіксації правопорушень, а також удосконалення координації комунальних служб, поліції та ДСНС.

Окремим методичним завданням є оцінювання результативності. Систематичний огляд і метааналіз досліджень, виконаний Е. Пізою, Б. Велшем, Д. Фаррінгтоном і А. Томас, засвідчив, що відеоспостереження пов’язане зі значущим, але помірним зниженням злочинності; найбільший і найстабільніший ефект спостерігався на автостоянках, значущий – у житлових районах, а системи з активним моніторингом і ті, що поєднувалися з іншими заходами, давали більший ефект [235]. Автори рекомендують спрямовувати відеоспостереження насамперед на запобігання злочинам, пов’язаним із транспортними засобами, і майновим злочинам та не застосовувати його як самостійний засіб профілактики [235].

К. Споришев і О. Бондаренко вважають завданням публічного управління обґрунтування показників – «індексів та індикаторів, які підлягають врахуванню під час комплексного моніторингу» руху українських міст до сталого розвитку [113, с. 134]. Настанови ООН-Хабітат (Програми ООН з населених пунктів) вимагають систематично оцінювати, наскільки дії зменшують незахищеність і кількість злочинів, та проводити коротко- і довгострокове оцінювання профілактичних політик [251, с. 18], а Кодекс практики щодо камер спостереження щороку переглядають необхідність, пропорційність і ефективність системи, порівнювати її з менш втручальними альтернативами та оцінювати майбутні витрати на утримання, персонал і ремонт [245, с. 16–17]. На думку автора, методичні основи запровадження систем «Безпечне місто» в Україні мають містити обов’язковий цикл оцінювання: визначення базових значень показників до запуску системи, щорічний моніторинг і незалежне оцінювання результатів із публічним звітом.

Висновки до розділу 1.

У першому розділі дисертаційного дослідження визначено Категоріальна сутність поняття проєкт «Безпечне місто», досліджено різновиди сучасних проєктів «Безпечне місто» та проаналізовано основи запровадження системи «Безпечне місто».

Під час дослідження наукових інформаційних джерел виявлено, що категоріальна сутність проєктів «Безпечне місто» полягає в тому, що вони є комплексними організаційно-правовими та програмно-технічними системами. Ці системи об'єднують відеоспостереження, аналітику даних та взаємодію громад із поліцією задля захисту мешканців, контролю трафіку та оперативного реагування на надзвичайні події в реальному часі.

Введення військового стану докорінно змінило порядок реалізації проєктів «Безпечне місто», змістивши фокус із загальної протидії злочинності на оперативні завдання національної безпеки та оборони. Раніше такі програми координувалися переважно органами місцевого самоврядування, але тепер їхнє впровадження регулюється у тісній взаємодії з військовими адміністраціями, Силами оборони та правоохоронними органами. Головні зміни у функціонуванні та реалізації проєктів охоплюють зміну пріоритетів моніторингу, кібербезпеку, інтеграцію інтелектуальних функцій та питання фінансування.

Замість фіксації переважно дрібних правопорушень та контролю дорожнього руху, системи відеоспостереження тепер критично важливі для відстеження пересування ворожої техніки, диверсійно-розвідувальних груп, коригувальників вогню, а також для контролю за дотриманням комендантської години. Посилилися вимоги до захисту каналів зв'язку та збереження даних. Доступ до інтегрованих платформ «Безпечне місто» суворо обмежено – повний контроль мають співробітники СБУ, Національної поліції та військові. Закриваються будь-які публічні трансляції з міських камер, щоб ворог не міг оцінювати наслідки ракетних чи дронових ударів.

Адміністрація українських міст активно закуповує камери з розпізнаванням облич, автомобільних номерів, а також оптику з тепловізійним

нічним баченням та модулями аналітики штучного інтелекту, що допомагає виявляти підозрілу активність у реальному часі.

Попри бюджетні обмеження, продовжується виділення значних коштів на ці системи (наприклад, масштабне розширення мереж камер у Житомирі, Одесі чи запуск нових проєктів у Миколаєві). Це обумовлено тим, що «Безпечне місто» стало частиною оборонного контуру регіонів.

Здійснено аналіз взаємопов'язаність підходів до визначення категорії проєктів «Безпечне місто». Проаналізовано взаємозалежність техноцентричного та охоронного. соціально-урбаністичного, багатовимірного, правового та просторово-гендерного підходів до визначення категорії проєктів «Безпечне місто». Їх об'єднують технології, міська інфраструктура та суспільна взаємодія задля безпеки громадян українських міст.

Досліджено низку наукових праць вітчизняних та зарубіжних науковців щодо питань запровадження проєктів «Безпечне місто». Аналіз наукових праць вітчизняних та зарубіжних вчених свідчить, що оперативно-розшукове та превентивне застосування відеоспостереження здійснюють вплив новітні технології, штучний інтелект та відеофіксація на запобігання правопорушенням у публічних місцях.

Проаналізовано, що проєкти «Безпечне місто» створюють єдиний інформаційний простір для цілодобового моніторингу, оперативного реагування на надзвичайні ситуації, розшуку злочинців та управління інфраструктурою

Визначено, етапи проведення аналізу ефективності міської програми «Безпечне місто», які охоплюють комплексний процес, який дозволяє оцінити раціональність використання бюджетних коштів, рівень зниження злочинності та реальне підвищення безпеки мешканців. Оцінити ефективність міської програми «Безпечне місто» можна через порівняння витрачених коштів із реальними результатами: кількістю розкритих злочинів за допомогою камер, зменшенням рівня злочинності на вулицях, станом дорожнього руху та відгуками жителів українських міст.

Особлива увага приділяється різновидам проєктів «Безпечне місто». Системи відеомоніторингу та аналітики фокусуються на розгортанні мереж камер відеоспостереження у публічних місцях. Вони використовують інтелектуальну аналітику: розпізнавання облич, детекцію залишених предметів та фіксацію скупчень людей.

Безпека дорожнього руху спрямована на контроль ситуації на дорогах. Включають автоматичну фіксацію порушень ПДР (швидкість, проїзд на червоне світло), розпізнавання автомобільних номерів (ANPR) та моніторинг трафіку для оптимізації роботи світлофорів.

Екологічний та техногенний моніторинг інтегрує датчики контролю якості повітря, радіаційного фону, рівня води у водоймах та виявлення хімічних загроз для запобігання надзвичайним ситуаціям.

Інформаційно-комунікаційні системи екстреної допомоги забезпечують координацію між різними службами (поліція, ДСНС, швидка допомога). Сюди входить розгортання єдиних диспетчерських центрів (аналогів системи 112) та встановлення тривожних кнопок «Громадянин-поліція» на вулицях міста.

Єдиний ситуаційний центр об’єднує всі вищезгадані підсистеми в одну цифрову систему. Він дозволяє операторам бачити повну картину життєдіяльності міста в реальному часі та координувати протидію кризовим ситуаціям.

Обґрунтовано доцільність доповнення класифікації проєктів «Безпечне місто» трьома ознаками: виміром безпеки (фактична або суб’єктивна), типом профілактики (ситуаційна, соціальна, громадська) і режимом функціонування (мирний час, підвищена готовність, надзвичайний або воєнний стан). Виокремлено оборонний різновид проєктів подвійного використання, що забезпечує ситуаційну обізнаність, превентивну сек’юритизацію тилу та інфраструктурну стійкість, виконуючи щодо сил оборони допоміжну інфраструктурно-інформаційну функцію.

Проаналізовано, що методичні основи системи «Безпечне місто» необхідні для створення єдиного, захищеного та стандартизованого середовища. Вони

запобігають хаотичному встановленню камер, забезпечують сумісність технологій та ефективне управління безпекою будь-якого українського міста

Доведено, що запровадження апаратно-програмного комплексу «Безпечне місто» базується на принципах системності, комплексності, законності та централізованого управління, об'єднуючи відеоспостереження, аналітику трафіку та координацію екстрених служб задля безпеки будь-якого українського міста.

Сформовано методичні вимоги до запровадження систем «Безпечне місто» за етапами (діагностика, обґрунтування мети, оцінка впливу на приватність, правила функціонування, прозорість і підзвітність, оцінювання, фінансування) на основі Настанов системи ООН щодо безпечніших міст і населених пунктів та британського Кодексу практики щодо камер спостереження. Запропоновано обов'язковий цикл оцінювання результативності, який полягає у визначенні базових значень показників до запуску системи, щорічному моніторингу і незалежном оцінюванні з публічним звітом.

Вивчено, що найвищу ефективність демонструють програми, інтегровані в довгострокові Стратегії розвитку міст, а не розроблені як відокремлені документи. Поширеним недоліком у багатьох українських містах залишається відсутність вимірюваних індикаторів ефективності, через що моніторинг часто зводиться до оцінки простого освоєння бюджетних коштів, а не реальних якісних змін для мешканців міст. Аналіз регіональних програм показує, що значна частина фінансування спрямовується на інфраструктурні об'єкти. Водночас інвестиції у відновлення людського капіталу часто ігноруються або фінансуються за залишковим принципом, проходячи етап публічного обговорення із залученням інститутів громадянського суспільства, що мають значно вищий рівень довіри та реальної результативності.

Обгрунтовано, що проєкти «Безпечне місто» є базовим елементом концепції «Розумне місто» (Smart City), спрямованим на створення комфортного та захищеного середовища для мешканців українських міст.

Висвітлено, що людиноцентричність і партисипативність перетворюють систему «Безпечне місто» з технічного нагляду на функціонуючий простір спільної безпеки. Людиноцентричність у концепції «Безпечне місто» орієнтована на захист прав, доступність та якість життя громадян українських міст. Партисипативність як залучення громадян до управління міста охоплює такі напрями, як участь жителів міст у обговоренні розташування камер чи освітлення, локальні ініціативи для покращення безпеки районів міст, використання цифрових сервісів та додатків для швидкого реагування на проблеми та комунікації з комунальними службами.

РОЗДІЛ ІІ
ОСОБЛИВОСТІ ФУНКЦІОНУВАНЯ СИСТЕМ «БЕЗПЕЧНЕ МІСТО» В УКРАЇНСЬКИХ РЕАЛІЯХ

2.1. Впровадження моделей світового досвіду в Україні

Впровадження світових моделей проєктів «Безпечне місто» має на меті створення єдиної інтегрованої системи цифрового моніторингу та управління для підвищення рівня безпеки громадян, зниження рівня злочинності та оптимізації роботи комунальних служб.

Використання вже перевіреного міжнародного досвіду (як-от моделей Лондона, Сінгапура чи Нью-Йорка) дозволяє містам не вигадувати велосипед, а впроваджувати готові, ефективні архітектури.

Світові стандарти побудовані на масштабованості. Модель «Безпечне містао» є основою метою, для маштабування освітлення, електронного врядування, екологічного моніторингу та цифрового громадського транспорту.

Таблиця 2.1

Напрями впровадження проєктів «Безпечне місто» (апробація світового досвіту в українських реаліях)

№п\п	**Напрями**	**Впроваджені заходи**
Підвищення громадської безпеки та протидія злочинності		
1.	Превентивний контроль	Камери з функцією розпізнавання облич, автомобільних номерів та аналізу поведінки (наприклад, виявлення залишених предметів або скупчень людей) допомагають зупиняти правопорушення до їхнього вчинення
2.	Швидке розслідування	Наявність єдиного архіву відеоданих високої якості скорочує час на пошук злочинців або викрадених цінностей з днів до кількох хвилин
3.	Моніторинг стратегічних об’єктів	Автоматичний нагляд за школами, лікарнями, мостами та державними установами
Оптимізація дорожнього руху		
4.	Керування трафіком	Світові моделі використовують "розумні" світлофори, які адаптують свій режим під щільність потоку машин, зменшуючи затори.

Продовження табл. 2.1

5.	Фіксація порушень ПДР	Автоматичний контроль швидкості, проїзду на червоне світло та правил паркування суттєво знижує аварійність
6.	Пріоритет для екстрених служб	Система може автоматично "відкривати" зелений коридор для швидких, пожежних машин чи поліції
Ефективне реагування на надзвичайні ситуації		
7.	Єдиний простір ситуаційних центрів	Об'єднання поліції, медиків, рятувальників ДСНС та комунальних служб в один координаційний центр
8.	Автоматичні сповіщення	Датчики диму, підтоплення, хімічного забруднення або звукові сенсори (наприклад, фіксація пострілу чи вибуху) миттєво передають сигнал тривоги без участі людини
Економічна вигода та оптимізація міського господарства		
9.	Зниження витрат	Автоматизація зменшує потребу у великій кількості патрульних чи інспекторів
10.	Контроль комунальників	Моніторинг якості прибирання доріг, вивезення сміття, стану ліній електропередач та ремонтних робіт
11.	Інвестиційна привабливість	Безпечні міста залучають більше туристів, міжнародного бізнесу та жителів

Джерело: складено автором на основі проведених досліджень

Впровадження концепції «Безпечне місто» в Україні опирається на передовий світовий досвід [73; 101; 187]. Воно передбачає створення інтегрованих систем відеоспостереження з аналітикою, авторозпізнаванням номерів, сенсорами моніторингу довкілля та єдиними операційними центрами реагування для таких міст, як Київ, Дніпро, Харків та Одеса.

Для реалізації проєктів «Безпечне місто» в Україні доцільно вивчити західну та східну (азійську) моделі. В рамках західної моделі (досвід ЄС та США) фокусуються на балансі безпеки та захисту приватного життя, використанні європейського/американського обладнання та залученні громадськості через прозорі муніципальні платформи [231]. Азійська/східна модель (досвід Сінгапуру, Китаю) характеризується тотальною цифровізацією, штучним інтелектом, прогнозна аналітика та глибока інтеграція біометричних даних.

Поєднання європейського прагнення до прозорості з екстреними викликами безпеки воєнного стану в Україні вимагає швидкої централізації даних МВС та захисту критичної інфраструктури [118; 129]. Відеокамери повинні мати аналітичну функцію розпізнавання облич та фіксації порушень правил дорожнього руху. Єдиний центр управління передбачає здійснення

швидкої координації поліції, ДСНС та комунальних служб в режимі реального часу. Обов'язковою є кібербезпека, тобто захист муніципальних мереж від зовнішніх втручань та атак.

Європейський досвід реалізації проєктів «Безпечне місто» змінився від простого встановлення камер спостереження до комплексних екосистем міської безпеки. Вони спираються не лише на технічні інновації, а й на інклюзивність, довіру мешканців та суворе дотримання прав людини. Ключові принципи та підходи до реалізації проєктів «Безпечне місто» в ЄС охоплює концепцію «Безпека через проєктування», яка передбачає досягнення балансування технологій та приватності даних при залученні мешканців міст.

Концепція «Безпека через проєктування» означає захист публічних просторів. яка інтегрується ще на етапі архітектурного планування (освітлення, оглядові зони, ландшафт і розміщення елементів міського середовища) без перетворення міст на укріплений пункт з міцними капітальними спорудами, постійним гарнізоном, озброєнням та різними запасами, призначеними для тривалої кругової оборони.

Всі цифрові та технологічні рішення проєктуються з орієнтацією на захист приватних персональних даних. Штучний інтелект для аналізу відео чи розпізнавання облич обмежується правилами Регламенту про захист даних (GDPR) [67], а обробка інформації часто здійснюється локально, а не на хмарних серверах загального доступу.

Європейська модель правового забезпечення проєктів «Безпечне місто» має багаторівневий характер, і саме ця багаторівневість визначає межі допустимих технічних рішень. Перший рівень утворює Загальний регламент про захист даних (Регламент (ЄС) 2016/679 від 27 квітня 2016 р.) [67], дія якого поширюється на муніципальних, комунальних і приватних операторів систем відеоспостереження. Для органів публічної влади принципове значення мають три його положення: обов'язок забезпечувати захист даних уже на етапі проєктування системи та за замовчуванням (ст. 25), віднесення біометричних даних, що обробляються з метою однозначної ідентифікації особи, до особливих

категорій персональних даних (ст. 9), а також обов’язкове проведення оцінки впливу на захист даних у разі систематичного масштабного моніторингу публічно доступних місць (п. «c» ч. 3 ст. 35). Отже, у державах – членах ЄС рішення про розгортання міської мережі камер не може бути ухвалене до завершення такої оцінки.

Другий рівень становить Директива (ЄС) 2016/680 від 27 квітня 2016 р., яка регулює обробку персональних даних поліцією та іншими компетентними органами з метою запобігання, розслідування, виявлення і переслідування кримінальних правопорушень [68]. Директива допускає обробку біометричних даних лише у разі суворої необхідності та за наявності належних гарантій (ст. 10), вимагає встановлення строків видалення даних або періодичного перегляду потреби в їх зберіганні (ст. 5), ведення журналів операцій в автоматизованих системах обробки – збирання, зміни, перегляду, розкриття, поєднання та видалення даних (ст. 25), а також попередньої оцінки впливу для обробки, що становить високий ризик (ст. 27). Для інтегрованих платформ «Безпечне місто», у яких дані муніципальних камер стають доступними поліції, це означає необхідність юридично розмежувати муніципальний і правоохоронний режими обробки та технічно забезпечити відстежування кожного звернення до даних.

Третій рівень сформовано Регламентом (ЄС) 2024/1689 від 13 червня 2024 р. про штучний інтелект [69]. Він заборонив використання систем віддаленої біометричної ідентифікації «в реальному часі» в публічно доступних місцях для правоохоронних цілей, за винятком вичерпно визначених випадків суворої необхідності: цільового пошуку жертв викрадення, торгівлі людьми, сексуальної експлуатації та зниклих осіб; запобігання конкретній, суттєвій і неминучій загрозі життю або фізичній безпеці людей чи реальній загрозі терористичного акту; встановлення місцеперебування або особи підозрюваного у вчиненні злочинів, перелічених у додатку II до Регламенту, за які передбачено позбавлення волі на строк не менше чотирьох років (п. «h» ч. 1 ст. 5). Навіть у цих випадках застосування потребує попереднього дозволу судового або незалежного адміністративного органу (ч. 3 ст. 5) та попередньої оцінки впливу

на основоположні права. Окремо заборонено створення або розширення баз даних для розпізнавання облич шляхом нецільового збирання зображень з інтернету чи записів камер відеоспостереження (п. «e» ч. 1 ст. 5), а також оцінювання ризику вчинення особою кримінального правопорушення виключно на підставі профілювання чи оцінки її особистісних рис (п. «d» ч. 1 ст. 5). Ці заборони застосовуються з 2 лютого 2025 р. Для «Безпечного міста» вони мають прямі проєктні наслідки: функції біометричної ідентифікації та прогнозної аналітики не можуть бути увімкнені в міській платформі за замовчуванням, а мають існувати як окремі модулі з власною правовою підставою, процедурою надання дозволу та журналом застосування.

Практичні орієнтири для операторів систем відеоспостереження містять Настанови Європейської ради із захисту даних 3/2019 [70]. Відповідно до них мета відеоспостереження має бути конкретно визначена до початку обробки, а загальне формулювання на зразок «для вашої безпеки» вважається недостатнім. Записи в більшості випадків рекомендовано видаляти, бажано автоматично, через кілька днів, а чим довшим є встановлений строк зберігання, особливо понад 72 години, тим ґрунтовнішим має бути обґрунтування законності мети й необхідності зберігання. Для українських міст, де строки зберігання записів нерідко визначаються технічною ємністю серверів, а не нормативно встановленою метою, ці орієнтири можуть стати основою типових регламентів функціонування систем.

Безпека розглядається як спільна взаємодія органів місцевого самоврядування, представників поліції та мешканців міст. Ініціативи Європейського форуму міської безпеки Efus активно залучають містян до оцінки рівня безпеки за допомогою мобільних додатків і опитувань [253]. Системи інтегрують дані відеомоніторингу, датчиків навколишнього середовища, управління транспортними потоками та аналіз соціальної напруги, дозволяючи прогнозувати ризики, а не лише реагувати на наслідки [65].

У Лондоні функціонує кілька масштабних ініціатив та технологічних проєктів, спрямованих на підвищення рівня безпеки та боротьбу зі злочинністю.

Співробітники міської поліції активно розширюють систему реального часу для сканування облич перехожих і порівняння їх із поліцейськими базами розшуку. Окрім мобільних фургонів із камерами, у центральних районах (зокрема, у Вест-Енді та Сохо) впроваджують стаціонарні пристрої на елементах міської інфраструктури для постійного моніторингу. Програма повітряного нагляду охоплює масштабування представниками поліції використання безпілотників, маючи на меті забезпечення постійного моніторингу за допомогою дронів у всіх районах Лондона [229].

Співробітники міської поліції Лондона ініціювали запровадження спеціальної програми для боротьби з вуличними крадіжками та зникненням речей, які були при вбитих чи поранених осіб у магазинах. Проєкт поєднує технології підвищеної видимості патрулювання на вулицях із сучасними інструментами аналізу даних для швидкого реагування на інциденти в районах підвищеного ризику.

Масштабування живого розпізнавання облич і повітряного спостереження в Лондоні актуалізує питання правових меж таких технологій, які в європейській і світовій практиці визначаються передусім судами. Для України ця практика має не лише порівняльне, а й юридичне значення: відповідно до ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» від 23.02.2006 № 3477-IV суди застосовують Конвенцію про захист прав людини і основоположних свобод 1950 р. [49] та практику Європейського суду з прав людини (ЄСПЛ) як джерело права [8]. Отже, стандарти, сформульовані у справах щодо відеоспостереження та біометричних технологій, є критеріями, за якими оцінюватиметься правомірність рішень органів влади, що проєктують і експлуатують системи «Безпечне місто».

Першим рішенням ЄСПЛ, яке безпосередньо стосувалося муніципальної системи відеоспостереження, стала справа «Пек проти Сполученого Королівства» (2003) [54]. Камери, встановлені радою округу Брентвуд, зафіксували заявника на вулиці в кризовому стані; оператор викликав поліцію, а згодом рада, прагнучи продемонструвати ефективність системи, передала записи

пресі й телебаченню без належного приховування обличчя. Суд зазначив, що саме по собі спостереження за особою в публічному місці без запису не становить втручання в приватне життя, однак оприлюднення записів зробило дії заявника відомими в обсязі, який значно перевищував усе, що він міг передбачити, і за відсутності належних гарантій порушило ст. 8 Конвенції; констатовано також відсутність ефективного засобу юридичного захисту (ст. 13). Суд окремо вказав, що рада мала інші можливості досягти своєї мети – отримати згоду особи або самостійно замаскувати зображення. Управлінський висновок для проєктувальників «Безпечного міста» полягає в тому, що порядок передання й оприлюднення записів, зокрема для інформаційних кампаній про ефективність камер, має бути регламентований не менш ретельно, як і порядок їх збирання.

Друга група рішень стосується зберігання біометричних даних і зображень. У справі «С. і Марпер проти Сполученого Королівства» (2008) Велика палата ЄСПЛ одностайно визнала загальне й невибіркове зберігання відбитків пальців, клітинних зразків і профілів ДНК осіб, які підозрювалися, але не були засуджені, непропорційним втручанням у приватне життя [55]. У справі «Gaughran v. the United Kingdom» (2020) Суд поширив цей підхід на безстрокове зберігання профіля ДНК, відбитків пальців і фотографії особи, засудженої за незначне правопорушення, за відсутності реальної можливості перегляду; суттєвим для визнання втручання стало те, що поліція могла застосовувати до таких фотографій технології розпізнавання облич [57]. У справі «Catt v. the United Kingdom» (2019) порушенням визнано зберігання даних мирного учасника протестів у поліцейській базі даних щодо так званого внутрішнього екстремізму за відсутності чіткого визначення підстав внесення до неї та гарантій щодо строків зберігання. Суд відхилив аргумент уряду про надмірну складність перегляду й видалення даних через неавтоматизований характер бази [56]. Із цих рішень випливає вимога, яку доцільно закладати вже в технічне завдання: архітектура системи має забезпечувати диференційовані строки зберігання, періодичний перегляд і вибіркове видалення даних, а технічна складність таких операцій не може виправдовувати безстрокове зберігання.

Третя група рішень стосується масової та автоматизованої аналітики. У справі «Біг Бразер Вотч та інші проти Сполученого Королівства» (2021) Велика палата ЄСПЛ визнала, що режим масового перехоплення комунікацій порушував ст. 8 і ст. 10 Конвенції через відсутність незалежного дозволу, невключення категорій критеріїв відбору (селекторів) до запиту на дозвіл та відсутність попереднього внутрішнього погодження селекторів, пов'язаних з конкретними особами; Суд сформулював вимогу «наскрізних гарантій» на кожному етапі обробки – від збирання до аналізу, зберігання й передання даних [58]. Федеральний конституційний суд Німеччини в рішенні від 16.02.2023 визнав неконституційними положення законодавства Гессену і Гамбургу про автоматизований аналіз поліцейських баз даних (у Гессені його здійснювали за допомогою платформи «hessenDATA»), оскільки вони не встановлювали достатніх порогів для втручання; суд підкреслив, що автоматизований аналіз має власну вагу втручання, яка залежить від виду й обсягу даних та допустимого методу аналізу [65]. Раніше, в ухвалі від 18.12.2018 щодо автоматизованого контролю номерних знаків у Баварії, вищезгадайний суд дійшов висновку, що втручання у право на інформаційне самовизначення є фіксація номера кожного транспортного засобу, навіть якщо збігу з розшуковими базами не виявлено, а застосування таких систем допустиме лише для захисту правових благ щонайменше значної ваги [64]. Для українських міст, де розпізнавання номерних знаків стало стандартним елементом «Безпечного міста», це означає потребу в законодавчо визначених цілях і місцях застосування систем та в негайному видаленні даних про транспортні засоби, щодо яких збігів не встановлено.

Четверта група стосується розпізнавання облич. У справі R (Bridges) v Chief Constable of South Wales Police (2020) Апеляційний суд Англії та Уельсу визнав незаконним застосування поліцією Південного Уельсу системи автоматизованого розпізнавання облич: правова база залишала поліцейським надмірну свободу розсуду щодо того, хто може бути внесений до списків спостереження і де розгортається система; оцінка впливу на захист даних була неналежною; поліція не вжила заходів, щоб переконатися у відсутності расової

чи гендерної упередженості програмного забезпечення [61]. Водночас суд не визнав використання технології непропорційним як такого, тобто проблема полягала не в самій технології, а у відсутності чітких правил її застосування. У справі «Глухін проти Росії» (2023), першій справі ЄСПЛ щодо розпізнавання облич, Суд встановив порушення ст. 8 і ст. 10 Конвенції у зв'язку з ідентифікацією, встановленням місцеперебування та затриманням учасника одиночного мирного пікету з використанням камер московського метрополітену [59]. За даними, наведеними в рішенні, станом на 1 вересня 2020 р. функцію живого розпізнавання облич мали всі близько 175 тис. камер Москви, а у 2022 р. кількість таких камер перевищила 220 тис. Суд наголосив на необхідності детальних правил щодо сфери застосування технології, процедур дозволу, порядку використання і зберігання отриманих даних, механізмів нагляду та засобів правового захисту, вказавши, що потреба в гарантіях є ще більшою у разі живого розпізнавання. Це рішення важливе й для оцінювання східної моделі, розглянутої нижче: технічна досконалість централізованої біометричної інфраструктури за відсутності таких гарантій створює ризики, несумісні з європейськими стандартами, на які орієнтується Україна.

Подальша практика підтвердила цей висновок. Рішенням від 21 квітня 2026 р. у справі R (Thompson and Carlo) v Commissioner of Police of the Metropolis Високий суд Англії та Уельсу відхилив позов щодо політики Столичної поліції Лондона із застосування розпізнавання облич у реальному часі, ухваленої 11 вересня 2024 р. [62]. Суд дійшов висновку, що ця політика не надає поліцейським необмеженої чи свавільної дискреції щодо застосування технології; до списків спостереження вносять лише визначені категорії розшукуваних осіб, а зображення облич людей, щодо яких збігу не виявлено, розмиваються [63]. За оцінкою юридичних аналітиків, поліція виграла справу насамперед тому, що переглянута політика усунула недоліки, виявлені у справі Bridges, а отже законність таких технологій визначається передусім надійністю механізмів управління ними [217]. Водночас правозахисники наголошують, що Парламент досі не ухвалив спеціального закону про розпізнавання облич, і

закликають зупинити розширення його застосування до такого врегулювання [229]. Для України зіставлення справ Bridges і Thompson означає, що біометричні функції систем «Безпечне місто» можуть бути законними лише за наявності заздалегідь визначених правил: хто і за якими критеріями вносить осіб до списків спостереження, де і як довго працює система, що відбувається з даними осіб, щодо яких збігу не виявлено.

Окремо слід зважати на правовий статус приватних камер, які дедалі частіше інтегруються в міські мережі. Суд Європейського Союзу у справі C-212/13 (Ryneš) (2014) встановив, що відеоспостереження, яке хоча б частково охоплює публічний простір, не може розглядатися як суто особиста чи побутова діяльність, а отже, підпадає під дію законодавства про захист персональних даних [60]. Тому програми залучення камер мешканців і бізнесу до «Безпечного міста» потребують договірного визначення ролей та обов’язків власників камер як власників персональних даних. Щодо повітряного спостереження показовим є рішення Апеляційного суду США четвертого округу у справі Leaders of a Beautiful Struggle v. Baltimore Police Department (2021), яким доступ поліції до даних програми тривалого спостереження з літаків над Балтимором визнано таким, що порушує Четверту поправку до Конституції США [66]. Для проєктів із використанням дронів це означає, що тривале площинне спостереження з повітря розглядається як окремий, більш інтрузивний вид втручання, що потребує спеціальної правової підстави.

Українська судова практика поки що оцінює відеофіксацію переважно з позицій допустимості доказів. Так, Касаційний кримінальний суд у складі Верховного Суду в постанові від 08.05.2025 у справі № 207/722/23 визнав допустимим доказом відеозапис з нагрудних камер поліцейських, здійснений без попередження особи, пославшись на ст. 40 Закону України «Про Національну поліцію» від 02.07.2015 № 580-VIII, яка дозволяє поліції застосовувати фото- і відеотехніку, у тому числі таку, що працює в автоматичному режимі [21; 53]. Конституційний Суд України ще в рішенні від 20.01.2012 № 2-рп/2012 визнав інформацію про особисте та сімейне життя особи конфіденційною, яка може

бути поширена без згоди особи лише у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [52]. Зіставлення цих позицій із наведеною практикою свідчить, що загальні повноваження поліції щодо відеофіксації не замінюють спеціального правового регулювання біометричної ідентифікації та автоматизованої аналітики. Відповідно, муніципальні програми «Безпечне місто» не можуть бути достатньою правовою підставою для таких функцій, що є додатковим аргументом на користь запровадження проєктів на державному рівні.

Специфіку воєнного часу визначає ст. 15 Конвенції, яка дозволяє державі в період війни відступати від окремих зобов'язань лише тією мірою, якої суворо вимагає гострота становища. Україна з 2022 р. повідомила Раду Європи про такий відступ, зокрема щодо ст. 8 Конвенції [50]. Це створює правову основу для заходів на кшталт обмеження публічних трансляцій з камер чи розширеного доступу сил безпеки та оборони до відеоданих, проте не скасовує вимог пропорційності й тимчасовості. З управлінського погляду системи слід проєктувати з можливістю переходу між режимами воєнного та мирного часу, документуючи кожне розширення доступу, щоб після припинення воєнного стану їх функціонування можна було привести у відповідність до повного обсягу конвенційних стандартів.

Узагальнення розглянутої практики дає змогу визначити її вплив на управлінські рішення при проєктуванні систем «Безпечне місто»:

- правова підстава: біометрична ідентифікація, розпізнавання номерних знаків та автоматизована аналітика потребують закону, який визначає, хто, де, з якою метою і як довго може застосовувати ці функції;
- оцінка впливу: оцінку впливу на захист даних і права людини слід проводити до закупівлі та розгортання системи, а не після введення її в експлуатацію;
- строки зберігання: диференційовані строки, автоматичне видалення і процедури перегляду мають бути закладені в основу технічного завдання;

- оприлюднення записів: потрібен регламент передання записів третім особам і медіа з обов'язковим знеособленням;
- біометричні функції: необхідні критерії формування списків спостереження, перелік місць застосування, незалежний дозвіл і перевірка алгоритмів на упередженість у процедурі закупівлі;
- аналітика: потрібні наскрізні гарантії, журналювання кожного доступу та незалежний аудит;
- приватні камери: інтеграція можлива лише на договірних засадах з визначенням обов'язків власників як володільців даних;
- воєнний стан: режим розширеного доступу має бути задокументований і мати план повернення до стандартів мирного часу.

Проблеми впровадження європейської моделі світового досвіду в Україні полягають у:

- залежності від окремих масових закордонних виробників апаратного забезпечення;
- недостатньому обсязі фінансування на рівні окремих міст в умовах воєнного стану;
- ризики порушення прав громадян на приватність через недосконалість законодавчого поля щодо регулювання біометричних даних.

Досвід США у впровадженні концепції «Безпечне місто» базується на переході від реактивного реагування на злочини до проактивного управління безпекою за допомогою Центрів оперативного реагування в реальному часі, інтеграції різнопланових сенсорів та державно-приватного партнерства [212; 239]. Водночас американські дослідження «шляху до злочину» свідчать, що правопорушники здебільшого вчиняють злочини неподалік від місця проживання – як правило, в межах однієї-двох миль від дому [243]. Ключові елементи американської моделі «Безпечне місто» охоплюють спеціальні аналітичні центри поліції, AI-камери для автоматичного розпізнавання номерів, акустичні детектори пострілів, програми інтеграції приватних камер та дрони як перші реагувальники.

Спеціальні аналітичні центри поліції (наприклад, у Лас-Вегасі, Мемфісі, Ричмонді) функціонують як «диспетчерські для патрульних». Вони агрегують потоки даних з вулиць та передають опрацьовану інформацію про підозрюваних на планшети офіцерів поліції за лічені секунди [239].

Масове використання систем із інноваційними технологіями від компанії Flock Safety дозволяє автоматично виявляти розшукуваний автотранспорт за допомогою технологічних AI-камер для розпізнавання номерів (LPR).Системи типу ShotSpotter (виробництва компанії SoundThinking) у режимі реального часу автоматично виявлення, локалізації та реєстрації звуків пострілів за допомогою акустичних датчиків та миттєво передавати координати в спеціальні аналітичні центри [211]. Основна мета такої технології полягає у забезпеченні швидкого реагування екстрених або військових служб, оскільки, за статистикою, значна частина випадків стрілянини в містах не надходить на гарячі лінії поліції [209].

У Бірмінгемі поліцейські департаменти залучають мешканців підприємців до добровільної реєстрації та об'єднання зовнішніх камер відеонагляду в єдину мережу для прискорення розслідувань. За сучасних умов у США передбачено запуск безпілотників за сигналом emergency services ще до приїзду патрульних, що дає змогу оцінити ситуацію з повітря [212; 214].

У США на законодавчому рівні жорстко обмежується або забороняється використання китайського обладнання (наприклад, камер Hikvision/Dahua чи дронів DJI) через кіберзагрози та приховані ризики ураження апаратури [71; 215].

Найвідомішим аналогом концепції «Безпечне місто» в Нью-Йорку є масштабний проєкт Domain Awareness System (DAS), створений Поліцейським управлінням Нью-Йорка (NYPD) спільно з компанією Microsoft. Проєкт був ініційований в межах Манхеттену для захисту фінансового центру та боротьби з тероризмом, а згодом охопив усі райони міста Нью-Йорк. Централізована система DAS інтегрує дані понад 80 000 державних та приватних камер відеоспостереження, сканери автомобільних номерів (LPR), датчики радіації та хімічної безпеки. Дані з екстрених викликів (emergency services/311), архівів

арештів та детективних звітів миттєво зводяться в єдину аналітичну інформаційну панель для оперативного реагування. Мобільний доступ для патрульних поліції, кожен з яких має доступ до елементів системи через службові смартфони чи планшети в автомобілі для перевірки ситуації на маршруті.

Проблеми, пов'язані з реалізацією концепції «Безпечне місто», стосуються суспільної критики за порушення конфіденційності та оцінки ефективності окремих інструментів. Використання мілітарних технологій та систем розпізнавання облич викликає протести правозахисників через ризики тотального стеження та порушення прав громадян. Через високу вартість та суперечливі результати оцінки ефективності окремих інструментів у деяких містах. Так, у Чикаго у 2024 р. не продовжили контракт на систему акустичного виявлення пострілів ShotSpotter, яку місто використовувало з 2012 р., систему відключили у вересні 2024 р., а подальші заходи міська влада пов'язала зі співпрацею з громадами та організаціями із запобігання насильству [255].

Суперечливість оцінок ефективності окремих інструментів зумовлює потребу опиратися на доказові дані, а не на декларації виробників чи звіти про кількість встановленого обладнання. Найповнішим узагальненням таких даних є систематичний огляд із метааналізом, що охопив результати оцінювальних досліджень за 40 років [235]. Його висновки свідчать, що відеоспостереження пов'язане зі статистично значущим, але помірним зниженням злочинності; найбільший і найстабільніший ефект зафіксовано на автостоянках, значущий ефект – також у житлових кварталах. Системи з активним моніторингом операторами показали кращі результати, ніж пасивні системи запису, а поєднання камер з іншими профілактичними заходами давало більший ефект, ніж їх використання як самостійного засобу. Автори дійшли висновку, що відеоспостереження доцільно та раціонально спрямовувати на протидію злочинам щодо транспортних засобів і майна, а не розглядати як універсальний інструмент.

Приклад акустичних детекторів пострілів демонструє, як незалежний аудит може змінити оцінку технології. Управління генерального інспектора м. Чикаго проаналізувало 50 176 сповіщень системи ShotSpotter, підтверджених як імовірні постріли, за період з 1 січня 2020 р. до 31 травня 2021 р. і встановило, що докази правопорушення, пов'язаного з вогнепальною зброєю, було виявлено лише у 9,1 % випадків реагування поліції, а слідчі зупинки, безпосередньо зумовлені сповіщенням, – у 2,1 % випадків [211]. Аудит також зафіксував, що наявність системи впливала на поведінку поліцейських у районах із частими сповіщеннями, а недоліки обліку ускладнювали оцінювання результативності. Показово, що предметом аудиту була не технічна точність системи, а її операційна цінність для поліції.

Протилежним прикладом є нью-йоркська система Domain Awareness System, розробка якої розпочалася у 2008 р. Згідно з публікацією фахівців Поліцейського управління Нью-Йорка, система поєднує розпізнавання образів, машинне навчання та візуалізацію даних, а її впровадження забезпечило оцінену економію близько 50 млн дол. США на рік завдяки підвищенню ефективності роботи персоналу; після розгортання в усьому управлінні у 2013 р. загальний індекс злочинності в місті знизився на 6 % [227]. Ці дані слід інтерпретувати обережно, оскільки йдеться про самооцінку відомства, а зниження злочинності має багатофакторну природу. Водночас нью-йоркський досвід демонструє й інструменти публічної підзвітності: поліцейське управління оприлюднює політику впливу і використання системи, яка описує її можливості, правила застосування, заходи безпеки та строки зберігання даних; чинну редакцію оновлено 4 лютого 2026 р. [233].

Для України з цього випливає, що програми «Безпечне місто» повинні містити механізм оцінювання результатів: визначення базових показників до встановлення обладнання, пілотні проєкти з порівнянням територій, показники результатів (динаміка злочинності, час реагування, розкриття правопорушень), а не лише показники витрат і кількості камер, а також незалежний аудит. Закупівля

технологій без підтвердженої операційної цінності в умовах обмежених бюджетів громад є невиправданим використанням публічних коштів.

Східна (азійська) модель «Безпечне місто» базується на жорсткій державній координації, масовому впровадженні штучного інтелекту, систем розпізнавання облич, Інтернету речей (IoT) та об'єднанні всіх комунальних і правоохоронних служб у єдині централізовані ситуаційні центри реагування в реальному часі [218]. Ключовою рисою східної (азійської) моделі є домінування централізованого державного управління та єдиних вертикальних протоколів замість ініціатив представників місцевих органів влади [218]. На думку автора, що ґрунтується на сукупному аналізі джерел, у межах цієї моделі перспективним є застосування безпілотників із панорамними камерами для моніторингу масових скупчень людей з повітря. Прямі канали зв'язку забезпечують миттєву передачу зашифрованого відеопотоку на планшети патрульних поліцейських ще до їх прибуття на місце події [218].

Східна модель (зокрема досвід країн Східної та Південно-Східної Азії, таких як Сінгапур, Південна Корея чи Японія) у створенні проєктів «Безпечне місто» спирається на тотальну цифрову інтеграцію, жорсткий державний контроль та концепцію «панування даних» у реальному часі [218]. Тому основними рисами східної (азійської) моделі вважається централізоване управління, застосування штучного інтелекту

Вся інформація з камер, датчиків та систем спостереження надходить до національних або міських ситуаційних центрів. Широке використання біометричної аналітики, систем розпізнавання облич, моніторинг поведінкових звичок об'єктів перебування в публічних місцях. Пріоритет надається громадському порядку та державній безпеці над приватністю мешканців східних країн світу.

Тісна співпраця представників місцевих органів державної влади із групою найбільших і найвпливовіших ІТ-компаній світу, які домінують у сфері цифрових технологій, інтернету, хмарних послуг та штучного інтелекту для

розробки та масштабування інноваційних платформ. До провідної групи «Великої п’ятірки» (GAFAM) входять:

- Alphabet (Google) – пошуковий сервіс, онлайнреклама, операційна система Android, хмарні рішення;
- Amazon – найбільший маркетплейс у світі та лідер у сфері хмарних обчислень (AWS);
- Apple – виробник iPhone, Mac, розробник iOS та екосистеми сервісів;
- Meta (Facebook, Instagram, WhatsApp) – глобальна імперія соціальних мереж та комунікаційних платформ;
- Microsoft – розробник Windows, офісного пакету 365, власник сервісів Azure та інвестор у галузі ШІ.

Поряд із величезними економічними можливостями, найвпливовіші ІТ-компанії світу формують правила повсякденного цифрового життя, що привертає пильну увагу державних управлінців усього світу.

Головні переваги східної моделі запровадження проєктів «Безпечне місто» вважаються миттєве реагування на надзвичайні ситуації та правопорушення завдяки прогнозованій аналітиці, високий рівень розкриття злочинів та профілактика правопорушень, а також повна синхронізація роботи поліції, екстрених служб і комунальної інфраструктури.

Китайська модель проєктів «Безпечне місто» – це масштабні державні системи масового відеоспостереження та аналізу даних, що інтегрують штучний інтелект, і єдині центри управління для тотального контролю громадського порядку та превенції правопорушень. Забезпечується широке покриття мережами камер високої роздільної здатності на вулицях, у транспорті та громадських місцях. Автоматично здійснюється розпізнавання облич, аналіз поведінки та відстеження пересування громадян у реальному часі. Інформаційні даних поліції, комунальних служб та приватних систем зведені у єдині хмарні платформи. Ключовою ознакою китайської моделі проєктів «Безпечне місто» є використання технологічної бази та програмного забезпечення масштабних локальних виробників (таких як, Hikvision чи Dahua) [71; 218].

Переваги застосування китайської моделі реалізації концепції «Безпечне місто» можна віднести високу швидкість розкриття злочинів, миттєве реагування на надзвичайні ситуації, зниження рівня вуличної злочинності. Китайська модель проєкту «Безпечне місто» характеризується залежністю від закритих державних алгоритмів, несучи в собі загрози приватності, ризики масового стеження та обмеження громадянських свобод.

Аналізуючи китайську модель, слід враховувати, що вона є не лише моделлю управління, а й експортним продуктом. Дослідження Центру стратегічних і міжнародних досліджень (CSIS) за відкритими джерелами ідентифікувало 73 угоди компанії Huawei щодо рішень «Safe City» у 52 країнах [218]. Сімдесят один відсоток таких угод припадає на країни, які за оцінками Freedom House у 2009–2018 рр. мали в середньому статус «частково вільних» або «невільних», 59 % – на країни Азії та Африки на південь від Сахари, 71 % – на країни із середнім рівнем доходу. Автори дослідження дійшли висновку, що задекларовані переваги цих рішень важко перевірити, а в окремих випадках вони видаються суттєво перебільшеними, тоді як високі витрати на заміну обладнання створюють ефект технологічної прив'язки держав-замовників до постачальника.

Безпекові ризики постачальників дедалі частіше стають предметом законодавчих рішень. У США Законом імені Джона С. Маккейна про повноваження в галузі національної оборони на 2019 фінансовий рік (Pub. L. 115-232), підписаним 13 серпня 2018 р., федеральним органам заборонено закуповувати телекомунікаційне обладнання Huawei і ZTE, а також обладнання для відеоспостереження й телекомунікацій виробництва Hikvision, Dahua та Hytera, призначене для цілей громадської безпеки, охорони урядових об'єктів, фізичного спостереження за критичною інфраструктурою та інших цілей національної безпеки (ст. 889) [71]. Для України в умовах війни питання походження обладнання і програмного забезпечення систем «Безпечне місто» має розглядатися як складова кібербезпеки, засади якої визначає Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [23]. Це передбачає включення до тендерної документації вимог щодо

безпеки ланцюгів постачання, відкритих стандартів і сумісності обладнання, що зменшує ризик технологічної прив'язки, а також можливості незалежного аудиту програмного забезпечення.

Сінгапур реалізує концепцію безпечного та інтелектуального міста в межах загальнонаціональної ініціативи Smart Nation [247], спрямованої на впровадження цифрових технологій, штучного інтелекту та великих даних у всі сфери міського життя. Ініціатива Smart Nation об'єднує державні послуги, відеоспостереження та інтернет речей. Основні компоненти сінгапурської моделі проєктів «Безпечне місто» представлені національною сенсорною мережею, платформами аналізу даних, мобільним застосунком myResponder.

Сінгапур функціонує як єдине ціле (місто-держава), що усуває бюрократичні перешкоди між різними міністерствами (наприклад, Міністерством внутрішніх справ та Економічним комітетом). Технології розгортаються не як окремі пілотні проєкти, а як єдина державна операційна система. Доступ до даних суворо регламентований правилами кібербезпеки та інформаційного управління. Різні відомства мають доступ лише до того масиву інформації, який необхідний для виконання їхніх безпосередніх завдань [241].

Управлінською особливістю принципів впровадження сінгапурської моделі проєкту «Безпечне місто» є концепція «Цифрового близнюка». Високодеталізована 3D-модель усього міста-держави, яка в реальному часі відображає параметри будівель, транспортні потоки та пересування населення. Це дозволяє моделювати надзвичайні ситуації, планувати евакуацію та оптимізувати міську інфраструктуру у віртуальному середовищі [197]. Проактивне патрулювання розкривається у випробуванні автономних наземних роботів: у вересні 2021 р. робот Xavier, розроблений Агентством науки і технологій Home Team (HTX) разом з A*STAR, патрулював район Тоа Пайо, виявляючи за допомогою відеоаналітики небажану поведінку в публічному просторі та сповіщаючи операторів [220]. На думку автора, логічним продовженням цього підходу є використання дронів для повітряного моніторингу та «розумних» елементів міської інфраструктури, зокрема ліхтарів

із датчиками, для сигналізування про інциденти. Високий рівень контролю та відеоспостереження загалом сприймається суспільством як прийнятна плата за нульовий рівень злочинності та комфортне середовище проживання.

Залучення досвідчених волонтерів до надання першої допомоги до приїзду екстрених служб здійснюється за допомогою платформи аналізу даних та мобільного застосунку myResponder (офіційний додаток Сінгапурської служби цивільної оборони (SCDF), який сповіщає волонтерів про наближення надзвичайних ситуацій). Проєкти зі встановлення інтерактивних тривожних кнопок та сенсорів руху в житлових кварталах (HDB) призначені для захисту літніх людей, оперативного сповіщення опікунів та служб допомоги. Комплексні програми захисту цифрової інфраструктури та інструменти перевірки алгоритмів штучного інтелекту забезпечують кібербезпеку сінгапурських міст та довіру їхнього населення.

Тотальна інтелектуальна інфраструктура сенсорів представлена мережею камер спостереження високої роздільної здатності. Вона охоплює житлові квартали, транспортні вузли та місця громадського паркування. До 2030 року кількість таких камер планують збільшити до 200 000 одиниць. Вони оснащені функціями розпізнавання облич, аналізу скупчення людей та зчитування автомобільних номерів. Паралельно здійснюється трансформація національної сенсорної системи – понад 110 000 ліхтарних стовпів на вузли з датчиками для моніторингу довкілля, трафіку та систем розпізнавання.

Спільні розробки фахівцями Міністерства внутрішніх справ та технологічних партнерів проявилися у платформах аналізу даних, які здійснюються для прогнозування надзвичайних ситуацій, керування транспортними потоками та реагування на інциденти в реальному часі. Міжвідомча інтеграція даних (Платформа MAG1C / Safe City Test Bed) означає об’єднання інформації не лише для поліції, але й для служби надзвичайних ситуацій, екологічного нагляду та муніципальних служб. Дані з камер, датчиків якості повітря, повеней та навіть реакцій у соцмережах систематично зводяться до єдиного аналітичного центру для прогнозування інцидентів [232].

Сінгапурська модель «Безпечне місто» є частиною масштабної національної ініціативи Smart Nation і розглядається у світовій практиці як еталонний приклад глибокої централізації, міжвідомчої інтеграції та використання проактивної відеоаналітики. Ця модель перетворила острівну державу на одне з найбезпечніших місць земної кулі завдяки системному поєднанню технологій, прагматичного законодавства та високого рівня довіри суспільства.

У Китаї чи Сінгапурі використовується велика кількість камер із функціями біометричного аналізу, відстеження розташування та параметрів транспортних засобів у реальному часі за допомогою супутникових систем навігації та прогнозування можливих правопорушень [101].

Японська модель проєкту «Безпечне розумне місто» (Safe/Smart City) зосереджена не лише на відеоспостереженні чи поліцейському контролі, а на комплексній стійкості до стихійних лих, турботі про старіння суспільства та безпецки довкілля. Її ключовою особливістю вважається державно-приватне партнерство та участь громадян за принципом добровільна згода користувача на отримання повідомлень, розсилок або участь у комунікації замість тотального нагляду [219; 224].

Національна ініціатива Уряду Японії проєкт PLATEAU, ключовими технологічними та інституційними елементи якого є розробка масових 3D-моделей міст у відкритому доступі для симуляції надзвичайних ситуацій та планування безпеки [237]. Цифрові сервіси та сповіщення про небезпеку підключаються за згодою мешканців на добровільну підписку, що знімає етичні та соціальні бар’єри захисту приватного життя міст Японії. Міські вузли проєктуються так, щоб мінімізувати затори й забезпечити швидку евакуацію людей та логістику вантажів. Тому базові принципи японського підходу до реалізації проєктів «Безпечне місто» ґрунтуються на зпобіганні катастроф, а саме системи раннього оповіщення про землетруси, цунамі та тайфуни на базі штучного інтелекту інтегровано в загальну міську мережу [207; 224].

Інтеграція локальної електричної системи, сонячних панелей та водневого палива на рівні окремих кварталів (як у відомих японських проєктах Kashiwa-no-ha або Fujisawa SST, які демонструють інноваційні моделі сталого розвитку, енергоефективності та комфортного середовища для життя) обумовлена необхідністю забезпечення енергонезалежності жителів японських міст [246].

Використовуються єдині платформи обміну даними, які інтегрують середовища міського транспорту, медичних служб та комунальних підприємств [224]. Функціонують експериментальні майданчики майбутнього (наприклад, Woven City від Toyota) для тестування в реальних умовах, а саме відпрацювання взаємодії пішоходів, роботів та безпілотного транспорту.

Модель Південної Кореї у проєктах «Безпечне місто» базується на концепції інтегрованої платформи Smart City Integrated Platform, яка об'єднує поліцію, пожежників, екстрені медичні служби та муніципальні центри управління в єдину цифрову систему реального часу [236; 242].

На даному етапі здійснюється перехід від пасивного нагляду до інтелектуального моніторингу – використання AI-камер для розпізнавання загроз, прогнозування скупчення людей, аналізу трафіку та раннього виявлення надзвичайних ситуацій. До розробки та масштабування рішень активно залучаються технологічні партнери, серед яких Samsung SDS, LG CNS, KT). Дані з камер відеоспостереження (CCTV), датчиків погоди, екології та транспорту автоматично передаються до екстрених служб «112» (поліція) та «119» (пожежні/швидка) в момент надходження виклику. Міжвідомча інтеграція здійснюється за допомогою 3G/4G/5G та інтернет засобів.

Застосування спеціальних експериментальних нормативно-правових режимів дозволяє швидко тестувати та впроваджувати інновації без жорстких бюрократичних перепон [230]. Головні переваги моделі Південної Кореї у проєктах «Безпечне місто» полягають у:

- скороченні часу реагування екстрених служб на надзвичайні події на 30–50%.

- зниженні рівня злочинності та підвищення ефективності управління у критичних ситуаціях (повені, пожежі, техногенні аварії);
- стандартизації рішень на національному рівні, що унеможливлює створення ізольованих одне від одного відомчих баз даних.

Зіставлення розглянутих моделей із національною правовою базою дає змогу окреслити зміст адаптації світового досвіду. Конституція України гарантує невтручання в особисте і сімейне життя та забороняє збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ст. 32) [1]. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [16] не передбачає обов'язкової оцінки впливу на захист даних і спеціальних правил для систем віддаленої біометричної ідентифікації та автоматизованої аналітики. Законопроєкт № 8153 «Про захист персональних даних», зареєстрований 25.10.2022 і покликаний оновити національне регулювання у цій сфері, станом на грудень 2025 р. перебував на стадії підготовки до другого читання [177]. Повноваження поліції щодо застосування фото- і відеотехніки визначено ст. 40 Закону України «Про Національну поліцію» [21], однак ця норма не встановлює спеціальних правил для біометричної ідентифікації в публічних місцях, на кшталт тих, яких вимагає наведена судова практика.

Практика окремих міст свідчить про розрив між технологічними можливостями та регуляторними рамками. Так, у 2019 р. в межах київського проєкту «Безпечне місто» тестувався аналітичний модуль відеоспостереження, камери якого фіксували обличчя людей, а дані зберігалися на сервері протягом 30 днів; загальноміська система на той час налічувала близько 6 тис. камер [185]. Такий строк зберігання значно перевищує орієнтири, які Європейська рада із захисту даних визначає для типових систем відеоспостереження [70], і в європейській практиці потребував би окремого обґрунтування. Ще розпорядженням Кабінету Міністрів України від 06.02.2013 № 51-р було схвалено Концепцію Державної цільової правоохоронної програми

встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року [37], а Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р [39; 41; 180], визначила загальні засади державної політики у сфері штучного інтелекту, однак спеціального нормативного регулювання систем «Безпечне місто» на державному рівні так і не було створено.

Отже, адаптація світового досвіду для України полягає не стільки в запозиченні технічної архітектури тієї чи іншої моделі, скільки в перенесенні правових і управлінських гарантій: закріпленні на рівні закону переліку функцій систем та підстав їх застосування, обов'язкової оцінки впливу, нормативних строків зберігання і порядку доступу до даних, незалежного нагляду та механізмів оцінювання ефективності.

Впровадження світового досвіду в Україні вимагає не простого копіювання ефективних іноземних моделей проєктів «Безпечне місто», а їхньої глибокої адаптації до національної специфіки економічних, правових та соціальних умов. Ефективна імплементація передбачає поєднання міжнародних стандартів із внутрішнім потенціалом української держави, особливо в умовах євроінтеграції та післявоєнного відновлення. Реформи мають впроваджуватися поетапно, із ретельним попереднім моделюванням та системним прогнозуванням ризиків. Відповідно до світового досвіду моделі, що поєднують міжнародне фінансування, інвестиції підприємницьких структур та державну підтримку [10]. Цифровізація процесів у формі використання передових ІТ-рішень прискорює трансляцію світових практик в українське законодавство та управління. Ефективність реалізації проєктів «Безпечне місто» залежить від готовності державних інституцій прозоро й ефективно адмініструвати правила проєктів.

2.2. Розвиток соціальної політики держави у проєктах «Безпечне місто»

Проєкти «Безпечне місто» впроваджуються від виключно правоохоронних інструментів до важливих елементів соціальної політики держави, інтегруючи цифрові технології та інфраструктуру задля захисту вразливих верств населення, підтримки ветеранів, ВПО та створення інклюзивного середовища [78; 92; 110].

Дослідження розвитку соціальної політики в контексті проєктів «Безпечне місто» **демонструє** важливу трансформацію: ініціатива, яку традиційно вважали суто технічною та безпековою (камери, сервери, датчики) є дієвим інструментом інтеграції інновацій у соціальну сферу українського суспільства. Вона виступає базовим елементом цифрової трансформації міського управління та сталого розвитку міст України [86].

Традиційний підхід до реалізації проєктів «Безпечне місто» передбачав:

- постфактумне реагування співробітників поліції чи комунальних служб на вже наявні правопорушення або аварії;
- розслідування інцидентів за допомогою відеоархівів після звернення громадян;
- ручний розподіл ресурсів екстрених служб за фактом надзвичайної події;
- реалізацію локальних точкових заходів без єдиного інформаційного простору.

Проєкти «Безпечне місто» впливають на модернізацію соціальної політики шляхом трансформування від функцій контролю до соціальної безпеки. Початково системи міського відеонагляду фокусувалися на локальній фіксації правопорушень. Сучасні пріоритети проєкту «Безпечне місто» наблизилися до соціальної безпеки на території України, а саме зниження рівня тривожності, забезпечення психологічної стійкості та комфорту українських громадян, покращення інклюзивності міського середовища та захист прав вразливих верств населення (табл. 2.2). Інклюзія людей з інвалідністю та вразливих груп до активного життя функціонально реалізується за допомогою захищених

цифрових середовищ та комунальних сервісів підтримки. Створення єдиного інформаційного простору передбачає інтеграцію даних, що, у свою чергу, дозволяє координувати роботу комунальних служб, соціальних працівників, ДСНС та поліції. Сучасні програми проєктів «Безпечне місто» можна розглядати як стратегічне підґрунтя для соціальної стабілізації та повоєнній відбудові українських міст [164; 179].

Таблиця 2.2

Порівняння традиційного та соціально-орієнтованого підходів до реалізації проєктів «Безпечне місто»

Критерій порівняння	**Традиційний підхід (технічний)**	**Сучасний підхід (соціально-орієнтований)**
Головна мета	Фіксація правопорушень і контроль трафіку	Підвищення якості життя та соціальна згуртованість
Цільова аудиторія	Правоохоронні органи, поліція, ДСНС	Уся громада (включаючи маломобільні та вразливі групи)
Технологічний фокус	Лише камери та збереження відеоархіву	AI-аналітика, екологічні датчики, превентивне реагування
Роль місцевої влади	Пасивний замовник обладнання	Активний розробник безпекової та соціальної політики

Джерело: складено автором на основі проведених досліджень

Соціально-орієнтований підхід до реалізації проєктів «Безпечне місто» передбачає формування системи випереджувальних заходів, спрямованих на запобігання правопорушенням до того, як вони настануть. Він ґрунтується на використанні штучного інтелекту та відеоаналітики для прогнозування ризиків, автоматизоване оповіщення профільних служб до настання критичної ситуації. Інтеграція соціальних сервісів, муніципальних варт та медичної допомоги у спільну цифрову систему з метою раннього виявлення загроз життю та здоров'ю вразливих верств населення в реальному часі.

Теоретичним підґрунтям соціально орієнтованого підходу є концепція людської безпеки, сформульована в Доповіді про людський розвиток Програми розвитку ООН 1994 р. [249]. Вона змістила акцент із безпеки територій на безпеку людей, а з озброєнь – на розвиток, і виокремила сім взаємопов'язаних вимірів безпеки: економічну, продовольчу, безпеку здоров'я, екологічну,

особисту, безпеку спільноти та політичну. Для проєктів «Безпечне місто» принципово, що особиста безпека, тобто захищеність від фізичного насильства, у цій концепції не відокремлюється від інших вимірів і розглядається як частина цілісної системи умов людського розвитку. Відповідно, система, яка фіксує правопорушення, але не впливає на соціальні чинники їх виникнення, забезпечує лише частковий рівень безпеки. На недооціненість соціального виміру в концепціях «розумного міста» вказують і дослідники, які характеризують соціальну політику як «забутий вимір» таких проєктів [256].

Другою теоретичною основою є запобігання злочинності засобами середовищного проєктування (Crime Prevention Through Environmental Design, CPTED). Цей підхід отримав міжнародне нормативне оформлення у стандарті ISO 22341:2021, який визначає базові елементи, стратегії та процеси запобігання злочинності й страху перед злочинністю в новому або наявному забудованому середовищі [221]. Стандарт використовує широке розуміння безпеки та адресований публічним і приватним організаціям незалежно від їх типу й розміру, що робить його придатним для муніципального управління. У межах цього підходу відеоспостереження є лише одним з інструментів поряд із плануванням публічних просторів, освітленням, забезпеченням природного нагляду (видимості вулиць із вікон будинків та з інших громадських місць), розмежуванням публічних і приватних територій та належним утриманням середовища. Тим самим міжнародна стандартизація підтверджує недостатність технократичного трактування «Безпечного міста» як мережі камер.

Поєднання цих двох підходів дає змогу визначити соціально орієнтовану модель «Безпечного міста» як систему, у якій ситуативні заходи (камери, освітлення, проєктування простору) доповнюються соціальними (послуги для вразливих груп, робота з громадами, підтримка ветеранів і постраждалих від насильства), а оцінювання результатів охоплює не лише кількість зафіксованих правопорушень, а й рівень страху перед злочинністю та доступність міського простору для всіх груп населення. Основою такого вимірювання можуть стати

опитування щодо суб'єктивного відчуття безпеки, результати яких уже використовуються для порівняння українських міст, як показано в підрозділі 2.3.

Пріоритетними напрямами взаємодії проєкту «Безпечне місто» та соціальної політики вважається інклюзія та безпека міського простору. Відеомоніторинг допомагає оцінювати доступність міської інфраструктури для маломобільних груп населення та швидко реагувати на аварійні ситуації, пов'язані з пересуванням людей з обмеженими можливостями чи літніх осіб. З метою зниження ризиків гендернозумовленого насильства здійснюється монтування освітлення та відеоспостереження у зонах парків, скверів та переходів, які не проглядаються камерами, патрулями або природним світлом через густі кущі, рельєф чи будівлі.

Доцільність поєднання освітлення з іншими заходами безпеки підтверджують доказові дослідження. Систематичний огляд, підготовлений для Кемпбеллівської співпраці на основі тринадцяти оцінювальних досліджень у США та Великій Британії, засвідчив, що покращення вуличного освітлення пов'язане зі статистично значущим зниженням злочинності в середньому на 21 % порівняно з контрольними територіями [254]. Показово, що злочинність у нічний час не знижувалася більшою мірою, ніж у денний; на думку авторів огляду, це свідчить про дію не лише механізму нагляду, а й механізму зміцнення гордості громади за свій простір і неформального соціального контролю. Рандомізований експеримент у Нью-Йорку, у межах якого в березні – серпні 2016 р. тимчасове освітлення випадковим чином розподілили між комплексами соціального житла, показав зниження нічної злочинності на вулицях щонайменше на 36 % [210]. Для українських громад, які в умовах енергетичних обмежень воєнного часу змушені скорочувати вуличне освітлення, ці дані мають практичне значення: освітлення небезпечних ділянок є самостійним інструментом безпеки, а не лише технічною умовою роботи камер, і потребує окремого пріоритету в програмах енергетичної стійкості громад.

Міжнародну рамку такої політики задають Цілі сталого розвитку. Завдання 11.7 передбачає до 2030 р. забезпечити загальний доступ до безпечних,

інклюзивних і доступних зелених та громадських просторів, насамперед для жінок і дітей, людей похилого віку та осіб з обмеженими можливостями; його виконання вимірюється, зокрема, індикатором 11.7.2 – часткою осіб, які протягом попередніх 12 місяців зазнали фізичних або сексуальних домагань, у розрізі статі, віку, статусу інвалідності та місця події [250]. Україна визначила Цілі сталого розвитку орієнтирами національної політики на період до 2030 року [31], тож цей індикатор може бути використаний як показник результативності соціально орієнтованих програм «Безпечне місто»: на відміну від кількості встановлених камер, він вимірює реальний досвід безпеки різних груп населення. Для моніторингу цього завдання UN-Habitat пропонує інструмент загальноміської оцінки публічних просторів, що дає змогу встановити базові показники й відстежувати прогрес, а також загальноміські стратегії розвитку публічних просторів [250].

Практичну модель реалізації цього підходу пропонує глобальна ініціатива UN Women «Безпечні міста та безпечні громадські простори», започаткована в листопаді 2010 р. п’ятьма програмами-засновницями в Кіто, Каїрі, Нью-Делі, Порт-Морсбі та Кігалі; згодом вона охопила понад 35 міст [240]. Ініціатива стала першою глобальною програмою, що розробляє, впроваджує та оцінює інструменти, політики й комплексні підходи до запобігання сексуальним домаганням та іншим формам сексуального насильства щодо жінок і дівчат у публічних просторах та реагування на них. Серед її результатів – зміни до місцевого нормативного регулювання в Кіто та запровадження аудитів безпеки жінок у містобудівне планування на рівні профільного міністерства Єгипту [240]. Для українських міст ця методологія сумісна з уже наявним досвідом аудитів безпеки територій, описаним вище, і може бути інтегрована до програм «Безпечне місто» як обов’язковий етап планування розміщення камер та освітлення.

Розвиток соціальної політики України у сфері протидії насильству спрямований на перехід від точкового реагування до створення загальнонаціональної людиноцентричної системи. Муніципальні ініціативи

проєктів «Безпечне місто» та регіональних програм «Міста і громади, вільні від домашнього насильства» інтегрують безпеку, соціальні послуги й екстрену допомогу на рівні кожного регіону [182]. «Міста і громади, вільні від домашнього насильства» – це масштабний проєкт Фонду ООН у галузі народонаселення (UNFPA) в Україні, спрямований на розбудову локальних систем запобігання та протидії гендерно зумовленому й домашньому насильству. Програма допомагає українським органам місцевої влади налагоджувати ефективну взаємодію між поліцією, соціальними службами, медиками та судами, а також створювати спеціалізовані сервіси підтримки для постраждалих. Проєкт стартував протягом 2020-2023 років у 15 містах-партнерах (серед яких Вінниця, Дніпро, Київ, Костянтинівка) і динамічно розвивається на території України. За даними Міністерства соціальної політики України [150], кількість учасників зросла до понад 53 міст та громад. У межах регіональних програм фінансується та реалізується:

- розвиток інфраструктури допомоги (створення притулків (шелтерів), кризових кімнат денного перебування, денних центрів та запуск мобільних бригад соціально-психологічної допомоги);
- організація комплексних навчальних тренінгів від місцевих фахівців щодо розпізнавання, превенції та координації дій під час реагування на випадки насильства [142]. Раннє виявлення та запобігання проявам домашнього чи гендерно зумовленого насильства (докладні практики описані у збірнику UN Women Ukraine [166]).

За підтримки міжнародних партнерів (зокрема, UNFPA Україна) на території країни функціонують інформаційні кампанії, метою яких є подолання терпимості до насильства та його попередження в умовах стресу та війни (наприклад, інформативна компанія «Що тут зайве?», що реалізується спільно з Міністерством соціальної політики).

Правовою основою інтеграції проєктів «Безпечне місто» з політикою протидії насильству є Закон України «Про запобігання та протидію домашньому насильству» від 07.12.2017 № 2229-VIII [15]. Він визначає систему суб’єктів, які

здійснюють заходи у цій сфері, – органи місцевого самоврядування, уповноважені підрозділи поліції, служби у справах дітей, суб'єктів надання соціальних послуг, спеціалізовані служби підтримки постраждалих осіб тощо, – і покладає на них обов'язок взаємодії. Ратифікація Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульської конвенції) Законом України від 20.06.2022 № 2319-IX [25] посилила ці зобов'язання: для України Конвенція набула чинності 1 листопада 2022 р. і вимагає забезпечувати постраждалим особам якнайкращий захист і підтримку, сприяти їх фізичному, психологічному та соціальному відновленню [181]. Отже, безпекова інфраструктура міст має бути підпорядкована не лише фіксації правопорушень, а й цим цілям.

Масштаб проблеми ілюструють дані Національної поліції, надані на інформаційний запит: у 2021 р. до поліції надійшло 325 599 звернень щодо домашнього насильства, у 2022 р. – 244 381, у 2023 р. – 291 428, у 2024 р. – 195 174, а за січень – травень 2025 р. – 53 606 звернень; у 2024 р. 6 545 звернень надійшло від неповнолітніх [77]. Динаміку цих показників не можна однозначно інтерпретувати як зміну рівня насильства, оскільки вона залежить також від готовності постраждалих звертатися по допомогу, доступності поліції в умовах війни та особливостей обліку. Саме тому для «Безпечного міста» важливими є не лише технічні засоби фіксації, а й канали звернення та маршрути перенаправлення: виклик поліції щодо домашнього насильства має ініціювати залучення соціальних служб, а дані про постраждалих – оброблятися в режимі обмеженого доступу.

Закон України «Про соціальні послуги» від 17.01.2019 № 2671-VIII [27] покладає на органи місцевого самоврядування визначення потреб населення громади в соціальних послугах та організацію їх надання. Тому інтеграція муніципальних безпекових систем із системою соціальних послуг є не додатковою опцією, а складовою повноважень громад: знеособлені дані ситуаційних центрів про повторювані виклики, кризові ситуації чи місця

концентрації ризиків можуть використовуватися для планування соціальних послуг, а не лише для розподілу патрулів.

В Україні реалізуються програми з урахуванням Резолюції Ради Безпеки ООН 1325. На Вінниччині реалізується Регіональний план дій з виконання резолюції Ради Безпеки ООН 1325 «Жінки, мир, безпека»: обласна військова адміністрація провела форум «Створюємо місцеві рішення разом: місцеві плани дій 1325» за участю органів влади, місцевого самоврядування та громадських організацій [155]. Український Жіночий Фонд застосовує власну методологію локалізації резолюції 1325 і сприяє створенню місцевих коаліцій, до яких входять представники правоохоронних органів, органів влади, громадських організацій, навчальних закладів і медіа [183]. На думку автора, такі ініціативи, зокрема аудити безпеки територій, тренінги з питань безпеки для працівників освіти та студентів і залучення молоді до розроблення рішень, доповнюють технічну складову проєктів «Безпечне місто» соціальною.

В Україні активно розвивається ініціатива «Цифрова інклюзія», в рамках якої здійснюється впровадження спеціалізованих інструментів, таких як україномовний додаток Digital Inclusion [167] для людей із порушеннями мовлення та розладами спектру аутизму. Зокрема, створено Digital Inclusion – перший україномовний мобільний застосунок та вебплатформу для соціалізації, розвитку й альтернативної комунікації. Додаток розроблено за ініціативи компанії «Хуавей Україна» у партнерстві з державними органами та громадськими організаціями. Він містить спеціальні символи та інструменти для людей, які потребують додаткової чи доповненої комунікації (зокрема дітей і дорослих із порушеннями мовлення). Застосунок є безкоштовним, його можна завантажити на офіційному сайті проєкту або через популярні магазини мобільних застосунків.

Цифрова інклюзія (Digital Inclusion) – це забезпечення рівного та безперешкодного доступу всіх людей до сучасних цифрових технологій, інтернету та навичок їх використання задля повноцінного життя в суспільстві. Поняття охоплює не лише технічну можливість виходу в мережу, а й здатність

користуватися електронними послугами, навчатися та працювати онлайн незалежно від віку, стану здоров'я чи місця проживання. Доступним є створення контенту, інтерфейсів і застосунків, якими можуть користуватися люди з особливими потребами або порушеннями комунікації.

Безбар'єрна інфраструктура передбачає поєднання систем відеомоніторингу й аналітики систем проєктів «Безпечне місто» з елементами інклюзивної навігації та міської мобільності. Державна програма «Цифрова інклюзія» спрямована на перенавчання та залучення людей з інвалідністю до економічно активного населення України шляхом здобуття цифрових професій (наприклад, у сфері кібербезпеки).

Напрями допомоги вразливим категоріям у межах концепції «Безпечне місто» охоплюють оперативний моніторинг і розшук, адресне реагування в кризових умовах та створення безпечних просторів. Швидке знаходження зниклих осіб за допомогою систем розпізнавання облич та відеоархівів. Перенаправлення сигналів з екстрених та муніципальних центрів безпосередньо до територіальних центрів соціального обслуговування. Розширення мережі безбар'єрних зон, притулків та центрів життєстійкості в громадах.

Міжнародно-правовим орієнтиром політики безбар'єрності є Конвенція про права осіб з інвалідністю, ратифікована Україною Законом від 16.12.2009 № 1767-VI [51]. Її ст. 9 зобов'язує держави забезпечувати особам з інвалідністю доступ нарівні з іншими до фізичного оточення, транспорту, інформації та зв'язку, а також до інших об'єктів і послуг, відкритих або наданих для населення, а ст. 11 – вживати всіх необхідних заходів для забезпечення їх захисту й безпеки в ситуаціях ризику, зокрема збройних конфліктів і надзвичайних гуманітарних ситуацій. На національному рівні ці зобов'язання конкретизовано в Національній стратегії із створення безбар'єрного простору в Україні на період до 2030 року, схваленій розпорядженням Кабінету Міністрів України від 14.04.2021 № 366-р [38]. Актуальність цих норм зростає з огляду на наслідки війни: за даними, які наводить Дослідницька служба Верховної Ради України з посиланням на Міністерство соціальної політики, від початку

повномасштабного вторгнення кількість осіб з офіційно встановленою інвалідністю зросла на 300 тис. і становить майже 3 млн [158].

Розрив між цими зобов'язаннями та практикою найбільш наочно виявляється в стані захисних споруд, які в умовах війни є критичним елементом безпеки міст. За результатами моніторингу Секретаріату Уповноваженого Верховної Ради України з прав людини, який у другому півріччі 2025 р. здійснив 1066 моніторингових візитів, рекомендації щодо усунення недоліків було надано для 991 об'єкта фонду захисних споруд, тобто для переважної більшості перевірених укриттів; найбільш критичною проблемою визначено їх недоступність для осіб з інвалідністю та інших маломобільних груп населення [176]. Це означає, що проєкти «Безпечне місто» мають охоплювати не лише моніторинг доступу до укриттів, а й достовірне інформування про їх фактичну доступність: цифрові мапи укриттів повинні містити дані про наявність пандусів, ширину проходів і режим роботи, а системи оповіщення – дублювати сигнали у звуковому й текстовому форматах.

Трансформація проєкту «Безпечне місто» Перехід від виключно поліцейських систем нагляду (камер з розпізнаванням облич) до комплексного захисту безпекового середовища та прав мешканців. Інтеграція у міську інфраструктуру регіональних можливостей та інформаційних платформ. Наприклад, портал Ветеран PRO [147] – це офіційна єдина державна цифрова платформа, створена Міністерством у справах ветеранів України спільно з Міністерством цифрової трансформації України, яка об'єднує всі доступні державні програми, послуги та соціальні гарантії для українських захисників, захисниць та їхніх сімей в одному місці. Простір функціонує як у форматі окремого вебпорталу Ветеран PRO, так і у вигляді інтегрованого цифрового розділу в застосунку Дія.

Організація безбар'єрних громадських територій, установ та об'єктів для психосоціальної реабілітації [40]. Наприклад, Ветеранський простір Чернігівської міської ради [195] – спеціалізована муніципальна установа,

створена для комплексної підтримки ветеранів війни, демобілізованих осіб, захисників та захисниць України, а також їхніх родин і сімей загиблих воїнів.

Інститут супроводу ветеранів в Україні – це державна програма та професійна служба, що забезпечує всебічну підтримку демобілізованих військових, ветеранів, ВПО та їхніх родин на рівні громад [45]. Офіційну заяву на участь у відборі або пошук послуг можна здійснити через платформу е-Ветеран [141]. Основні завдання Інституту ветеранів в Україні полягають у створенні умов для адаптації та безпечного середовища для людей, що постраждали від військових бойових дій, а саме у економічній адаптації та підтримка ВПО-ветеранів. У Інституті працюють спеціально підготовлені радники (фахівці із супроводу), які допомагають демобілізованим та їхнім родинам орієнтуватися в соціальних гарантіях, медичних послугах та юридичних аспектах. Запущено програми грантової підтримки підприємств, професійної перекваліфікації та бізнес-інкубаторів для ветеранів і ВПО. Розширення державної допомоги на оренду житла для захисників із числа переселенців, які не мають власної домівки [143]. На рівні українських міст впроваджується послуга підтриманого проживання за принципом «гроші ходять за людиною» (що в Україні означає те, що державні кошти на соціальні послуги виділяються не на утримання конкретних закладів чи інтернатів, а спрямовуються безпосередньо до людини, яка потребує допомоги).

Ветеранська політика стає одним із визначальних чинників соціального виміру безпеки українських міст. За даними Дослідницької служби Верховної Ради України, загальна чисельність ветеранів війни, членів родин загиблих та осіб з інвалідністю внаслідок війни перевищує 1,3 млн осіб [141]. Правовий статус і соціальні гарантії цих категорій визначає Закон України «Про статус ветеранів війни, гарантії їх соціального захисту» від 22.10.1993 № 3551-XII [29], а стратегічні орієнтири – Стратегія ветеранської політики на період до 2030 року, схвалена розпорядженням Кабінету Міністрів України від 29.11.2024 р. № 1209-р [46]. Порядок забезпечення діяльності фахівців із супроводу ветеранів війни та демобілізованих осіб затверджено постановою Кабінету Міністрів України від

02.08.2024 № 881 [45]. Цей інститут ґрунтується на клієнтоцентричному підході: фахівець визначає потреби особи, скеровує її до надавачів послуг і забезпечує супровід відповідно до протоколів, а цифровим каналом доступу до інформації про послуги є платформа «е-Ветеран»; у застосунку «Дія» згенеровано понад 415 тис. електронних посвідчень ветерана; у центрах надання адміністративних послуг для ветеранів та їхніх родин доступні 19 послуг, лише у 2024 р. надано понад 220 тис. таких послуг, зокрема понад 10 тис. витягів з Єдиного державного реєстру ветеранів війни [141].

Для проєктів «Безпечне місто» це має кілька практичних наслідків. По-перше, інфраструктура безпеки має враховувати потреби ветеранів з інвалідністю внаслідок війни: безбар'єрні маршрути до центрів надання послуг, реабілітаційних закладів і ветеранських просторів, доступність транспорту та укриттів.

По-друге, існує ризик, що алгоритми відеоаналітики, налаштовані на виявлення «нетипової поведінки», некоректно інтерпретуватимуть особливості пересування людей з ампутаціями чи наслідками травм; тому перед застосуванням таких алгоритмів потрібне їх тестування на відповідних сценаріях і обов'язковий людський контроль за реагуванням. По-третє, протоколи реагування на кризові ситуації за участю ветеранів, зокрема пов'язані з психологічною травмою, мають передбачати залучення фахівців із супроводу та психологів, а не лише поліції, що узгоджується з клієнтоцентричною моделлю супроводу.

Державна політика безбар'єрності в проєктах «Безпечне місто» поступово еволюціонує від традиційного відеоспостереження до інклюзивного середовища. Використання штучного інтелекту та відеоаналітики дозволяє завчасно виявляти небезпечні ситуації за участю вразливих верств населення на вулицях. Цифрові та інфраструктурні рішення охоплюють потреби маломобільних груп, ветеранів та літніх людей, гарантуючи рівний доступ до безпеки, укриттів і послуг. Проєкти «Безпечне місто» трансформуються з інструментів виключного відеоспостереження на ініціювання новітніх платформ соціального захисту та

підтримки вразливих категорій населення (літніх людей, маломобільних громадян, сімей з дітьми) завдяки інтеграції місцевих та державних служб реагування [38; 51; 151].

Окремою групою, інтереси якої мають бути враховані в соціально орієнтованих проєктах «Безпечне місто», є діти та молодь [128; 163]. Інституційною рамкою для цього є всесвітня ініціатива ЮНІСЕФ «Громада, дружня до дітей та молоді», що діє з 1996 р. і охоплює муніципалітети понад 30 країн; Україна приєдналася до неї у 2018 р., коли було підписано відповідний меморандум між Кабінетом Міністрів України, Дитячим фондом ООН (ЮНІСЕФ), Фондом ООН у галузі народонаселення, Асоціацією міст України та громадськими організаціями [148]. Громада може стати кандидатом на здобуття відповідного статусу лише після розроблення та офіційного ухвалення плану дій з реалізації ініціативи, а сам статус надається за результатами оцінювання ЮНІСЕФ виконання цього плану [124]. В Україні такий підхід має попередній досвід: у Вінниці ініціатива «Вінниця – місто, дружнє до дітей» реалізується з 2009 р. [130].

Безпека дітей у закладах освіти вже стала предметом окремої державної політики [133]. За інформацією МВС, План внутрішньої стійкості України передбачає, що в кожному закладі загальної середньої освіти має бути поліцейський, відповідальний за безпеку дітей, а безпека шкіл поєднує присутність фахівця з технічними засобами, зокрема тривожними кнопками виклику поліції, якими обладнано майже всі такі заклади. На початку 2025 р. інспекторами Служби освітньої безпеки було забезпечено майже 1200 шкіл [138]. За даними Міністерства освіти і науки, у червні 2025 р. офіцери цієї служби працювали вже в понад 1,6 тис. шкіл, а на наступний рік планувалося охопити до 3 тис.; в опитуванні, проведеному МВС на початку 2024 р. серед понад 350 тис. батьків, 70 % респондентів підтримали присутність таких офіцерів у школах [76]. За даними МВС, оприлюдненими в липні 2026 р., служба охоплює вже понад 1,4 млн учнів у 1915 закладах освіти [139]. Для «Безпечного міста» це означає, що шкільна безпека має бути інтегрована в загальноміську систему реагування:

тривожні кнопки, камери на прилеглій території та маршрути до укриттів мають працювати як єдиний контур.

Для «Безпечного міста» участь громади в цій ініціативі означає, що питання безпеки дітей – маршрути до закладів освіти, освітлення та облаштування дитячих і спортивних майданчиків, доступність укриттів у закладах освіти мають вирішуватися з урахуванням думки самих дітей і молоді, а не лише технічних нормативів. Водночас відеоспостереження в закладах освіти й на дитячих майданчиках порушує приватність неповнолітніх, тому рішення про його запровадження потребують особливо ретельного обґрунтування мети, обмеження доступу до записів і заборони їх оприлюднення без знеособлення, з урахуванням підходів, сформульованих у практиці ЄСПЛ, розглянутій у підрозділі 2.1.

В українських містах функціонують мережі спеціалізованих служб: денні центри соціально-психологічної допомоги, кризові кімнати, притулки (шелтери) та мобільні бригади [108; 171; 204]. У міських центрах також здійснюється захист вразливих груп населення, з акцентом на профілактику насильства та соціальний супровід ВПО й ветеранів. Інформаційні кампанії спрямовані на популяризацію відсутності толерантності до насильства серед мешканців українських міст. Органи місцевого самоврядування міст нашої країни співпрацюють, об’єднуючи ресурси для надання безперервної підтримки постраждалим незалежно від місця проживання. Інтеграція екстрених служб і соціального захисту передбачає поєднання місцевих платформ безпеки з державними лініями (наприклад, взаємодія служб МВС та Міністерства соціальної політики через гарячі лінії для адресної допомоги маломобільним та людям старшого віку). Цілодобово функціонують конфіденційні та безкоштовні лінії підтримки, серед яких Урядова гаряча лінія з попередження домашнього насильства за номером 15-47.

Важливим елементом соціальної інфраструктури безпеки в умовах війни стала психосоціальна підтримка населення [162; 186]. Постановою Кабінету Міністрів України від 03.10.2023 № 1049 затверджено Порядок реалізації

експериментального проєкту із запровадження комплексної соціальної послуги з формування життєстійкості [43], а постановою від 23.01.2024 № 83 – Порядок організації діяльності та забезпечення функціонування центрів життєстійкості [44]. Проєкт є складовою реалізації Концепції розвитку охорони психічного здоров'я в Україні на період до 2030 року та Всеукраїнської програми ментального здоров'я; станом на кінець березня 2025 р. до нього було залучено 308 громад у 23 областях, з яких 230 уже відкрили центри життєстійкості, а ще 54 громади приєдналися до проєкту [158]. Послуга поєднує первинну оцінку звернень і скринінг потреб людини з подальшим перенаправленням до фахівців, надання психосоціальних послуг, координацію волонтерської діяльності та підтримку родин, а серед її цілей визначено, зокрема, підвищення соціальної згуртованості територіальної громади та зміцнення волонтерського руху [158].

Для «Безпечного міста» мережа центрів життєстійкості є тим соціальним ресурсом, до якого доцільно перенаправляти людей після надзвичайних подій – обстрілів, пожеж, руйнувань, – коли технічна система вже зафіксувала інцидент, а екстрене реагування завершено. Інтеграція протоколів ситуаційних центрів із маршрутами перенаправлення до центрів життєстійкості дає змогу перейти від одноразового реагування до супроводу постраждалих, що відповідає сутності соціально орієнтованого підходу.

Проєкти «Безпечне місто» еволюціонують від виключно правоохоронних систем відеоспостереження до ініціювання новітніх платформ соціального захисту [89; 206]. Цифровізація послуг передбачає об'єднання комунальних та соціальних сервісів у єдині локальні мережі. У цьому контексті цифровізація послуг забезпечує адресну підтримку вразливих верств, зменшує паперову бюрократію, оптимізує бюджетні витрати та гарантує інклюзивну безпеку мешканців українських міст.

Ключові інструменти та ініціативи щодо цифровізації соціальних послуг охоплюють:

- адресні виплати (впровадження захищених безготівкових транзакцій для швидкого доступу громадян до пільг і допомог);

- електронні сервіси (оптимізація взаємодії мешканців українських міст із комунальними та соціальними службами через єдині міські платформи);
- переведення виплат і допомог в онлайн (зокрема, через платформи Міністерство соціальної політики);
- моніторинг ресурсів (прозоре управління бюджетом та контроль ефективності витрат на соціальну підтримку).

Цифровізація соціальних послуг в Україні має власну інституційну основу. Постановою Кабінету Міністрів України від 14.04.2021 № 404 затверджено Положення про Єдину інформаційну систему соціальної сфери (у редакції постанови від 27.10.2023 № 1130) [42], що стало кроком до практичної реалізації Стратегії цифрової трансформації соціальної сфери [193]. Положенням передбачено, зокрема, ведення випадку (кейс-менеджмент) як складову системи – оцінювання потреб особи чи родини в соціальних послугах, складання індивідуального плану, обмін інформацією між надавачами послуг і оцінювання результатів [107; 158; 257]. На цій основі Міністерство соціальної політики у співпраці зі Всесвітньою продовольчою програмою та ЮНІСЕФ реалізує цифровий проєкт «Електронний кейс-менеджмент»: його бета-тестування з липня 2024 р. проводилося у Вінницькій, Дніпропетровській, Полтавській та Черкаській областях (по 15 громад у кожній), а у вересні 2024 р. запрацював Соціальний портал електронних послуг міністерства; у листопаді 2024 р. проєкт увійшов до короткого списку премії Європейської соціальної мережі (European Social Services Awards) у категорії «Цифрова трансформація» [158]. Під час розгляду законопроєкту «Про Єдину інформаційну систему соціальної сфери» (реєстр. № 11377) у профільному комітеті Верховної Ради України представники міністерства пояснювали, що система побудована клієнтоорієнтовано – навколо соціальної картки людини та даних про особу і родину [178].

Такий підхід відкриває можливість інтеграції з безпековими платформами громад: сигнал про кризову ситуацію може співвідноситися з інформацією про соціальні послуги, які вже отримує особа чи родина, та з відповідальним фахівцем. Водночас поєднання даних про безпеку з даними про здоров’я,

інвалідність, насильство чи бідність створює підвищені ризики для приватності. Тому обмін даними між безпековими і соціальними системами має бути вибірковим: соціальні служби отримують інформацію, необхідну для надання допомоги, а правоохоронні органи – лише ту частину соціальних даних, без якої неможливе реагування на загрозу життю чи здоров'ю. Такий розподіл узгоджується з принципом мінімізації даних, на якому ґрунтуються європейські стандарти, розглянуті в підрозділі 2.1.

Окремим чинником ефективності цифрових сервісів є цифрові навички населення. За результатами третьої хвилі загальнонаціонального дослідження цифрової грамотності, проведеного з ініціативи Міністерства цифрової трансформації, частка дорослого населення з рівнем цифрових навичок нижче базового у 2023 р. становила 53 % [145], тоді як за результатами першого дослідження 2019 р. цей показник складав 40,4 % [160]. Це означає, що в рамках проєктів «Безпечне місто» існує необхідность в подальшому зберігати нецифрові канали – телефонні лінії, кнопки виклику, особисті звернення до фахівців – і не робити цифровий доступ єдиною умовою отримання допомоги. Отже, попри позитивну динаміку показників розвитку цифрової грамотності, значна частина мешканців українських міст не може повною мірою користуватися мобільними застосунками безпеки та соціальними онлайн-сервісами.

Еволюція проєктів «Безпечне місто» трансформує соціальну політику державного управління: від вузького правоохоронного нагляду до новітньої платформи соціального захисту. Перехід від ліквідації наслідків до попередження загроз спирається на цифрову інфраструктуру, яка гарантує безпеку як базову потребу українського суспільства. Проєкти «Безпечне місто» трансформуються з інструментів відеоспостереження на новітні платформи соціального захисту. Інтеграція екстрених служб і соціальних відомств у єдиний цифровий простір дозволяє державі переходити від запізнілої реакції на кризові випадки до запобігання надзвичайним ситуаціям та підтримки вразливих груп населення в реальному часі [26; 151].

Трансформація державної соціальної політики в контексті концепції «Безпечне місто» передбачає зміну фокусування від виключно правоохоронного нагляду до інклюзивного та захищеного міського середовища. Об'єднання зусиль фахівців місцевого самоврядування, поліції, ДСНС разом з використанням штучного інтелекту та відеоаналітики для виявлення ризиків для життя й здоров'я громадян українських міст.

Трансформація соціальної політики під впливом реалізації проєктів «Безпечне місто» передбачає перехід від реагування на надзвичайні події постфактум до запобігання ризикам за допомогою штучного інтелекту. Використання великих даних (Big Data) застосовується для вивчення та аналітики запитів або потреб соціальних груп українських міст. Формування безбар'єрного середовища здійснюється шляхом інтеграції інклюзивних цифрових рішень та архітектурних вимог для маломобільних груп населення. Здійснюється переорієнтація міської інфраструктури на потреби травмованих осіб та людей з інвалідністю. Фізична доступність лікарень, ЦНАПів та транспортних зупинок забезпечується облаштуванням безбар'єрних маршрутів. Цифровізація доступу до інформації щодо укриттів передбачає об'єднання даних про захисні споруди з інструментами Мапи безбар'єрності [146].

Інтеграція екстрених служб і служб соціального захисту дозволила сформувати оперативні ситуаційні центри. Забезпечується швидкий обмін даними між диспетчерами служби 101, 102, 112 та підрозділами соціального забезпечення. Адресна допомога в реальному часі означає миттєве залучення соціальних працівників або кризових реабілітологів у випадках домашнього насильства, бездомності чи нещасних випадків на вулиці. Моніторинг громадських просторів задля виявлення вразливих категорій (осіб похилого віку, дітей або людей з інвалідністю), які потребують захисту, екстреної медичної чи соціальної допомоги.

Правовою основою такої інтеграції є Закон України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» від 13.03.2012 № 4499-VI [26], яким передбачено створення центрів екстреної

допомоги населенню за номером 112, оперативно-диспетчерських служб і підрозділів екстреної допомоги, що працюють у межах єдиної системи. Практичне впровадження системи тривалий час відставало від законодавчих рішень, однак станом на початок 2026 р., за даними, які наводять громадські організації з посиланням на МВС, служба 112 опрацювала понад 10,5 млн викликів, а звернутися до неї можна також через мобільний застосунок; У 2026 р. служба охоплює всю територію країни [157]. За даними МВС, у грудні 2025 р. запрацював мобільний застосунок «112 Ukraine», доступний навіть за відсутності мобільного зв'язку, а впродовж року оператори служби опрацювали понад 6,4 млн звернень [139]. Подальший розвиток системи пов'язаний із проєктом «Впровадження системи екстреної допомоги населенню за єдиним телефонним номером 112 з урахуванням потреб осіб з інвалідністю», фінансову угоду щодо якого з Європейським інвестиційним банком Президент України вніс на ратифікацію до Верховної Ради (реєстр. № 0364 від 03.02.2026) [165].

Для «Безпечного міста» значення має передусім те, що єдиний номер створює точку входу, через яку безпекові й соціальні сценарії можуть поєднуватися: виклик щодо домашнього насильства, зникнення людини похилого віку чи кризового стану ветерана має передаватися не лише поліції, а й відповідній соціальній службі громади. Технічною передумовою цього є сумісність диспетчерських систем громад із системою 112, а організаційною – затверджені маршрути перенаправлення та розподіл відповідальності між службами. Включення вимог доступності для осіб з інвалідністю до самого проєкту модернізації системи 112 є прикладом того, як соціальна політика може бути закладена в технічну архітектуру безпеки ще на етапі проєктування.

Розвиток державної соціальної політики через концепцію «Безпечне місто» та програму «Цифрова інклюзія» передбачає перехід від базового фізичного захисту до створення рівного, безбар'єрного й доступного цифрового простору для всіх мешканців. Партнерська співпраця держави, громадських організацій та соціально відповідальних підприємств дозволила сутнісно та цільово інтегрувати вразливі групи (людей з інвалідністю, літніх громадян,

невербальних пацієнтів) у загальне системне середовище міської безпеки. Досягнуто подолання «цифрового розриву» та забезпечення рівного доступу до сучасних е-послуг і засобів комунікації.

Сучасна соціальна політика України еволюціонує від точкової допомоги до людиноцентричних муніципальних проєктів, де концепція «Безпечне місто» розширюється з технократичного відеоспостереження до створення безпечного та інклюзивного середовища, просторової інтеграції, а також адміністрування якісного супроводу ветеранів і внутрішньо переміщених осіб (ВПО) [79; 91; 112].

Соціально орієнтований підхід до безпеки має і власне поліцейське втілення – модель поліцейської діяльності, орієнтованої на громаду. В Україні її реалізує проєкт «Поліцейський офіцер громади»: поліцейський офіцер громади – це офіцер Національної поліції, який живе та працює в певній територіальній громаді; за оцінкою керівництва МВС. Саме до таких офіцерів громадяни мають найвищий рівень довіри серед представників поліцейської професії, а реалізація проєкту ґрунтується на співпраці з органами місцевого самоврядування, багато з яких, зокрема, забезпечили офіцерів службовим транспортом [131]. Поєднання цієї моделі з технічними засобами «Безпечного міста» змінює логіку використання камер: відеодані стають інструментом розв’язання конкретних проблем громади, які офіцер визначає разом із мешканцями, а не лише джерелом доказів після вчинення правопорушення. Для малих громад, які не мають ресурсів на розгорнуті аналітичні системи, постійна присутність офіцера громади в поєднанні з базовим відеоспостереженням у ключових точках може бути реалістичною моделлю «Безпечного міста», співмірною з їхньою спроможністю, що детальніше розглянуто в підрозділі 2.3.

Проєкт «Безпечне місто» перестав бути суто поліцейською чи комунальною програмою. Завдяки гнучким підходам та інтеграції штучного інтелекту він трансформувався у платформу для соціальної роботи, яка спрямована на гарантування безпеки як базової потреби українських громадян. Попри, значний потенціал можна виділити кілька критичних проблем впровадження проєктів «Безпечне місто». Принципи інформаційної безпеки та

приватності вимагають від представників місцевих органів влади суворого дотримання прав людини під час збору, збереження та аналізу персональних даних. Представники влади часто працюють без належного документального оформлення та чітких регламентів правового регулювання доступу до даних.

Соціальна орієнтація «Безпечного міста» вимагає окремої уваги до ризиків, які технології спостереження створюють саме для вразливих груп. Дослідження Національного інституту стандартів і технологій США, яке охопило алгоритми розпізнавання облич значної кількості розробників, засвідчило, що частота хибних збігів у різних демографічних групах часто відрізняється в 10–100 і більше разів; хибних збігів більше щодо жінок, ніж щодо чоловіків, а також щодо людей похилого віку та дітей, причому ефект найбільший для найстарших і наймолодших [216]. Отже, саме ті групи, яких соціально орієнтований підхід має захищати, частіше за інших можуть ставати об'єктами помилкової ідентифікації. Крім того, ЄСПЛ у справі «Глухін проти Росії» наголосив, що застосування високоінтрузивних технологій розпізнавання облич може мати стримувальний ефект [59]; за аналогією можна припустити, що для вразливих груп таким ефектом стане відмова від звернення по допомогу або від відвідування публічних просторів, де діє біометричне спостереження.

Ще одним ризиком є так зване розширення функцій, коли дані, зібрані для соціальної підтримки (про звернення щодо насильства, інвалідність, психологічний стан), згодом використовуються для контролю чи профілактичного обліку. Довіра вразливих груп до системи, без якої вони не звертатимуться по допомогу, залежить від чітких меж використання таких даних. З огляду на це соціально орієнтовані програми «Безпечне місто» мають передбачати:

- оцінку впливу на рівність до запровадження аналітичних функцій (недотримання обов'язку щодо рівності стало однією з підстав визнання незаконним застосування розпізнавання облич у справі Bridges, розглянутій у підрозділі 2.1 [61]);

- участь організацій, що представляють інтереси осіб з інвалідністю, ветеранів, постраждалих від насильства, дітей і молоді, у визначенні місць розміщення камер та правил використання даних;
- заборону використання соціальних даних для цілей, не пов'язаних із наданням допомоги, без окремої правової підстави;
- зрозуміле інформування мешканців про те, які дані збираються, з якою метою і хто має до них доступ.

2.3. Характеристика рівня управління українськими населеними пунктами при реалізації проєктів «Безпечне місто»

Управління українськими населеними пунктами під час реалізації проєктів «Безпечне місто» характеризується переходом від фрагментарного реагування до інтегрованого цифрового публічного управління в умовах децентралізації та воєнного стану. Представники влади українських міст є головним замовником та координатором безпекових систем, об'єднуючи зусилля комунальних служб, Національної поліції та ДСНС [95; 234].

Управлінський процес при реалізації концепції «Безпечне місто» поєднує два вектори: вертикально-горизонтальна структура координації. При горизонтальному рівні управління представники органів місцевого самоврядування забезпечують фінансування з місцевих бюджетів, закупівлю серверного обладнання та встановлення відеокамер з використанням інструментів штучного інтелекту. Вони ж координують інтеграцію відеопотоків для потреб ЖКГ, екологічного моніторингу та контролю за трафіком [95]. Вертикальний рівень управління означає те, що дані з муніципальних систем інтегруються до Ситуаційних центрів Головних управлінь Національної поліції та ДСНС. Це дозволяє забезпечити оперативне реагування, автоматичне розпізнавання номерних знаків чи облич та швидке розкриття правопорушень [111].

Правову основу такої вертикально-горизонтальної взаємодії становлять кілька рівнів регулювання. Повноваження виконавчих органів сільських, селищних і міських рад щодо забезпечення законності, правопорядку, охорони прав, свобод і законних інтересів громадян визначено ст. 38 Закону України «Про місцеве самоврядування в Україні» [19], тоді як право поліції застосовувати фото- і відеотехніку, у тому числі таку, що працює в автоматичному режимі, закріплено ст. 40 Закону України «Про Національну поліцію» [21]. Проте жоден із цих актів не розмежовує ролей власника камер та розпорядника персональних даних і користувачів відеоінформації, що й зумовлює правову невизначеність, про яку йдеться нижче.

Інституційним підґрунтям муніципальних проєктів «Безпечне місто» стала реформа децентралізації. За оцінкою ОЕСР, реформи регіонального розвитку та децентралізації, що впроваджувалися з 2014 р., призвели до об'єднання понад 10 тис. місцевих рад у 1469 громад із новими повноваженнями, а публічне фінансування регіонального та місцевого розвитку у 2015–2019 рр. у реальному вимірі зросло втричі; понад 70 % громад, опитаних ОЕСР до війни, повідомили про покращення якості адміністративних і соціальних послуг [238]. Водночас ОЕСР констатувала значні відмінності між громадами в адміністративній, кадровій та фінансовій спроможності, які війна суттєво поглибила [234]. Саме ці відмінності визначають, на якому рівні управління – початковому, аналітичному чи інтегрованому – здатна функціонувати система «Безпечне місто» в конкретній громаді.

Додатковий вимір багаторівневості створює воєнний стан. У частині громад повноваження органів місцевого самоврядування здійснюють військові адміністрації, утворені відповідно до Закону України «Про правовий режим воєнного стану» [24], а користувачами інтегрованих платформ є також сили безпеки й оборони. За таких умов система «Безпечне місто» функціонує щонайменше в трьох площинах – муніципальній (власник інфраструктури), правоохоронній (основний користувач даних) і оборонній (користувач в інтересах національної безпеки). Без чіткого законодавчого розподілу ролей

кожна з них діє на підставі власних актів, що ускладнює і контроль за законністю доступу до даних, і відповідальність за його порушення.

Рівень управління населеними пунктами при реалізації проєктів «Безпечне місто» суттєво варіюється залежно від масштабу населеного пункту та наявної ІТ-інфраструктури – від початкового (оглядового) до високого рівня (інтегрованого).

Початковий (оглядовий) рівень означає, що у місті лише встановлюються камери без належного аналітичного програмного забезпечення та чіткого регламенту збереження даних. Відео використовується як постфактум для фіксації інцидентів.

Середній (аналітичний) рівень характеризується впровадженням інтелектуальних систем відеоаналітики (розпізнавання облич, детекція швидкості, фіксація маркерів небезпеки). На цьому етапі управління населеними пунктами при реалізації проєктів «Безпечне місто» стає проактивним [85].

Найпоширенішим прикладом аналітичного рівня є автоматична фіксація порушень правил дорожнього руху [3]. За даними МВС, лише впродовж одного року встановлено 100 нових комплексів автофіксації та облаштовано 14 нових ділянок контролю середньої швидкості, загальна кількість яких сягнула 335; за той цей же період кількість загиблих у дорожньо-транспортних пригодах зменшилася на 5 %, травмованих – на 2,4 %, а пригод із постраждалими – на 2,2 % [139]. Ці показники відображають позицію відомства, а зменшення аварійності має багатофакторну природу, проте сам підхід – оприлюднення результатів поряд із показниками запровадження технології є прикладом того, як рівень управління може оцінюватися через результати, а не лише через кількість встановленого обладнання.

Водночас перехід на аналітичний рівень змінює правову природу системи. Як показано в підрозділі 2.1, Федеральний конституційний суд Німеччини визнав автоматизовану перевірку номерних знаків втручанням в основні права навіть тоді, коли збіг не виявлено, і вимагав, щоб її підстави, мета та межі були чітко визначені законом [64]. Отже, кожна нова аналітична функція

(розпізнавання номерних знаків, облич, поведінкова аналітика) має запроваджуватися як окреме управлінське рішення з власним правовим обґрунтуванням, а не як технічне оновлення програмного забезпечення.

Високий (інтегрований) рівень передбачає створення повноцінних ситуаційних центрів. У цьому випадку концепція «Безпечне місто» функціонує як інтеграційний інструмент сталого розвитку, поєднуючи різні платформи цифрових інструментів кіберзахисту [85; 95].

Наведена трирівнева характеристика може бути операціоналізована за допомогою міжнародних стандартів. Першим міжнародно стандартизованим набором міських показників став ISO 37120, уперше опублікований у 2014 р., який згодом доповнили стандарти показників «розумних» і стійких міст [244]. Стандарт ISO 37106 пропонує модель «розумного» операційного управління містом – набір практик спільного й цифрово підтриманого управління врядуванням, послугами, даними та системами в масштабі всього міста [244]. Стандарт ISO 37122:2019 встановлює визначення та методики показників «розумного міста», які разом із показниками ISO 37120 утворюють повний набір для вимірювання прогресу [222], а ISO 37123:2019 – показники стійкості міст, придатні для будь-якого міста, муніципалітету чи органу місцевого самоврядування, незалежно від їх розміру й розташування, з метою порівнюваного та перевірного вимірювання результатів [223]. Для «Безпечного міста» це означає, що перехід від початкового до інтегрованого рівня має фіксуватися не кількістю камер, а сукупністю показників управління даними, послугами та стійкістю.

В Україні вже існує національний інструмент подібного вимірювання. Міністерство цифрової трансформації запровадило Індекс цифрової трансформації регіонів, який оновлюється щоквартально й охоплює п’ять груп показників (цифрова економіка, цифрові навички, цифрова інфраструктура, цифровізація публічних послуг і цифровізація територіальних громад), а також Індекс цифрової трансформації територіальних громад із чотирма групами показників [135]. За результатами І кварталу 2025 р. середнє значення індексу

регіонів становило 30 балів зі 100, а громад – лише 16; серед регіонів лідирували Дніпропетровська, Львівська (по 43 бали) та Тернопільська (42 бали) області, а серед громад – Криворізька (62,97), Вінницька (62,75), Тернопільська (60,35), Львівська (55,61) та Харківська (54,57) [87]. За підсумками 2025 р. лідерами стали Львівська область серед тилових регіонів і Дніпропетровська серед прифронтових, а міністерство повідомило про доопрацювання методики з урахуванням відмінностей між цими двома групами регіонів [152].

Водночас окремої групи показників щодо безпекових систем громад (стан відеомоніторингу, кіберзахист, інтеграція з екстреними службами) у структурі цих індексів немає. Її запровадження могло б стати інструментом державного моніторингу рівня управління проєктами «Безпечне місто», оскільки дало б змогу порівнювати громади за єдиною методикою, а не на підставі фрагментарних даних окремих муніципальних програм.

Сучасний етап реалізації проєктів «Безпечне місто» в Україні накладає особливо специфічні вимоги до муніципального менеджменту в умовах воєнного стану. Проєкти «Безпечне місто» адаптуються для швидкого відновлення зв'язку під час обстрілів та забезпечення стабільного захисту критичної інфраструктури. Оскільки системи відеонагляду є вразливими до ворожих кібератак, рівень управління вимагає суворих протоколів захисту даних та обмеження доступу. До систем «Безпечне місто» активно інтегрують моніторинг об'єктів цивільного захисту, укриття, автоматизацію систем оповіщення населення, організовуючи координацію з Центрами безпеки [156].

Особливої ваги в цих умовах набуває кіберуправління муніципальними системами [106]. Показовим є випадок, оприлюднений СБУ на початку січня 2024 р.: під час масованої атаки на Київ російські спецслужби отримали доступ до двох вуличних вебкамер, змінили кут їх огляду та підключили до стримінгової платформи, використовуючи для збору даних із метою коригування ударів; загалом від початку повномасштабного вторгнення кіберфахівці СБУ заблокували близько 10 тис. IP-камер, які могли бути використані противником [118]. СБУ наголосила, що публікація подібних відеоматеріалів розцінюється як

коригування ворожого вогню і є злочином [173]. Отже, кожна камера, підключена до мережі, – муніципальна чи приватна – є потенційною точкою атаки, а захищеність системи визначається її найслабшим елементом.

Із цього випливають управлінські вимоги, які доцільно закріпити в типових регламентах відповідно до засад, визначених Законом України «Про основні засади забезпечення кібербезпеки України» [23]: ведення реєстру всіх пристроїв, підключених до міської системи; заборона публічних трансляцій [161] і обов'язкова заміна заводських паролів; відокремлення мереж відеоспостереження від інших мереж громади; журналювання доступу; узгоджені з уповноваженими органами процедури реагування на кіберінциденти; урахування походження обладнання під час закупівель, про що йшлося в підрозділі 2.1. Для приватних камер, які інтегруються в міські мережі, дотримання цих вимог має бути умовою підключення.

На загальнодержавному рівні інтегрований підхід уже реалізується в системі цивільного захисту: за даними МВС, у системі ДСНС створено Державний центр управління в надзвичайних ситуаціях із цифровими інструментами, що дають змогу моніторити радіаційну, гідрометеорологічну та сейсмічну обстановку, аналізувати супутникові дані для раннього виявлення пожеж, прогнозувати наслідки загроз і координувати сили реагування, а систему оповіщення модернізовано з переходом до диференційованого оповіщення про повітряні тривоги на рівні районів [139]. Сумісність муніципальних ситуаційних центрів із цією системою є необхідною умовою, щоб «Безпечне місто» стало складовою національної системи стійкості, а не відокремленою міською ініціативою.

Попри наявність ефективно реалізованих проєктів багатьох українських міст (Тернополя, Києва, Рівного), в управлінні населеними пунктами при реалізації проєктів «Безпечне місто» часто виникають проблеми правової неврегульованості та обмеженості фінансування [126; 184; 234]. Муніципальні системи працюють за локальними програмами, оскільки єдині загальнодержавні

стандарти для систем відеоконтролю та захисту персональних даних із залученням штучного інтелекту потребують доопрацювання.

Спроби врегулювати цю сферу на загальнодержавному рівні робилися й раніше, однак, як показано в підрозділі 2.1, цілісної законодавчої рамки для систем відеомоніторингу так і не було створено. Новим етапом стало створення Єдиної системи відеомоніторингу стану публічної безпеки. За повідомленням МВС, до неї планувалося під'єднати 50 тис. камер, із яких 8 тис. на момент повідомлення вже було інтегровано, а правила розміщення камер, доступу до інформації та централізованого контролю за її захистом мав визначити закон [129]. Відповідний законопроєкт «Про єдину систему відеомоніторингу стану публічної безпеки» (реєстр. № 11031 від 20.02.2024) передбачає вимоги до побудови та функціонування систем відеомоніторингу центрального, регіонального та місцевого рівнів, а також відомчих систем підприємств, установ, організацій і фізичних осіб, установлених у публічних місцях, порядок доступу до інформації та захисту персональних даних [184]. Користувачами системи визначено уповноважених осіб сил безпеки та сил оборони, органів державної влади й органів місцевого самоврядування, яким у встановленому порядку надано права доступу [126].

Водночас аналітики звертали увагу, що законопроєкт чітко не визначає, хто саме матиме право доступу до інформації з камер [126]. З огляду на практику, розглянуту в підрозділі 2.1, саме це питання є визначальним: у справі Bridges незаконність застосування розпізнавання облич зумовила надмірна свобода розсуду щодо того, хто і де може бути об'єктом спостереження [61], а в справі «Глухін проти Росії» ЄСПЛ вимагав детальних правил щодо сфери застосування технологій, процедур дозволу, використання і зберігання даних та механізмів нагляду [59]. Отже, державний рівень запровадження «Безпечного міста» має полягати не лише в технічній інтеграції муніципальних камер у систему МВС, а насамперед у законодавчому визначенні кола користувачів, цілей обробки, строків зберігання, порядку застосування біометричних функцій і незалежного

нагляду. Без цього інтеграція лише перенесе наявні ризики з муніципального на загальнодержавний рівень і збільшить їх масштаб.

Органам місцевого самоврядування не вистачає кваліфікованих IT-фахівців та менеджерів цифрової трансформації, що наразі частково вирішується через освітні програми.

В Україні діють інші освітні ініціативи та платформи для розвитку цифрових лідерів, державних службовців і фахівців у сфера IT, які створюють цифрові рішення, сервіси та програмне забезпечення для державного сектору та покращення взаємодії громадян з владою. Аналогічні ініціативи та платформи схожі за концепцією на CDTO Campus (перший у світі національний освітній проєкт і повноцінна освітня платформа для підготовки команд цифрових лідерів, які впроваджують інноваційні технологічні проєкти в державному та місцевому управлінні та місцях) [192].

Аналогічною українською ініцітивою є Дія. Освіта – національна платформа верифікованого навчання, де можна знайти серіали та гайди щодо цифровізації, кібербезпеки і штучного інтелекту. Лідерські програми, наприклад, Школа державного управління часто реалізуються за підтримки міжнародних фондів та урядових проєктів. Наприклад, Фонду Східої Європи [191] як провідна українська благодійна неприбуткова організація. AI HOUSE та партнерські IT-академії проводять короткотривалі та глибокі технічні програми з використання штучного інтелекту й аналізу даних для публічного та приватного секторів. CISO Campus/GovTech факультет пропонує спеціалізовані напрями всередині системи цифровізації для вивчення кіберзахисту й управління IT-проєктами.

Інституційною відповіддю на кадровий дефіцит стало запровадження мережі керівників цифрової трансформації (CDTO). Станом на березень 2023 р. CDTO працювали в 17 міністерствах, 21 центральному органі виконавчої влади та 16 обласних військових адміністраціях, а метою Мінцифри було визначено наявність CDTO в усіх органах державної влади та цифрових лідерів в усіх територіальних громадах [153]. Восени 2023 р. міністерство запустило національний проєкт із навчання лідерів цифрової трансформації CDTO Campus,

а серед регіонів за кількістю реалізованих проєктів цифрової трансформації лідирували Дніпропетровська (58 проєктів), Черкаська (24) та Закарпатська (21) області [192]. До платформи «Дія. Цифрова громада», за даними міністерства, долучилося понад 950 цифрових лідерів громад [154].

Водночас наявність цифрового лідера ще не забезпечує спроможності експлуатувати безпекові системи. Для «Безпечного міста» потрібні окремі компетенції – оператори моніторингу, адміністратори мереж, фахівці з кібербезпеки та захисту персональних даних, – чисельність яких має відповідати масштабу системи [88]. Тому державні вимоги до рівнів управління доцільно доповнити кадровими нормативами (кількість операторів і адміністраторів залежно від кількості камер і режиму моніторингу), а програми навчання CDTO – модулем з управління безпековими системами громад.

Українські міста можна розділити на категорії за рівнем фінансової спроможності для впровадження смарт-технологій: великі міста-мегаполіси та обласні центри (з високим рівнем спроможності) та невеликі міста, районні центри та селища (з низьким рівнем спроможності). Невеликі міста та селища обмежені у фінансуванні, тому, зазвичай, неспроможні самостійно розгорнути дорогі аналітичні комплекси (наприклад, повноцінні платформи проєктів «Безпечне місто» [182] зі штучним інтелектом) і часто обмежуються точковим встановленням базових камер відеонагляду. Така ситуація є поширеною через фінансову та інфраструктурну нерівність.

Адміністрації міст Києва, Дніпра, Львова, Одеси, Кривого Рогу, Житомира, Чернігова мають достатньо коштів у місцевих бюджетах, залучаючи міжнародні гранти та допомогу органів МВС та Національної поліції. Вони встановлюють тисячі камер, організовують великі Центри обробки даних, ситуаційні кімнати та купують дорогу відеоаналітику (модулі розпізнавання облич, автомобільних номерів, фіксації трафіку й виявлення порушень).

Навіть у фінансово спроможних містах рівень управління визначається не лише бюджетом. Показовим є досвід Львова, описаний працівником профільного управління міської ради: система «Безпечне місто Львів»

розвивається в межах Міської комплексної програми зміцнення законності, безпеки та порядку на 2022–2026 роки; у 2016 р. вона налічувала 50 камер, а станом на 2024 р. – понад 2000, включно з камерами з аналітичними функціями, розпізнаванням облич і номерних знаків та тепловізійним виявленням пожеж [111]. У 2024 р. за допомогою системи було встановлено 1540 винуватців дорожньо-транспортних пригод і виявлено 506 порушень громадського порядку, опрацьовано 644 запити Національної поліції на отримання відеозаписів, а випадків оперативної співпраці з патрульною поліцією зафіксовано 28 734; окремо в межах програми «Безпека житлових кварталів» встановлено 101 оглядову камеру у восьми об'єднаннях співвласників багатоквартирних будинків [111].

Водночас той самий досвід засвідчує інституційні обмеження: дві штатні одиниці, які у 2016 р. обслуговували 50 камер, і у 2024 р. відповідали за понад 2000 камер, а приміщення центру безпеки потребувало розширення через перевантаження застарілої електропроводки [111]. Отже, перехід міста на інтегрований рівень за технічними параметрами може не супроводжуватися відповідним зростанням кадрової та інфраструктурної спроможності, що підтверджує потребу в кадрових і технічних нормативах для кожного рівня. Крім того, застосування функції розпізнавання облич муніципальною системою за відсутності спеціального законодавчого регулювання, про яку йшлося в підрозділі 2.1, становить правовий ризик навіть для успішних міських проєктів.

На думку автора, що ґрунтується на сукупному аналізі джерел, бюджетні кошти невеликих містечок, сіл та селищ без великих промислових підприємств здебільшого спрямовані на утримання комунальної інфраструктури та соціальні потреби. Адміністрація таких міст виділяє бюджет лише на кілька десятків (або навіть одиниць) звичайних камер, які ставлять точково на в'їздах до населеного пункту, біля сільради чи на центральній площі. Ці камери просто записують відео в архів на звичайний сервер (або SD-карти), не маючи функцій штучного інтелекту.

Невеликі міста характеризуються низьким рівнем спроможності в реалізації проєктів «Безпечне місто». Бюджет вимагає закупівлі якісної IP-камери та ліцензії на аналітичне програмне забезпечення для кожної камери (наприклад, штучний інтелект для пошуку за силуетом). Вартість камер та обладнання в системі «Безпечне місто» залежить від масштабу проєкту, кількості точок спостереження та функціоналу (наприклад, розпізнавання номерів чи облич). У середньому ціна за один проєкт або закупівлю суттєво різниться по містах та громадах України. Узагальнення доступних даних дає змогу автору дійти висновку, що вартість таких рішень коливається від сотень тисяч гривень за закупівлю окремих партій камер до десятків мільйонів гривень за розгортання міських систем, а поточне обслуговування вже наявного обладнання потребує окремих щорічних видатків. Так, в Ужгороді у 2019 р. було придбано 44 відеокамери загальною вартістю 803 тис. грн, а станом на червень 2020 р. у місті було встановлено 164 камери [120]. У місті Миколаєві за п’ять років будівництва системи відеонагляду та відеоаналітики «Безпечне місто» спрямували 60,7 млн грн [188]; за оцінкою автора, в інших громадах вартість розширення мережі на кількасот сучасних камер може сягати 90 млн грн. Ці оцінки частково ґрунтуються на повідомленнях медіа; для їх перевірки та порівняння цін на однотипне обладнання між громадами доцільно використовувати первинні дані про конкретні закупівлі в електронній системі публічних закупівель Prozorro.

Ринок обладнання та послуг для систем «Безпечне місто» характеризується високою концентрацією, що створює ризики для конкурентності закупівель. Так, за повідомленням ЗМІ, у 2024 р. в закупівлі послуг з обслуговування камер відеоспостереження у Львові вартістю понад 4,3 млн грн узяв участь лише один учасник – компанія, яка реалізує програми «Безпечне місто» також у Києві, Одесі, Дніпрі та інших містах і посідає перше місце за кількістю виграних тендерів на встановлення та обслуговування систем відеоспостереження в громадах; при цьому вона використовує обладнання виробника, внесеного до переліку «міжнародних спонсорів війни» [144]. Цей приклад ілюструє одразу дві

проблеми, розглянуті вище: технологічну прив’язку громад до постачальника та безпекові ризики походження обладнання.

Організація економічного співробітництва та розвитку (ОЕСР) серед пріоритетів післявоєнного відновлення рекомендує посилювати спроможність громад у сферах стратегічного планування, оцінювання проєктів, закупівель і прозорості, спрощувати механізми фінансування регіонального розвитку, щоб уникати надмірного розпорошення ресурсів, а також запроваджувати національні та місцеві механізми прозорості використання коштів на відновлення [238]. Для «Безпечного міста» це означає необхідність оцінювати повну вартість володіння системою (встановлення, обслуговування, оновлення програмного забезпечення, ліцензії, кіберзахист) ще на етапі планування, поділяти закупівлі на лоти з метою розширення конкуренції, вимагати відкритих протоколів і сумісності обладнання, а також оприлюднювати дані про вартість і результати програм. Наведені вище приклади, коли обслуговування наявної системи коштує сотні тисяч гривень на рік, свідчать, що для невеликих громад саме експлуатаційні витрати, а не первинне встановлення, є головним бар’єром для переходу на вищий рівень управління. Одним із механізмів розширення мереж без надмірного навантаження на місцевий бюджет є співфінансування з об’єднаннями співвласників багатоквартирних будинків, як у львівській програмі «Безпека житлових кварталів» [111]. Паралельно такі камери мають підключатися до міської системи лише за умови дотримання вимог щодо кібербезпеки та захисту персональних даних.

У невеликих містечках, селах та селищах відсутня базова смарт-інфраструктура. Для роботи аналітики потрібна швидкісна мережа передачі даних (оптоволокно) по всьому місту та потужне серверне обладнання, що потребує значних капіталовкладень [111; 234]. У маленьких містах не проживають кваліфіковані ІТ-спеціалісти, здатні обслуговувати складні серверні комплекси та підтримувати кібербезпеку системи.

На фоні процесу децентраізації в Україні представники місцевої влади невеликих міст намагаються інтегрувати поодинокі камери до Єдиної

інтеграційної платформи відеоспостереження на базі обласних управлінь Національної поліції або МВС. Це дозволяє навіть базовій камері у маленькому селі передавати потік до серверу хмарних технологій, де обробку здійснюватимуть потужні державні сервери з аналітикою штучного інтелекту.

ОЕСР відзначала, що до повномасштабної агресії Україна досягла суттєвого прогресу у скороченні регіональних диспропорцій, зокрема в доступі до широкосмугового інтернету [234], проте ця тенденція зазнала удару війни. Нерівність спроможності громад поглиблюється нерівномірністю воєнних руйнувань. За п'ятою Швидкою оцінкою збитків і потреб (RDNA5), підготовленою Урядом України, Групою Світового банку, Європейською комісією та ООН, станом на 31 грудня 2025 р. загальні потреби у відновленні та відбудові України на десятирічний період оцінено майже в 588 млрд дол. США, що майже втричі перевищує номінальний ВВП 2025 р.; прямі збитки перевищили 195 млрд дол., найбільше постраждали житло, транспорт та енергетика, а збитки й потреби зосереджені у прифронтових областях і великих містах; найбільші потреби припадають на транспортний сектор (понад 96 млрд дол. США), а щонайменше 20 млрд дол. потреб уже покрито за рахунок невідкладних ремонтів і заходів раннього відновлення [252]. Масштабні руйнування енергетики роблять автономне живлення та резервні канали зв'язку обов'язковою умовою роботи систем відеоспостереження, насамперед у малих громадах. Оцінка передбачає відбудову за принципом «відбудувати краще, ніж було» та розширення інтегрованих територіальних підходів до відновлення, зокрема в межах урядової пілотної програми комплексного відновлення, започаткованої у 2024 р. [248].

Для «Безпечного міста» це створює можливість, якою доцільно скористатися на державному рівні: безпекова інфраструктура (камери, освітлення, оповіщення, укриття, канали зв'язку) може закладатися в проєкти відбудови житлових кварталів, транспортних вузлів і соціальних об'єктів ще на етапі проєктування, а не встановлюватися окремими закупівлями після їх завершення. Водночас саме громади з найбільшими руйнуваннями мають найнижчу фінансову спроможність, тож без державних стандартів і механізму

співфінансування розрив між «інтегрованими» великими містами та громадами «початкового» рівня лише зростатиме.

В Україні оцінка міст за безпековими, інфраструктурними та якісними індексами суттєво змінилася під впливом воєнних реалій, логістичних переваг та стійкості громад. Згідно з даними відкритих рейтингів і досліджень, зокрема Міністерства розвитку громад та територій України, програми Transparent Cities та платформи Numbeo, сформувався чіткий перелік міст-лідерів (табл. 2.3).

Львів є стабільним лідером за загальним індексом якості життя та комфорту серед великих міст України. Місто демонструє найвищий індекс комфортності завдяки розвиненій сфері послуг та відносній віддаленості від фронту. Також Львів посів перше місце у національному рейтингу фізичної безбар'єрності та доступності міської інфраструктури [149].

Тернопіль належить до лідерів за сприйняттям безпеки самими мешканцями: у рейтингу безпечності обласних центрів, складеному на основі Третього всеукраїнського муніципального опитування на замовлення Міжнародного республіканського інституту та статистики кримінальних правопорушень, він посів друге місце після Хмельницького [189]. На думку автора, цьому сприяють порівняно низький рівень вуличної злочинності та стійкість базової інфраструктури.

Вінниця є традиційним лідером багатьох внутрішньоукраїнських муніципальних опитувань. Місто входить до топ-3 міст за фінансуванням і розвитком безбар'єрної інфраструктури [149], а також увійшло до трійки лідерів рейтингу прозорості інвестиційної сфери програми Transparent Cities [137].

Івано-Франківськ та Ужгород вважаються лідерами за безпековим показником мінімальної частоти обстрілів та близькості до кордонів країн ЄС/НАТО. Узагальнення проаналізованих джерел дає змогу автору віднести Ужгород до міст із відносно низьким рівнем зареєстрованої злочинності, а Івано-Франківськ – до міст, інфраструктура яких виявилася адаптивною до релокації бізнесу.

Хмельницький демонструє чудові результати в розрізі доступності інфраструктури, посівши друге місце в Україні за комплексним Індексом безбар'єрності серед громад із населенням понад 100 тисяч людей.

Таблиця 2.3

Порівняльна таблиця ключових лідерів за різними метриками

Місто	Пріоритетний індекс / Позиція в рейтингах	Ключові інфраструктурні переваги
Львів	№1 за якістю життя (Numbeo), №1 за фізичною безбар'єрністю	Потужний логістичний та культурний центр, висока щільність укриттів
Тернопіль	Один із лідерів за рівнем суб'єктивної безпеки громадян	Стійкий агросектор, низька частота повітряних тривог/прильотів
Вінниця	Топ-3 за прозорістю інвестиційної сфери (Transparent Cities) і за фізичною безбар'єрністю (Мінрозвитку)	Ефективне муніципальне управління, високий рівень фінансування інфраструктури
Ужгород	Найвищий рівень воєнної безпеки	Максимальна географічна віддаленість від лінії зіткнення
Хмельницький	**№2** за комплексним Індексом безбар'єрності громад	Зручність для ведення релокованого бізнесу, розвиток соціальних сервісів

Джерело: складено автором на основі проведених досліджень

Великі міста, Київ та Харків, стабільно утримують високі позиції за рівнем розвитку IT-інфраструктури, бізнес-можливостей та медичного обслуговування. Проте у загальних індексах безпеки вони поступаються західним регіонам через постійні воєнні загрози, ризики транзитних блекаутів та підвищене навантаження на комунальні мережі.

Для об'єктивної характеристики рівня управління важливо спиратися на рейтинги з відкритою методологією. Так, за результатами щорічного дослідження програми «Прозорі міста» Transparency International Ukraine за 2024 р., оприлюдненого 19 травня 2025 р., рейтинг прозорості серед 100 міст із 21 області очолили Чернівці; оцінювання здійснювалося за 70 критеріями, при цьому 72 міста залишилися в категорії непрозорих, а Львів із 2020 р. стабільно утримує рівень прозорості в межах 75–85 % [194]. Попереднє адаптоване дослідження роботи міських рад в умовах війни, у межах якого оцінювалося 70

міст, віднесло до категорії прозорих лише Дніпро, Львів і Мукачево, тоді як 57 міст опинилися серед непрозорих [196]. Показники цифрової трансформації громад, розраховані Мінцифри, засвідчують лідерство Кривого Рогу, Вінниці, Тернополя, Львова та Харкова [87].

Водночас частина показників, які використовуються в публічному дискурсі для порівняння міст за рівнем безпеки і якості життя, ґрунтується на краудсорсингових даних або разових опитуваннях і не має статусу офіційного моніторингу. Тому для оцінювання рівня управління проєктами «Безпечне місто» доцільно поєднувати три групи джерел: офіційну статистику (злочинність, час реагування, кількість звернень), показники з відкритою методологією (індекси прозорості та цифрової трансформації, показники стандартів ISO 37122 і ISO 37123) та репрезентативні опитування щодо суб'єктивного відчуття безпеки. Лише за такого поєднання можна відрізнити реальні управлінські результати від наслідків географічного розташування міста відносно лінії фронту.

Аналіз міст, що лідирують за безпековими та інфраструктурними індексами показує, що рівень управління найбільше залежить від двох факторів:

- політичної волі управлінців (готовність інвестувати у цифровізацію та ухвалювати непопулярні інфраструктурні рішення);
- здатності довгострокового системного планування замість хаотичних точкових закупівель обладнання.

Наведені чинники доцільно доповнити ще двома, які підтверджуються емпіричними даними. Перший – кадрова спроможність: приклад Львова, де дві штатні одиниці обслуговували понад 2000 камер [111], свідчить, що без відповідного персоналу навіть розгалужена технічна система не може повною мірою реалізувати свій аналітичний потенціал. Другий – прозорість управління: результати рейтингу прозорості міст [194] показують, що відкритість місцевої влади не є прямою функцією розміру чи бюджету міста, а отже, є самостійним показником якості управління, який доцільно враховувати й під час оцінювання проєктів «Безпечне місто». Обидва чинники піддаються вимірюванню, тож

можуть бути включені до державного моніторингу поряд із технічними показниками.

Реалізація проєктів «Безпечне місто» в Україні дозволяє сформувати комплексні висновки щодо характеристики рівня управління українськими населеними пунктами. Спостерігається трансформація управлінського підходу при реалізації концепції «Безпечне місто». Рівень управління поступово еволюціонує від простого локального контролю (фіксація правопорушень камерами) до системного забезпечення внутрішньої стійкості громади [168]. Сукупний аналіз джерел дає автору підстави дійти висновку, що проєкт «Безпечне місто» перестав бути виключно комунальною ініціативою і сформувався як важливий інструмент публічного управління у сфері національної безпеки [168], що особливо критично в умовах воєнного стану.

Незважаючи на прогрес, управлінський рівень у багатьох населених пунктах стримується низкою чинників: відсутністю єдиного правового поля та недостатністю кваліфікованих кадрів. В Україні досі концепція «Безпечне місто» на рівні законодавчо-нормативних актів належно не врегульовані, що створює хаотичність при впровадженні систем на місцях. В органах місцевого самоврядування часто працюють технічні спеціалісти з низьким кваліфікаційним рівнем. Для них непросто ефективно адмініструвати складні аналітичні системи [111; 234].

Альтернативою дорогим аналітичним комплексам для громад із низькою спроможністю може бути модель «безпечної громади», яку розвиває система МВС [121]. Ще у 2021 р. МВС повідомляло про створення 31 Центру безпеки, що поєднує поліцейську станцію та пост ДСНС, з перспективою приєднання до таких осередків і сервісних центрів; тоді ж Міністр розвитку громад і територій наголошував, що МВС і Національна поліція першими у встановлені законом строки привели свої структури у відповідність до нового адміністративно-територіального устрою [156]. Ця обставина важлива для «Безпечного міста», оскільки збіг територіальної організації поліції та громад є передумовою спільного планування безпеки. За даними МВС, оприлюдненими в липні 2026 р.,

проєкт «Поліцейський офіцер громади» забезпечив постійний доступ до поліцейських послуг понад 13 млн мешканців у 1125 громадах; офіцери-рятувальники громади запрацювали в усіх 1293 підконтрольних Україні територіальних громадах; за рік створено 6 нових Центрів безпеки та 88 підрозділів місцевої й добровільної пожежної охорони; служба 112 опрацювала понад 6,4 млн звернень, а в грудні 2025 р. запрацював мобільний застосунок «112 Ukraine»; Служба освітньої безпеки охоплює понад 1,4 млн учнів у 1915 закладах освіти; мережу укриттів розширено на 3455 об'єктів, запроваджено диференційоване оповіщення про повітряні тривоги на рівні районів, а у грудні 2025 р. утворено міжнародну Коаліцію укриттів за участю 11 держав і 4 міжнародних організацій [139]. Ці дані є офіційною позицією відомства і потребують незалежної перевірки, однак вони свідчать про формування базової безпекової інфраструктури саме на рівні громад.

Для проєктів «Безпечне місто» це відкриває можливість визначити мінімальний безпековий пакет для громад початкового рівня: поліцейський офіцер і офіцер-рятувальник громади, центр безпеки або інший пункт спільного реагування, базове відеоспостереження на в'їздах і в ключових точках, підключення до регіонального ситуаційного центру та системи 112, доступні укриття й оповіщення. Такий пакет реалістичний для малих громад і водночас може слугувати першою сходинкою до аналітичного та інтегрованого рівнів управління.

Спостерігається суттєвий диспропорційний розрив між великими містами-лідерами (які впроваджують інтелектуальне відеоспостереження із застосуванням штучного інтелекту) та невеликими громадами, де фінансування покриває лише базові камери без аналітики. Здійснюється слабкий рівень інтеграції, координації та оперативного обміну даними між муніципальними інфраструктурами, Національною поліцією, ДСНС та іншими силовими відомствами [129; 234]. Крім того, бюджетна нерівність фінансових можливостей великих та малих міст України відображається на рівні реалізації проєктів «Безпечне місто».

Рівень управління українськими населеними пунктами при реалізації проєктів «Безпечне місто» характеризується як перехідний – від фрагментарно-технічного до стратегічно-аналітичного**.** Головним викликом залишається подолання кадрового голоду, інтеграція систем цивільного захисту в єдиний безпековий контур та синхронізація зусиль місцевої влади й державних структур.

Узагальнення наведених даних дає змогу конкретизувати зміст кожного з рівнів управління та умови переходу між ними.

Початковий рівень відповідає громадам, які мають базову мережу камер і архів записів. Мінімальними вимогами до нього мають бути: визначення володільця даних і затверджений регламент функціонування системи з метою, строками зберігання та порядком доступу; інформування мешканців про відеоспостереження; базова кібергігієна (реєстр пристроїв, заміна заводських паролів, заборона публічних трансляцій); підключення до системи 112 та регіонального ситуаційного центру.

Аналітичний рівень передбачає використання відеоаналітики, зокрема розпізнавання номерних знаків. Додатковими умовами для нього мають бути оцінка впливу на захист даних до запровадження аналітичних функцій, чітко визначені законом підстави й обмеження їх застосування, аудит алгоритмів, наявність у громаді відповідального фахівця з цифрової трансформації та кібербезпеки, а також технічна сумісність із системою МВС.

Інтегрований рівень передбачає ситуаційний центр, що об’єднує дані муніципальних служб, поліції, ДСНС і соціальних служб. Для нього визначальними стають показники результатів (час реагування, динаміка правопорушень, відчуття безпеки мешканців), незалежний аудит і публічна звітність, зокрема оприлюднення політики використання системи на зразок тієї, що застосовується в Нью-Йорку [233].

Для кожного рівня необхідно також нормативно визначити розподіл ролей: орган місцевого самоврядування як власник інфраструктури і, як правило, володілець персональних даних; оператор системи (комунальне підприємство чи підрядник) як розпорядник, що діє на підставі договору з чітко визначеними

обов’язками щодо захисту даних; правоохоронні органи та інші суб’єкти як користувачі, доступ яких здійснюється за запитом, із журналюванням і в межах визначених законом цілей. Саме відсутність такого розподілу, як показано вище, є спільною причиною правової невизначеності на всіх трьох рівнях управління.

Перехід між рівнями не може залежати лише від фінансових можливостей окремих громад. Державний рівень запровадження проєктів «Безпечне місто» має забезпечити єдині вимоги до кожного рівня, механізм співфінансування для громад із низькою спроможністю, включення безпекової інфраструктури до програм відбудови та державний моніторинг, зокрема через доповнення наявних індексів цифрової трансформації безпековою складовою.

Висновки до розділу 2

У розділі 2 дисертаційного дослідження охарактеризовано впровадження моделей світового досвіду проєктів «Безпечне місто» в Україні, досліджено розвиток соціальної політики держави у проєктах «Безпечне місто», досліджено рівень управління українськими населеними пунктами при реалізації проєктів «Безпечне місто».

Доведено, що впровадження концепції «Безпечне місто» в Україні спирається на передовий світовий досвід. Воно передбачає створення інтегрованих систем відеоспостереження з аналітикою, авторозпізнаванням номерів, сенсорами моніторингу довкілля та єдиними операційними центрами реагування для таких міст, як Київ, Дніпро, Харків та Одеса.

Європейський досвід реалізації проєктів «Безпечне місто» еволюціонував від простого встановлення камер спостереження до комплексних екосистем міської безпеки. Вони спираються не лише на технічні інновації, а й на інклюзивність, довіру мешканців та суворе дотримання прав людини. Ключові принципи та підходи до реалізації проєктів «Безпечне місто» в ЄС охоплює концепцію «Безпека через проєктування», яка передбачає досягнення балансування технологій та приватності даних при залученні мешканців міст.

Встановлено, що європейська модель правового забезпечення проєктів «Безпечне місто» має трирівневий характер: Загальний регламент про захист даних (Регламент (ЄС) 2016/679) вимагає забезпечувати захист даних на етапі проєктування та проводити оцінку впливу в разі систематичного моніторингу публічних місць, Директива (ЄС) 2016/680 встановлює окремий режим обробки даних поліцією, а Регламент (ЄС) 2024/1689 про штучний інтелект з 2 лютого 2025 р. заборонив віддалену біометричну ідентифікацію «в реальному часі» в публічних місцях для правоохоронних цілей, крім вичерпно визначених випадків за попереднім незалежним дозволом. Для України як держави – кандидата на членство в ЄС ці вимоги є орієнтиром для проєктування систем, у яких біометричні й аналітичні функції мають існувати як окремі модулі з власною правовою підставою [136].

Обґрунтовано, що для реалізації проєктів «Безпечне місто» в Україні доцільно вивчити західну та східну (азійську) моделі. В рамках західної моделі (досвід ЄС та США) фокусуються на балансі безпеки та захисту приватного життя, використанні європейського/американського обладнання та залученні громадськості через прозорі муніципальні платформи. Азійська/східна модель (досвід Сінгапуру, Китаю) характеризується тотальною цифровізацією, штучним інтелектом, прогнозна аналітика та глибока інтеграція біометричних даних.

Досліджено, що проблеми впровадження європейської моделі світового досвіду запровадження проєктів «Безпечне місто» в Україні полягають у залежності від окремих масових закордонних виробників апаратного забезпечення, недостатньому обсязі фінансування на рівні окремих міст в умовах воєнного стану, ризики порушення прав громадян на приватність через недосконаліть законодавчого поля щодо регулювання біометричних даних.

Конкретизовано, що недосконаліть національного законодавства полягає у відсутності обов’язкової оцінки впливу на захист даних, спеціальних правил для віддаленої біометричної ідентифікації й автоматизованої аналітики та нормативних строків зберігання записів: чинний Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI таких норм не містить, а

законопроєкт «Про захист персональних даних» (реєстр. № 8153 від 25.10.2022) станом на грудень 2025 р. перебував на стадії підготовки до другого читання.

Визначено, проблеми, пов'язані з реалізацією концепції «Безпечне місто», стосуються суспільної критики за порушення конфіденційності та оцінки ефективності окремих інструментів. Використання мілітарних технологій та систем розпізнавання облич викликає протести правозахисників через ризики тотального стеження та порушення прав громадян. Через високу вартість та суперечливі результати оцінки ефективності окремих інструментів у деяких містах.

Узагальнено практику Європейського суду з прав людини, Суду справедливості ЄС і національних судів щодо відеоспостереження, зберігання біометричних даних, масової аналітики та розпізнавання облич. Доведено, що вона формує сукупність управлінських вимог до проєктування систем «Безпечне місто»: закон має визначати, хто, де, з якою метою і як довго може застосовувати біометричні та аналітичні функції; оцінка впливу має передувати закупівлі; строки зберігання, журналювання доступу, незалежний аудит і порядок інтеграції приватних камер мають закладатися в технічне завдання, а розширений доступ в умовах воєнного стану – документуватися з планом повернення до стандартів мирного часу. З'ясовано також, що доказові дані засвідчують помірний і залежний від контексту ефект відеоспостереження, найбільший – на автостоянках і в системах з активним моніторингом, тож ефективність проєктів визначається цільовим застосуванням і незалежним оцінюванням результатів, а не кількістю встановленого обладнання.

Східна (азійська) модель «Безпечне місто» базується на жорсткій державній координації, масовому впровадженні штучного інтелекту, систем розпізнавання облич, Інтернету речей (IoT) та об'єднанні всіх комунальних і правоохоронних служб у єдині централізовані ситуаційні центри реагування в реальному часі. Ключовою рисою східної (азійської) моделі є домінування централізованого державного управління та єдиних вертикальних протоколів замість ініціатив представників місцевих органів влади. На думку автора, у

межах східної моделі перспективним є застосування безпілотників із панорамними камерами для моніторингу масових скупчень людей з повітря. Прямі канали зв'язку забезпечують миттєву передачу зашифрованого відеопотоку на планшети патрульних поліцейських ще до їх прибуття на місце події.

Досліджено, що головними перевагами східної моделі запровадження проєктів «Безпечне місто» вважаються миттєве реагування на надзвичайні ситуації та правопорушення завдяки прогнозній аналітиці, високий рівень розкриття злочинів та профілактика правопорушень, а також повна синхронізація роботи поліції, екстрених служб і комунальної інфраструктури.

Виявлено, що східна модель є й експортним продуктом, задекларовані результати якого важко перевірити, а обмеження закупівель обладнання для відеоспостереження окремих китайських виробників для цілей громадської безпеки, запроваджені у США, свідчать, що вибір моделі та постачальника є питанням кібербезпеки й безпеки ланцюгів постачання. Для України це зумовлює потребу включати до тендерної документації вимоги щодо походження обладнання, відкритих стандартів, сумісності та можливості незалежного аудиту програмного забезпечення.

Виявлено, що соціально-орієнтований підхід до реалізації проєктів «Безпечне місто» передбачає формування системи випереджувальних заходів, спрямованих запобіганню правопорушенням до того, як вони настануть. Він ґрунтується на використанні штучного інтелекту та відеоаналітики для прогнозування ризиків, автоматизоване оповіщення профільних служб до настання критичної ситуації. Інтеграція соціальних сервісів, муніципальних варт та медичної допомоги у спільну цифрову систему з метою раннього виявлення загроз життю та здоров'ю вразливих верств населення в реальному часі.

Обґрунтовано, що теоретичним підґрунтям соціально орієнтованого підходу є концепція людської безпеки, яка зміщує акцент із безпеки територій на безпеку людей, та концепція запобігання злочинності засобами середовищного проєктування, міжнародно закріплена в стандарті ISO 22341:2021; у межах цих

підходів відеоспостереження є лише одним з інструментів поряд із плануванням простору, освітленням і природним наглядом. Самостійну роль освітлення підтверджують доказові дослідження, зокрема рандомізований експеримент у Нью-Йорку, що засвідчив зниження нічної злочинності на вулицях щонайменше на 36%. Як показник результативності соціально орієнтованих програм запропоновано використовувати індикатор 11.7.2 Цілей сталого розвитку – частку осіб, які зазнали фізичних або сексуальних домагань у публічних місцях.

Трансформація ролі проєкту «Безпечне місто» в соціальній політиці характеризується переходом від реакції до попередження. Основні напрями державної та місцевої політики соціальної спрямованості полягають у допомозі вразливим категоріям. Забезпечується підтримка літніх людей та маломобільних громадян через інтеграцію соціальних служб і міських систем спостереження. Здійснюється гарантування безпеки та захист прав дітей та неповнолітніх у навчальних закладах та громадських місцях. Інклюзивний моніторинг передбачає інтеграцію камер із аналітикою для допомоги людям із порушеннями зору чи слуху.

Висвітлено, розвиток соціальної політики України у сфері протидії насильства спрямований на перехід від точкового реагування до створення загальнонаціональної людиноцентричної системи. Муніципальні ініціативи на кшталт проєктів «Безпечне місто» та регіональних програм «Міста і громади, вільні від домашнього насильства» інтегрують безпеку, соціальні послуги й екстрену допомогу на рівні кожного регіону.

Встановлено, що правову основу інтеграції проєктів «Безпечне місто» з політикою протидії насильству становлять Закон України «Про запобігання та протидію домашньому насильству» від 07.12.2017 № 2229-VIII, Стамбульська конвенція, ратифікована Законом України від 20.06.2022 № 2319-IX, та Закон України «Про соціальні послуги» від 17.01.2019 № 2671-VIII. Обґрунтовано, що така інтеграція має забезпечувати маршрути перенаправлення, за яких виклик через систему 112 ініціює залучення соціальних служб і подальший супровід,

зокрема в центрах життєстійкості, а дані про постраждалих обробляються в режимі обмеженого доступу.

Виявлено, що державна політика безбар'єрності в проєктах «Безпечне місто» поступово еволюціонує від традиційного відеоспостереження до інклюзивного середовища. Використання штучного інтелекту та відеоаналітики дозволяє завчасно виявляти небезпечні ситуації за участю вразливих верств населення на вулицях. Цифрові та інфраструктурні рішення охоплюють потреби маломобільних груп, ветеранів та літніх людей, гарантуючи рівний доступ до безпеки, укриттів і послуг. Проєкти «Безпечне місто» трансформуються з інструментів виключного відеоспостереження на ініціювання новітніх платформ соціального захисту та підтримки вразливих категорій населення (літніх людей, маломобільних громадян, сімей з дітьми) завдяки інтеграції місцевих та державних служб реагування.

З'ясовано, що зобов'язання щодо безбар'єрності випливають із Конвенції про права осіб з інвалідністю, ратифікованої Законом України від 16.12.2009 № 1767-VI, однак за результатами моніторингу укриттів, здійсненого Секретаріатом Уповноваженого Верховної Ради України з прав людини у 2025 р., їх недоступність для осіб з інвалідністю визначено найбільш критичною проблемою. Зростання чисельності ветеранів війни, членів родин загиблих та осіб з інвалідністю внаслідок війни понад 1,3 млн осіб, а також розвиток Служби освітньої безпеки та ініціативи «Громада, дружня до дітей та молоді» визначають групи користувачів, потреби яких мають ураховуватися вже на етапі проєктування безпекової інфраструктури.

Доведено, що соціальна орієнтація «Безпечного міста» потребує запобіжників щодо ризиків для вразливих груп: алгоритми розпізнавання облич демонструють суттєво вищу частоту хибних збігів щодо жінок, людей похилого віку та дітей, тому інтеграція безпекових і соціальних даних має ґрунтуватися на принципі мінімізації, оцінці впливу на рівність і участі організацій, що представляють інтереси вразливих груп. З огляду на те, що у 2023 р. 40,4%

дорослого населення мали цифрові навички нижче базового рівня, нецифрові канали звернення по допомогу мають зберігатися.

Визначено, що управління українськими населеними пунктами під час реалізації проєктів «Безпечне місто» характеризується переходом від фрагментарного реагування до інтегрованого цифрового публічного управління в умовах децентралізації та воєнного стану. Представники влади українських міст є головним замовником та координатором безпекових систем, об'єднуючи зусилля комунальних служб, Національної поліції та ДСНС.

Встановлено, що реформа децентралізації, у межах якої понад 10 тис. місцевих рад було об'єднано в 1469 громад, створила інституційне підґрунтя для муніципальних проєктів «Безпечне місто», однак зумовила значні відмінності між громадами в адміністративній, кадровій та фінансовій спроможності, які поглибила війна. В умовах воєнного стану такі системи функціонують щонайменше в трьох площинах – муніципальній, правоохоронній та оборонній, – тоді як чинне законодавство не розмежовує ролей власника камер, володільця й розпорядника персональних даних і користувачів відеоінформації.

Попри наявність ефективно реалізованих проєктів багатьох українських міст (Тернополя, Києва, Рівного), в управлінні населеними пунктами при реалізації проєктів «Безпечне місто» часто виникають проблеми правової неврегульованості та обмеженості фінансування. Муніципальні системи працюють за локальними програмами, оскільки єдині загальнодержавні стандарти для систем відеоконтролю та захисту персональних даних із залученням штучного інтелекту потребують доопрацювання.

Виявлено, що законопроєкт «Про єдину систему відеомоніторингу стану публічної безпеки» (реєстр. № 11031 від 20.02.2024), спрямований на інтеграцію систем центрального, регіонального та місцевого рівнів, чітко не визначає кола осіб, які матимуть доступ до інформації. Обґрунтовано, що державний рівень запровадження проєктів «Безпечне місто» має полягати не лише в технічній інтеграції муніципальних камер у систему МВС, а насамперед у законодавчому визначенні користувачів, цілей обробки, строків зберігання, порядку

застосування біометричних функцій, незалежного нагляду та вимог кібербезпеки, необхідність яких підтверджує блокування СБУ від початку повномасштабного вторгнення близько 10 тис. IP-камер, які могли бути використані противником.

Охарактеризовано суттєвий диспропорційний розрив між великими містами-лідерами (які впроваджують інтелектуальне відеоспостереження із застосуванням штучного інтелекту) та невеликими громадами, де фінансування покриває лише базові камери без аналітики. Здійснюється слабкий рівень інтеграції, координації та оперативного обміну даними між муніципальними інфраструктурами, Національною поліцією, ДСНС та іншими силовими відомствами. Крім того, бюджетна нерівність фінансових можливостей великих та малих міст України відображається на рівні реалізації проєктів «Безпечне місто».

Запропоновано конкретизувати зміст трьох рівнів управління; для початкового рівня – визначення володільця даних, регламент функціонування системи, інформування мешканців, базова кібергігієна та підключення до системи 112; для аналітичного – попередня оцінка впливу, законні підстави кожної аналітичної функції, аудит алгоритмів і відповідальний фахівець; для інтегрованого – ситуаційний центр за участю муніципальних, правоохоронних, рятувальних і соціальних служб, показники результатів, незалежний аудит і публічна звітність. Для громад із низькою спроможністю обґрунтовано мінімальний безпековий пакет, що поєднує поліцейського офіцера й офіцера-рятувальника громади, центр безпеки, базове відеоспостереження в ключових точках, доступні укриття й оповіщення.

Обґрунтовано, що перехід між рівнями не може залежати лише від фінансових можливостей окремих громад: державний має забезпечити єдині вимоги до кожного рівня, кадрові нормативи, механізм співфінансування, конкурентні закупівлі з оцінкою повної вартості володіння, включення безпекової інфраструктури до проєктів відбудови та державний моніторинг на

основі показників стандартів ISO 37122 і ISO 37123 та Індексу цифрової трансформації, доповненого безпековою складовою.

РОЗДІЛ ІІІ
ЗАПРОВАДЖЕННЯ СИСТЕМ «БЕЗПЕЧНЕ МІСТО» НА РІВНІ УКРАЇНСЬКОЇ ДЕРЖАВИ

3.1. Концепція стратегічного розвитку систем «Безпечне місто» на території України

Концепція «Безпечне місто» в Україні вважається стратегічним інструментом публічного управління та єдиним інформаційним простором для посилення безпеки в українських містах [96]. Проєкт об'єднує інноваційні технології з метою безпеки, контролю порядку та управління міською інфраструктурою на території України. Основні завдання складної системи «Безпечне місто» полягають у автоматичній інтеграції систем камер моніторингу, де здійснюється фіксація транспортного і пішохідного трафіку, розпізнавання номерів автомобілів та облич громадян з подальшим аналізом подій у реальному часі. Цифрова трансформація аналітики відеоспостереження передбачає перехід від простих камер до елементів «розумного міста» (Smart City) як складової публічного управління [102].

Оперативна взаємодія та координування дій співробітників служб національної поліції, рятувальників Державної служби з надзвичайних ситуацій (ДСНС), представників органів місцевого самоврядування та комунальних підприємств забезпечуватиметься завдяки функціонуванню ситуаційних центрів реагування. Переформатування функціоналу систем «Безпечне місто» в умовах воєнного стану для посилення захисту критичної інфраструктури та обороноздатності України [97].

Багато українських міст (серед яких Київ, Харків, Хмельницький) впроваджують елементи «Smart City» та ситуаційні центри для контролю правопорядку та управління міським середовищем. Технічні рішення реалізуються у співпраці з телеком-операторами (зокрема, проєкти на рішень від

компанії «Датагруп» [172]) та за методологічною підтримкою наукових і правоохоронних інститутів.

Правові аспекти легітимності використання відкритих даних відеомоніторингу в регіонах України базуються на балансі між гарантуванням публічної безпеки / доступом до публічної інформації та захистом права громадян на приватність. Головне потиріччя полягає в тому, що самі по собі відкриті дані мають бути вільно доступними, але відеозаписи громадян підпадають під суворе регулювання як персональні дані. Легітимність використання таких даних регулюється кількома базовими нормативно-правовими актами: Конституція України, Цивільний кодекс України, Закон України «Про захист персональних даних», Закон України «Про доступ до публічної інформації».

У статті 32 Конституції України визначено: ніхто не може зазнавати втручання в його особисте і сімейне життя. Заборонено збирання, зберігання та поширення конфіденційної інформації про особу без її згоди.

Закон України «Про захист персональних даних» відображають відеозображення особи, за яким її можна ідентифікувати (включаючи біометричні дані чи розпізнавання облич), є персональними даними. Відповідно, їх поширення як «відкритих даних» без згоди або знеособлення є незаконним.

Стаття 307 Цивільного кодексу України інформує, що фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згоди [6]. Згода припускається (мовчазна згода), якщо зйомка ведеться відкрито на вулиці, на зборах, конгресах або інших заходах публічного характеру.

Кримінальна відповідальність настає за незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу (ст. 182 ККУ). Використання прихованих або негласних засобів відеоспостереження суворо заборонено всім, крім правоохоронних органів за рішенням суду (ст. 359 ККУ) [5].

Закон України «Про доступ до публічної інформації» визначає статус відкритих даних. Системи відеомоніторингу населених пунктів «Безпечне місто»

діють на стику цього закону та обмежень національної безпеки. Щоб використання даних відеомоніторингу у форматі трансляцій відкритих даних вважалося правомірним, мають виконуватися умови, які описуються критеріями легітимності використання відкритих даних (табл. 3.1) – знеособлення, публічності та повідомлення про оприлюднення, балансу цільових інтересів.

Таблиця 3.1

Критерії легітимності використання відкритих даних

Критерій	Особливості та вимоги
Знеособлення (Анонімізація)	Якщо відеопотік публікується у відкритому доступі для аналітики (наприклад, підрахунок трафіку, завантаженість доріг), якість зображення або програмні алгоритми повинні виключати можливість розпізнавання облич чи номерних знаків автівок. Без цього дані втрачають статус "відкритих" і стають незаконним поширенням персональних даних.
Публічність та повідомлення	На території, де ведеться моніторинг, обов'язково мають бути встановлені попереджувальні таблички («Ведеться відеоспостереження»). Людина повинна знати, що фіксується зйомка.
Баланс інтересів та легітимна мета	Збір даних державними органами чи громадами має відбуватися виключно задля легітимної мети: безпека громадян, запобігання злочинам, регулювання дорожнього руху.

Джерело: складено автором на основі проведених досліджень

В Україні розроблено Законопроєкт № 11031 («Про єдину систему відеомоніторингу стану публічної безпеки») для нормативно-правового обгрунтування централізації всіх камер та чітко регламентувати хто має право доступу до повних відеопотоків (переважно правоохоронні органи); яка саме інформація та в якому обсязі може відображатися для широкого загалу без порушення приватності. Впровадження закону дозволить забезпечити перехід від локальних систем контролю дорожнього руху до комплексних національних безпекових середовищ.

В умовах дії воєнного стану легітимність відкритих трансляцій є суттєво обмеженою. Оприлюднення точного розташування камер**,** а також онлайн-трансляція панорамних видів міст, об'єктів критичної чи транспортної інфраструктури заборонені або суворо обмежені**,** оскільки ці відкриті дані можуть бути використані ворогом для коригування ударів чи розвідки.

Правоохоронний сектор виступає головним користувачем, координатором та архітектором вимог до системи для попередження й розслідування злочинів. Міністерство внутрішніх справ України (МВС) забезпечує загальну державну стратегію інтеграції локальних систем відеонагляду в єдиний безпековий контур країни. Національна поліція України є основним практичним оператором, ситуаційні центри якого цілодобово використовують дані проєкту «Безпечне місто» для аналітики, патрулювання та реагування на правопорушення. Державна служба України з надзвичайних ситуацій (ДСНС) використовує можливості платформи для раннього виявлення пожеж, аварій та ліквідації наслідків надзвичайних ситуацій.

Мультиплатформенний проєкт «Безпечне місто» – це комплексна інформаційно-аналітична система відеоспостереження й безпеки громад, яка впроваджується на перетині технологій, практичної безпеки та науки. Проєкт має комплексну багаторівневу підтримку з боку державних інституцій, провідних відомчих університетів та науково-дослідних установ. Практичне впровадження й моніторинг мультиплатформенного проєкту «Безпечне місто» здійснюється правоохоронними органами та інститутами.

Методологія та навчання мультиплатформенного проєкту «Безпечне місто» забезпечується фахівцями профільними закладами вищої освіти та наукових інститутів. Співробітники відомчих та класичних університетів здійснюють науковий супровід проєкту, розробляють методичні рекомендації щодо цифровізації публічного врядування та інтегрують системи у навчальний процес для підготовки фахівців. Національна академія внутрішніх справ (НАВС) активно впроваджує технології проєкту «Безпечне місто» в освітній процес. Академія має офіційні партнерства з розробниками систем відеоаналітики для створення симуляційних та моніторингових класів, де навчають майбутніх аналітиків поліції. Дніпропетровський державний університет внутрішніх справ (ДДУВС) та Донецький державний університет внутрішніх справ (ДонДУВС) досліджують інструменти кримінального аналізу на базі міських відеосистем та розробляють теоретичні моделі безпеки громад у рамках воєнного стану.

Науковці Харківського національного університету внутрішніх справ (ХНУВС) фокусуються на правових аспектах кібербезпеки та впровадженні інтелектуального відеоспостереження (AI-аналітика, розпізнавання облич та автомобільних номерів).

У Київському національному університеті імені Т. Шевченка досліджують цифрові трансформації проєкту «Безпечне місто» крізь призму публічного управління та реформ сектору безпеки в межах міжнародних наукових ініціатив.

Оскільки кожна програма фінансується та затверджується локально органами місцевого самоврядування. Вагомим інституційним розробником виступають міські та селищні ради (наприклад, КМДА в Києві через КП «Інформатика», Дніпровську, Чернігівська міські ради тощо), які залучають до технічної підтримки державне IT-підприємство «Інфотех».

Рис. 3.1. Напрями розвитку проєктів «Безпечне місто» на території України

Джерело: складено автором на основі проведених досліджень

Стратегічний розвиток концепції системи «Безпечне місто» на території України є ключовим інструментом публічного управління в системі захисту населення, який зазнає глибокого функціонального переформатування під

впливом введення воєнного стану та цифрової трансформації. Сучасна стратегія спрямована на перехід від локальних розрізнених систем відеоспостереження до єдиного інтегрованого інформаційного простору національної безпеки, що координується МВС України, Національною поліцією та ДСНС.

Основні стратегічні вектори подальшого розвитку систем «Безпечне місто» базуються на концептуальних орієнтирах та адаптовані до викликів сьогодення:

- Інтеграція в оборонну інфраструктуру. Трансформація платформ «Безпечне місто» в елемент забезпечення обороноздатності (моніторинг переміщення ворожої техніки, повітряних загроз, координація дій у разі обстрілів).
- Єдині аналітичні центри. Створення ситуаційних центрів та Єдиних операційних центрів у великих містах (досвіду Києва та Дніпра) для збору даних в один інтерфейс.
- Інтелектуальне відеоспостереження: Впровадження камер із функціями штучного інтелекту (розпізнавання облич, автомобільних номерів, виявлення підозрілих предметів, фіксація порушень комендантської години).
- Поєднання систем моніторингу систем проєкту «Безпечне місто» з єдиним номером екстрених служб 112 для миттєвого реагування на виклики громадян українських міст.

У регіонах України структуру безпекового простору вирішено формувати за двома компонентами – о’бєкти та ситуації (рис. 3.1).

Проблеми та виклики реалізації системи проєкту «Безпечне місто» полягають у розподілі повноважень. Наявна часткова невизначеність зон відповідальності в межах проєкту «Безпечне місто» між представниками органів державної влади (МВС, Національна поліція) та представниками органів місцевого самоврядування. З цим пов’язана необхідність остаточного затвердження та впровадження уніфікованих стандартів безпеки українських міст для оцінювання ефективності систем «Безпечне місто». Комплексний аналіз безпекового середовища в українських містах (зокрема, шляхом розробки

єдиного Індексу безпеки українських міст, регіональних рейтингів Інституту суспільно-економічних досліджень) пропонується базувати на поєднанні об'єктивних статистичних даних (від МВС, ДСНС, Національної поліції) та суб'єктивного сприйняття безпеки громадянами (що можна оцінити за допомогою результатів опитування жителів) [104].

Інститут суспільно-економічних досліджень (ГО «ІСЕД») як неурядовий аналітичний центр оприлюднює два великі резонансні дослідження та відповідні рейтинги міст України: рейтинг інституційної досконалості та рейтинг безпечності обласних центрів.

Рейтинг інституційної досконалості (готовності міст до сталого розвитку). Цей індекс розраховувався на основі міжнародних критеріїв сталого розвитку громад та даних всеукраїнських муніципальних опитувань. Він оцінював залучення мешканців до економіки, інтегрованість громади та якість міського управління. Наприклад, українські міста-лідери рейтингу, що готові до сталого розвитку: Луцьк (перше місце), Вінниця, Івано-Франківськ, Рівне та Тернопіль. Міста з найнижчими показниками: Суми, Херсон, Кропивницький (15-те місце).

Рейтинг безпечності обласних центрів України як індекс базується на поєднанні двох факторів: офіційної статистики МВС щодо кількості кримінальних правопорушень на 10 тисяч населення та результатів опитувань містян щодо їхнього суб'єктивного відчуття безпеки у вечірній час. Відповідно до рейтингу безпечності обласних центрів України найбезпечнішими оцінюються міста: Хмельницький (лідер за рівнем безпеки), а також Тернопіль, Чернівці, Чернігів та Івано-Франківськ. А найнебезпечнішими вважаються міста: Запоріжжя (останнє місце за рахунок високої кількості правопорушень), Кропивницький, Київ, Сєвєродонецьк та Миколаїв.

Структурно єдиний Індекс безпеки українських міст може поділяється на декілька ключових вимірювальних блоків: воєнна та техногенна безпека, кримінальна безпека, цивільна та екологічна безпека, соціально-медична та інклюзивна безпека, суб'єктивний вимір відчуття безпеки громадянами (рис. 3.2).

Рис. 3.2. Рекомендовані вимірювальні блоки єдиного Індексу безпеки українських міст

Джерело: складено автором на основі проведених досліджень

Офіційне обґрунтування необхідності побудови Єдиної державної системи відеомоніторингу стану публічної безпеки на базі чинних муніципальних систем «Безпечне місто» передбачає, в основному необхідності централізації правоохоронної та превентивної діяльності, усуненні технічної розрізненості регіональних камер і впровадженні штучного інтелекту для аналітики.

В Україні функціонує понад 60 000 камер у межах більш ніж 600 окремих локальних систем. Кожне місто самостійно розробляє програми «Безпечне місто», через що камери мають різні стандарти, а обмін даними між регіонами ускладнений. Впровадження єдиної державної системи відеомоніторингу дозволить створити уніфіковані функціональні й технічні стандарти для обміну інформацією через спільний інформаційний простір МВС (табл. 3.2).

Таблиця 3.2

Порівняльний аналіз архітектури систем «Безпечне місто» та єдиної державної системи відеомоніторингу

Критерій	**Локальна система «Безпечне місто»**	**Єдина державна система відеомоніторингу**
Рівень управління	Місцева влада (ТГ, міськради)	Центральний (МВС / Національна поліція)
Географічне охоплення	Локальне (межі населеного пункту)	Загальнодержавне (інтеграція всіх міст і трас)
Головна мета	Благоустрій, комунальний контроль, локальний правопорядок	Національна безпека, розкриття злочинів, протидія загрозам
Правова база	Регіональні програми та рішення міськрад	Профільні закони, постанови КМУ та стандарти МВС

Джерело: складено автором на основі проведених досліджень

Впровадження інтелектуальної відеоаналітики шляхом побудови єдиної платформи дозволить масштабувати інструменти біометричної ідентифікації та розпізнаванти (обличчя громадян, номерні знаки, марка/колір транспорту). Локальні бюджети не завжди спроможні самостійно фінансувати дорогі аналітичні модулі, тоді як підключення до центрального ядра МВС надасть представникам місцевої влади доступ до передових аналітичних інструментів. Об’єднання локальних систем «Безпечне місто» у єдину державну ланку відеомоніторингу дозволить контролювати витрати та уніфікувати державні закупівлі обладнання, оптимізувати видатки на адмініструвати серверну інфраструктуру та уникнути дублювання камер на одних і тих же ділянках доріг чи об’єктах інфраструктури міст України.

Підвищення рівня національної та публічної безпеки України пропонується забезпечувати шляхом здійснення централізованого відеомоніторингу. Це концептуально обґрунтовується потребами обороноздатності країни, протидії диверсійним загрозам в умовах воєнного стану, а також попередженням правопорушень. Інтеграція локальних систем «Безпечне місто» в Єдину державну систему відеомоніторингу дозволяє:

- ефективно відстежувати та розкривати кримінальні й адміністративні злочини «по гарячих слідах»;
- координувати дії співробітників Національної поліції, ДСНС та служб місцевих органів державної влади у режимі реального часу;
- автоматизувати пошук зниклих безвісти осіб та ідентифікацію транспортних засобів.

Міська безпекова інфраструктура в рамках концепції «Безпечне місто» перетворює вразливі українські міста на активні тилові. Вона не просто пасивно захищає, а дозволяє на рівні держави по можливість адаптуватися до ударів, швидко відновлюватися та продовжувати довготривалу боротьбу.

3.2. Використання хмарних технологій в рамках підвищення рівня безпеки в містах України

Використання хмарних технологій є ключовим фактором цифрової трансформації та підвищення рівня безпеки в містах України [83]. Впровадження хмарних технологій в концепцію «Безпечне місто» за стандартами «розумного міста» **(**Smart City) може бути безпосередньо адаптована до умов післявоєнного відновлення. В її основу покладено модель Cloud First, що дозволяє замінити знищену фізичну IT-інфраструктуру гнучкими, захищеними та децентралізованими хмарними сервісами.

Стратегічний підхід в управлінні процесом впровадження концепції «Безпечне місто» із застосуванням хмарних технологій дозволяє перейти від застарілих локальних серверів до сучасних гнучких моделей аналітики. Це

критично важливо в умовах воєнного стану, коли цифрова інфраструктура постійно наражається на кібератаки та фізичні руйнування. Сучасні хмарні сервіси суттєво змінюють підходи до безпеки українських міст за кількома основними напрямами:

- централізація та масштабування відеомоніторингу;
- інтеграція штучного інтелекту (AI) в аналітику;
- підвищення рівня здатності системи продовжувати свою роботу та виконувати задані функції навіть у разі виникнення збоїв, помилок або виходу з ладу окремих її компонентів та кібербезпеки як сукупності заходів, технологій і процесів, створених для захисту комп'ютерних систем, мереж, програм та електронних даних від цифрових атак [119; 259], пошкоджень або несанкціонованого доступу.

Хмарні технології забезпечують зберігання й оперативну обробку великого обсягу даних із тисяч смарт-камер та Інтернет-пристроїв. Представники органів місцевої влади можуть швидко збільшити обсяги сховищ без закупівлі дорогого фізичного обладнання. У такий спосіб створюються передумови для об'єднання локальних та регіональних систем у єдину національну платформу відеомоніторингу.

Завдяки хмарним AI-модулям системи автоматично ідентифікують об'єкти (автомобільні номери, обличчя громадян) з баз розшуку правоохоронців та фіксують нестандартну поведінку в реальному часі. Хмарні аналітичні інструменти допомагають прогнозувати ймовірність інцидентів правопорушень та автоматично інформувати ситуаційні центри поліції чи ДСНС. Ефективне керування транспортними потоками на основі хмарних обчислень дозволяє оптимізувати трафік, уникаючи заторів та оперативно реагувати на ДТП.

Перенесення даних у хмарні сховища (зокрема за межі України чи у захищені дата-центри) захист від фізичного знищення, тим самим гарантуючи безперервність роботи міських сервісів навіть під час обстрілів критичної інфраструктури (табл. 3.3). Провайдери хмарних послуг використовують найновіші технології захисту від кібератак, механізми шифрування,

багатофакторну автентифікацію та принципи нульової довіри. Передбачено процеси перенесення даних у хмарні сховища регулюювати Законом України «Про хмарні послуги» [30; 116]. Галузеві профілі безпеки систем, що використовуються для надання хмарних послуг, розробляються з урахуванням базових профілів безпеки систем, затверджених наказами Адміністрації Держспецзв'язку від 30.06.2025 № 409 (для систем, де обробляється відкрита або конфіденційна інформація) та від 02.07.2025 № 419 (для систем, де обробляється службова інформація) [48], а загальні підходи до кіберзахисту викладено в методичних рекомендаціях Держспецзв'язку щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури [47].

Таблиця 3.3

Порівняння локальної інфраструктури та хмарних технологій у проєктах «Безпечне місто»

Критерій	**Локальне розміщення об'єктів інфраструктури**	**Хмарні технології**
Швидкість масштабування	Низька (потребує закупівлі й монтажу нових серверів). Закупівля та налаштування фізичного обладнання займає місяці	Висока (ресурси додаються оперативно). Створення нових реєстрів або запуск послуг для ВПО за кілька годин
Фізична безпека	Вразлива до ракетних ударів та руйнувань будівель. Ризик фізичного знищення дата-центру та втрати всіх даних міських реєстрів	Максимальна (розподілені та георезервовані дата-центри). Захист завдяки географічному розподілу та резервному копіюванню в безпечні зони
Впровадження штучного інтелекту	Потребує купівлі спеціальних графічних процесорів (GPU)	Доступне як готова послуга
Оновлення захисту	Здійснюють локальні IT-спеціалісти	Автоматичне від провайдера з експертизою світового рівня
Економічна ефективність	Великі капітальні витрати (CAPEX) на техніку, яка швидко застаріває.	Оплата лише за фактично спожиті ресурси (OPEX), легке масштабування.
Інтеграція технологій	Обмежені можливості впровадження штучного інтелекту та Big Data через відсутність потужностей.	Готові хмарні інструменти аналітики, штучного інтелекту та машинного навчання «з коробки».

Джерело: складено автором на основі проведених досліджень

Перехід від капітальних витрат на купівлю обладнання (CAPEX – капітальні витрати або інвестиції в купівлю, створення чи модернізацію довгострокових необоротних активів) до операційних платежів (OPEX – це регулярні повсякденні витрати компанії на забезпечення її поточної діяльності та функціонування) дозволяє економно та раціонально використовувати кошти місцевих бюджетів [199]. Розподілене зберігання інформації на віддалених серверах гарантує безперебійну роботу критичної інфраструктури навіть у разі локальних надзвичайних ситуацій.

Використання хмарних технологій у проєктах «Безпечне місто» в Україні підвищує відмовостійкість цифрової інфраструктури та забезпечує ефективну обробку даних. Хмарні технології дозволяють накопичувати та зберігати великі обсяги даних інформації з камер відеоспостереження та датчиків без потреби будувати власні масивні серверні центри. Оперативні служби та муніципалітети отримують віддалений і швидкий доступ до відеозаписів та аналітики в реальному часі. Розподілена хмарна інфраструктура захищає систему від локальних збоїв чи пошкоджень обладнання на місцях. Масштабне збільшення кількості камер чи інтеграція нових модулів (наприклад, розпізнавання облич або номерів авто) відбувається швидше. Хмарні технології є надійним фундаментом для швидкого розгортання державних і міських сервісів в рамках концепції «Безпечне місто» без потреби купувати власне обладнання та сервери.

З метою повоєнного відновлення українських міст основними архітектурними складовими проєктів «Безпечне місто» з інтеграцією хмарних рішень пропонується вважати [169]:

1. Хмарну платформу даних. Зберігання та обробка інформації з великої кількості камер відеоспостереження, датчиків дорожнього руху та комунікаційних мереж на базі захищених хмарних дата-центрів. Розподілене зберігання даних на хмарних платформах захищає критичну міську інформацію від фізичного знищення локальних серверів.

2. Центр управління. Інтеграція комунальних служб та екстрених структур в єдиному цифровому середовищі для швидкого реагування на надзвичайні ситуації або аварії в інфраструктурі.

3. Енергоефективну мережу Інтернет речей. Вона, як сукупність фізичних пристроїв, оснащених датчиками, сенсорами та програмним забезпеченням, які збирають, передають та обмінюються даними дозволяє здійснювати керування вуличним освітленням і моніторинг ресурсів (тепло- та водопостачання) через хмарні платформи з віддаленим доступом.

Перевагами для післявоєнного відновлення українських міст з інтеграцією хмарних рішень є прозорість та економія. Можливість швидко масштабувати нові сервіси та підключати відновлені райони міст без потреби закуповувати високовартісне обладнання. У такий спосіб досягається зниження витрат на утримання IT-інфраструктури та прозора доступність аналітичних даних для громадян міст.

Практичне впровадження хмарних технологій за стандартами «розумне місто» (Smart City) в Україні може проілюструвати проєкти модернізації міської інфраструктури та системи «Безпечне місто». Адміністрація українських міст (зокрема, Київ, Харків, Луцьк) впроваджують елементи відеоспостереження та хмарних платформ для контролю за трафіком і громадським порядком. Вони активно інтегрують хмарні рішення для відмовостійкості, що також є основою для післявоєнної цифрової трансформації та відбудови інфраструктури за стандартами «розумне місто» (Smart City).

Впровадження хмарних технологій за стандартами «розумного міста» **(**Smart City) є ключовим інструментом для цифрової та післявоєнної трансформації відновлення міста Києва. Це дозволяє столиці перейти від застарілих локальних серверів на користь гнучкої, безпечної та масштабованої IT-інфраструктури.

Комплексне практичне застосування архітектурної інтеграції хмарних рішень для повоєнного відновлення столиці пропонується здійснювати на базовій моделі «Гібридна муніципальна хмара» (Kyiv City Hybrid Cloud). З метою

детальної аналітики та балансування між безпекою та інноваціями можна оптимально забезпечувати поєднання приватного міського дата-центру (для критичних персональних даних) та публічних хмарних сервісів (наприклад, іноземних операторів AWS, Microsoft Azure, Google Cloud або вітчизняного оператора De Novo).

Розумна інфраструктура є фундаментальною основою для розвитку сучасних українських міст за стандартами «розумне місто» (Smart City) в умовах повоєнної відбудови. Вона об'єднує традиційну фізичну інфраструктуру з цифровими технологіями, такими як Інтернет речі, штучний інтелект (AI), датчики та хмарні обчислення для оптимізації роботи в реальному часі.

Взаємодія з громадянами міста Києва може повністю здійснюватися через мобільний застосунок «Київ Цифровий» та міські сервіси, повністю спираючись на хмарну інфраструктуру. Це гарантує стабільність роботи під час різких пікових навантажень (наприклад, масове голосування за петиції чи сповіщення про надзвичайні ситуації). Smart City Cloud – це хмарні технології та цифрові платформи, які об'єднують міську інфраструктуру, пристрої Інтернету речей та служби управління в єдине цифрове середовище в реальному часі. Хмарні платформи забезпечують прозорий доступ міжнародних інвесторів до даних реєстрів руйнувань та використання коштів на відбудову, що мінімізує корупційні ризики.

За аналогією SAFECITY Івано-Франківськ (інтерактивна платформа Івано-Франківської міської ради) пропонуємо ініціювати створення платформи у місті Києві. Такі платформи призначені для оцінки безпеки міських просторів, позначення безпечних чи потенційно небезпечних зон та моніторингу комфорту пересування містом. Основні можливості платформи технологічно проявляються у формуванні карти безпеки. Користувачі можуть переглядати або самостійно додавати позначки на карті міста:

- зелена зона – безпечний простір (люди довкола, немає скритих зон чи перешкод);

- жовто-чорна зона – потенційно небезпечна зона (малолюдно, скриті зони, перешкоди або проблеми з благоустроєм).

Головна флагманська та всесвітньовідома ініціатива-проєкт Safecity некомерційної організації Red Dot Foundation – це краудсорсингова платформа (мобільний додаток та вебсайт), створена для боротьби з сексуальним та гендернозумовленим насильством у громадських місцях. Користувачі (переважно жінки та дівчата) можуть абсолютно анонімно повідомити про випадки сексуальних домагань, переслідувань, непристойних коментарів або насильства, вказавши точний час, дату та геолокацію. Отримані дані агрегуються та відображаються на інтерактивній мапі у вигляді «гарячих точок» (Hotspots). Очікується, що залученість у цей проєкт дозволить покращити безпеку в місті Києві і не тільки.

Організація Red Dot Foundation не просто збирає статистичні дані, а використовує їх як реальні інструменти змін та впливу на них. Фахівці організації співпрацюють з представниками поліції та місцевої влади. На основі карт співробітників організація доносить інформацію до представників органів місцевої влади та правоохоронців, щоб ті коригували маршрути патрулювання, покращували вуличне освітлення або облаштовували громадські вбиральні. Фахівці організації проводять навчальні тренінги та воркшопи для молоді та локальних лідерів, готуючи «амбасадорів безпеки». До проєкту активно залучаються особи чоловічої статі у діалог через програми гендерної чутливості, трансформуючи їх із потенційних правопорушників чи байдужих свідків на захисників безпечного простору.

Прогнозується, що впровадження хмарних технологій за стандартами «розумного міста» **(**Smart City) перетворить місто Київ на стійкий мегаполіс, здатний витримувати кризові навантаження. Це скорочує час ухвалення управлінських рішень у 5 разів та мінімізує витрати на обслуговування фізичної IT-інфраструктури

Рекомендовані напрями впровадження хмарних рішень для повоєнної відбудови інфраструктури міста Києва за стандартами «розумного міста» (Smart

City) (Додаток А) охоплюють єдиний міський масштабний державний цифровий проєкт та «Цифрових двійників», хмарний моніторинг, нейровідеоаналітику та хмарну безпеку (Safe City).

Цифрова повоєнна відбудова українських міст передбачає хмарні цифрові двійники та геоінформаційні системи. Хмарні цифрові двійники – це створення 3D-моделей зруйнованих або пошкоджених районів Києва на хмарних платформах. Це дозволяє симулювати архітектурні рішення та навантаження на мережі перед початком фізичного будівництва. Хмарні цифрові двійники – динамічна віртуальна модель реального фізичного об'єкта, процесу, системи або навіть всього Києва, яка оновлюється в реальному часі за допомогою даних із сенсорів та Інтернету речей. Це дозволяє архітекторам віртуально симулювати та планувати відновлення міста з урахуванням сучасних стандартів енергоефективності перед початком фізичних робіт.

Розміщення єдиної карти комунікацій (водопостачання, тепломережі, електромережі) здійснюватиметься на хмарній платформі. У разі пошкодження одного з вузлів геоінформаційної системи, решта автоматично прораховує сценарії перенаправлення ресурсів. Алгоритми хмарної платформи автоматично балансують навантаження на мережу, прогнозують можливі аварії та оперативно ізолюють пошкоджені ділянки.

В рамках системи «Безпечне місто» відеопотоки з великої кількості міських камер обробляються за допомогою штучного інтелекту на хмарних платформах. Це забезпечує автоматичне розпізнавання екстрених ситуацій, фіксацію руйнувань, контроль трафіку та пошук правопорушників. Нейровідеоаналітика – це технологія автоматизованого аналізу відеопотоку за допомогою штучного інтелекту та штучних нейронних мереж.

На відміну від класичної відеоаналітики, яка працює за жорстко заданими піксельними алгоритмами (наприклад, детекція руху), нейромережі здатні розпізнавати складні образи, класифікувати об'єкти та прогнозувати події подібно до людського зору. Датчики на мостах, шляхопроводах та у житлових будинках збирають дані про вібрації, просідання ґрунту або витоки води,

передаючи їх на хмарну платформу для миттєвого реагування муніципальних служб.

Енергоефективність комунальної сфери передбачає автоматизований облік ресурсів. Хмарні алгоритми аналізують дані Smart лічильників тепла та води в масштабах усього міста. Геоінформаційна система виявляє аномальні втрати (наприклад, приховані прориви труб) і оптимізує подачу енергії залежно від погодних умов. Хмарні IoT-платформи для збору даних у реальному часі через мережі LoRaWAN (бездротовий мережевий протокол з низьким енергоспоживанням, призначений для підключення пристроїв Інтернету речей на великі відстані).

Трирівнева інфраструктура є особливим архітектурним стандартом для створення масштабних національних рішень проєктів «Безпечне місто» (Додаток Б). Вона забезпечує стабільність, безпеку та здатність обробляти великі потоки інформації в режимі реального часу, що критично важливо для державних реєстрів, систем національної безпеки, екологічного моніторингу або розумних енергомереж.

Головне завдання на етапі моніторингу та обробки даних полягає у безперервному зборі первинної інформації з великої кількості географічно розподілених точок з подальшою передачею їх на наступний етап – обробки, аналізу та зберігання даних всієї системи. На цьому етапі накопичується, очищується та аналізується інформація. На національному рівні цей рівень зазвичай реалізується на базі розподілених хмарних технологій або мережі державних спеціально обладнаних приміщень, будівель чи комплексу споруд, що призначені для розміщення серверного, мережевого обладнання та систем зберігання даних. Рівень управління та прийняття рішень трансформує проаналізовані дані на конкретні дії, управлінські рішення чи автоматичні команди зворотного зв’язку. Ключові вимоги до архітектури трирівневої інфраструктури полягають у створенні масштабних національних рішень проєктів «Безпечне місто»:

- наскрізне шифрування (метод захисту даних, за якого інформація шифрується на пристрої відправника і може бути розшифрована лише на пристрої призначеного отримувача);
- нульова довіра (жоден користувач, пристрій чи мережеве з'єднання не вважаються надійними за замовчуванням, навіть якщо вони вже знаходяться всередині системи);
- розділення корпоративної мережі на окремі ізольовані зони;
- дублювання всіх вузлів;
- резервне копіювання, при якому копії даних зберігаються у географічно віддалених один від одного локаціях (наприклад, у різних містах України чи хмарних регіонах), що забезпечує гарантію виживання даних та безперервність підприємницької діяльності навіть у разі масштабних катастроф, які можуть повністю знищити основний центр обробки даних;
- здатність системи працювати автономно на рівні периферійних пристроїв у випадку зникнення зв'язку з центром;
- можливість маштабування, легко додаючи велику кількість нових датчиків або користувачів без перебудови ядра системи завдяки мікросервісній архітектурі;
- віртуалізація на рівні операційної системи, яка об'єднує застосунок разом із його бібліотеками, складовими та файлами конфігурації в один ізольований контейнер.

Периферійні обчислення – це архітектура розподілених обчислень, яка переносить обробку та зберігання даних ближче до джерела їхнього створення (до датчиків, пристроїв або локальних серверів користувачів), а не відправляє їх у віддалені централізовані дата-центри чи хмарні сховища.

«Розумні міста» – це Інтеграція периферійних обчислень з технологією 5G, що дозволяє автоматизувати керування трафіком, роботу вуличного освітлення та запуск дронів завдяки надшвидкісному мобільному зв'язку відповідно до стандартів «розумного міста» (Smart City). Периферійні обчислення не замінюють хмару повністю. Найчастіше вони працюють у гібридній моделі: периферія

відповідає за миттєві локальні рішення, а хмарні платформи – за довгострокове збереження даних, масштабну аналітику та глобальне навчання моделей штучного інтелекту

Шини обміну даними – це програмна інфраструктура, яка дозволяє різним інформаційним системам, реєстрам та додаткам взаємодіяти між собою за єдиними стандартами. Замість створення великої кількості окремих зв’язків між кожною парою програм, усі вони підключаються до однієї централізованої або децентралізованої шини.

Українська державна система «Трембіта» побудована на базі естонської технології X-Road. Це специфічний клас розподілених сервісних шин (децентралізованих платформ обміну), заточених під високі вимоги безпеки, юридичну силу повідомлень та взаємодію різних державних реєстрів. Кожен запит підписується електронною печаткою установи, шифрується, а центральний компонент лише фіксує сам факт обміну файлами, не бачачи змісту державних даних.

Технологія X-Road, розроблена в Естонії, стала міжнародним стандартом для побудови цифрових урядів (e-Government) [132]. Хмарні платформи працюють за принципом децентралізації: дані не копіюються в одне місце, а передаються напряму між учасниками у зашифрованому вигляді. Нове покоління української шини «Трембіта 2.0 (Україна)» впроваджує міжнародне шифрування (ECDSA, AES, SHA256) для майбутньої сумісності та обміну даними з аналогічними шинами країн ЄС. Система «Трембіта» маршрутизує запити, трансформує формати даних та забезпечує надійність доставки повідомлень, однак потребує розгортання власних серверів. Натоміть пропонуємо здійснити перехід на сучасні хмарні інтеграційні платформи класу iPaaS (Integration Platform as a Service) працюють повністю на базі хмарних технологій та дозволяють зв’язувати системи через спеціальні пристрої для швидкого, зручного та надійного з’єднання кабелів, проводів або електронних приладів між собою. До таких платформ належить Microsoft Azure Integration

Services – сукупність інструментів (Logic Apps, API Management, Service Bus) для побудови шин обміну в системі Microsoft.

Хмарні регіони в Україні як географічні зони розміщення великих дата-центрів глобальних гіперскейлерів (таких як Amazon Web Services, Microsoft Azure або Google Cloud) офіційно відсутні. Найближчі до України повноцінні хмарні кластери світових гігантів розташовані в країнах Центральної Європи, зокрема у містах Варшаві (Польща) та Франкфурті (Німеччина). Поняття «хмарних регіонів» та локальних зон доступності всередині України формується на базі національних провайдерів та їхньої інфраструктури.

Вітчизняний ринок хмарних послуг спирається на мережу географічно розподілених дата-центрів, переважно гарантує високий рівень надійності та відмовостійкості інфраструктури, зосереджених у двох ключових вузлах: Київському та Західноукранському. Київський регіон оцінюється як найбільший цифровий центр країни, де зосереджена основна кількість комерційних дата-центрів, які обслуговують хмарні сховища великих операторів. Західноукраїнський регіон з центром у місті Львів став критично важливою альтернативною зоною доступності. Сюди мігрувала значна частина інфраструктури для забезпечення відмовостійкості, дублювання даних та захисту від критичних руйнувань.

Національні лідери будують власні мультирегіональні архітектури, поєднуючи українські майданчики з європейськими для захисту підприємницьких та державних структур. Компанія GigaCloud вважається найбільшим хмарним оператором країни за обсягом доходу. Нею розгортається інфраструктура в зонах Києва, Львова та Познані/Варшави (Польща). Компанія De Novo надає хмарні сервіси (зокрема, з графічними процесорами для штучного інтелекту AI/ML) із локаціями у містах Києві та Львові, а також у Німеччині (міста Франкфурт та Карлсруе).

Дата-центр «Парковий» має власну інфраструктуру в Києві та захищені резервні майданчики в європейських країнах. Компанії UCloud та Tucha пропонують диверсифіковані локальні та закордонні хмарні потужності.

Для посилення стійкості провідні гравці ринку (компанії GigaCloud, De Novo, дата-центр «Парковий») створили Альянс цифрового суверенітету України (DSUA). Вони розвивають та інтегрують географічно розподілену мережу високої доступності всередині країни для надійного контролю та збереження стратегічних державних і корпоративних даних.

Сучасний ринок систем безпеки демонструє стрімкий перехід від пасивного, технологіями штучного інтелекту та розпізнавання облич, до активного, що вже стала стандартом. Зміна архітектури з граничного штучного інтелекту, який передбачає впровадження алгоритмів та моделей нейромереж безпосередньо на локальних периферійних пристроях у хмарні технології. Найважливішим технологічним трендом є перенесення аналітичних потужностей безпосередньо на процесор камери. Сучасні Smart-камери оснащені нейропроцесорами (NPU), які дозволяють обробляти та порівнювати біометричні дані локально, без необхідності постійного надсилання важкого відеопотоку на сервер чи реєстратор (NVR). Переваги застосування граничного штучного інтелекту на базі хмарних технологій полягає в швидкості обробки подій. Камера надсилає в хмару/центр моніторингу не гігабайти відео, а лише легкі метадані та крихітні фото-«кропи» знайдених облич, що економить трафік. Система продовжує автономно функціонувати навіть у разі відсутності Інтернет-з'єднання.

Сучасні комплекси відеоаналітики вирішують завдання у трьох основних напрямах (табл. 3.4): безпека та системи контролю і управління доступом, розумне місто (Smart City), розумний дім та рітейл.

Таблиця 3.4

Ключові сфери застосування та функціональні можливості сучасних комплексів відеоаналітики

Сфера застосування	Основні сценарії інтеграції	Переваги
Безпека та системи контролю і управління доступом	Заміна фізичних перепусток на біометричне розпізнавання. Створення «чорних» та «білих» списків клієнтів/персоналу.	Висока точність, неможливість підробити чи передати перепустку іншій особі.
Розумне місто (Smart City)	Відстеження людей за допомогою декількох камер одночасно (Multi-camera Tracking / Re-Identification), пошук зниклих або правопорушників.	Можливість вести пошук за прикметами (колір одягу, стать, вік), навіть якщо обличчя частково перекрите.
Розумний дім та рітейл	Ідентифікація мешканців будинку (нові розробки Apple, Google Nest, Amazon Ring) або VIP-клієнтів у магазинах.	Персоналізація сервісу, автоматичне зняття будинку з охорони для членів родини.

Джерело: складено автором на основі проведених досліджень

Інтеграція розпізнавання облич у Smart-камер повністю змінила підхід до безпеки. Технологія зміщується в бік автономних AI-камер, які не просто фіксують картинку, а миттєво розуміють контекст, мінімізуючи навантаження на мережу та хмарні сховища. Сучасне обладнання лідерів ринку (табл. 3.6) на базі штучного інтелекту здатне:

- підтримувати бази даних обсягом понад 100000 знімків на локальних серверах чи реєстраторах;
- одночасно розпізнавати десятки облич в одному кадрі в умовах щільного потоку людей;
- нівелювати спроби обману системи за допомогою роздрукованих фотографій чи масок завдяки технології Liveness Detection (перевірка людини за допомогою 3D-мапування або інфрачервоних датчиків).

Компанії Hikvision, Dahua та Incoresoft – це провідні бренди у сфері відеоспостереження та безпеки. Компанії Hikvision та Dahua є глобальними

гігантами з виробництва апаратного забезпечення (камер та реєстраторів), а компанія Incoresoft є розробником інтелектуального програмного забезпечення. Головний зв'язок між ними полягає в технологічній інтеграції: програмна платформа відеоменеджменту (VMS) та модулі штучного інтелекту VEZHA від компанії Incoresoft створені для безперевної роботи з потоками ONVIF/RTSP від камер брендів Hikvision та Dahua без потреби заміни наявної інфраструктури обладнання.

Таблиця 3.5

Порівняльна характеристика ролей спеціалізацій забезпечення у проєктах «Безпечне місто»

Компанія / бренд	Основна спеціалізація	Роль у системі відеоспостереження
Hikvision	Апаратне забезпечення (IP-камери, NVR, системи контролю доступу)	Постачальник фізичних камер та первинної бортової аналітики (наприклад, AcuSense).
Dahua	Апаратне забезпечення (камери, реєстратори WizSense/TiOC)	Постачальник пристроїв фіксації відеопотоку та інфраструктурних рішень.
Incoresoft	Програмне забезпечення (VMS, AI-аналітика [VEZHA AI Engine])	Система агрегує відео з камер Dahua/Hikvision та запускає розширену аналітику (розпізнавання облич, номерів, детекція зброї, вогню тощо).

Джерело: складено автором на основі проведених досліджень

Камери брендів Hikvision або Dahua фіксують зображення на об'єкті та транслюють його. Потік відео передається за універсальними протоколами ONVIF/RTSP на сервери. Система Incoresoft VMS приймає ці потоки та за допомогою нейромереж виконує надточний аналіз подій за долі секунди. Це дозволяє наділяти навіть старі моделі китайських камер функціями стандартів «розумного міста» (Smart City) в рамках проєктів «Безпечне місто».

Головними стримуючими факторами запровадженням-провідних брендів у сфері відеоспостереження та безпеки приватніості, якості зображення та освітлення. В Україні питання масштабного розгортання та збереження баз даних облич усе ще перебуває у процесі законодавчо-правового врегулювання, що викликає занепокоєння правозахисників. Для коректного розпізнавання

облич потрібна правильна роздільна здатність камери (кількість пікселів на обличчя особі має бути не менше 40-100 пікселів), правильний кут нахилу та якісне інфрачервоне підсвічування для нічного часу.

Інтелектуальні системи інтеграції відеоданих відіграють критичну роль у сучасній координації служб порятунку, забезпечуючи перехід від пасивного спостереження до проактивного реагування в режимі реального часу (табл. 3.8). Вони об'єднують потоки з тисяч камер (міських, автомобільних, камер на тілі, дронів) в єдине цифрове середовище для прийняття рішень. Інтелектуальні системи інтеграції відеоданих кардинально прискорюють функціонування таких напрямів:

1. Миттєве автоматичне розпізнавання загроз та фільтрація хибних інцидентів. Штучний інтелект у реальному часі аналізує відеопотоки й автоматично виявляє задимлення, вогонь, ДТП, залишені предмети або скупчення людей. Система зіставляє дані з повідомлень громадян із відеокамерами поруч, дозволяючи диспетчеру за секунди підтвердити масштаб аварії без виїзду розвідки.

2. Оптимізація маршрутів на основі аналізу дорожньої ситуації та керування світлофорами. Інтелектуальні системи аналізують та оцінюють затори та автоматично коригують маршрути для спеціального транспорту (карети швидких допомог, пожежних машин). Інтеграція з інтелектуальними системами, які функціонують за стандартами «розумного міста» (Smart City), дозволяє автоматично створювати умови для проїзду екстрених служб на основі їхнього поточного геолокаційного треку та відео з перехресть.

3. Ситуаційна обізнаність на місці події, що досягається передачею відеопотоку з дронів та натільних камер. Координаційні центри отримують картинку безпосередньо з місця надзвичайної ситуації. Це допомагає оцінити конструктивні руйнування будівель, поширення вогню чи хімічної загрози ще до того, як основні рятувальники прибудуть на місце. Відеодані в інфрачервоному спектрі допомагають знаходити постраждалих під завалами або в умовах щільного задимлення.

4. Ефективний розподіл ресурсів на основі прогнозування масштабу події. За результатами візуального аналізу (наприклад, щільності натовпу чи інтенсивності горіння) система рекомендує кількість бригад, техніки чи специфічного обладнання (драбини, детоксикаційні набори) потрібно відправити.

Таблиця 3.6

Порівняльння підходів впровадження інтелектуальних систем

Параметр	**Традиційний підхід**	**Підхід з інтелектуальною інтеграцією відео**
Час виявлення надзвичайних ситуацій	Очікування дзвінка від очевидців (від 5 до 15 хвилин)	Автоматично (до 10-30 секунд)
Оцінка ситуації	Зі слів очевидців або після прибуття першого екіпажу	Дистанційно, ще в процесі руху екіпажів
Побудова маршруту	Навігатори загального користування	Динамічний «зелений коридор» з урахуванням габаритів

Джерело: складено автором на основі проведених досліджень

Оцінка ефективності вітчизняних програмних рішень у сфері відеоаналітики, особливо в контексті «Безпечне місто». залежить від технічних метрик алгоритмів, економічної доцільності та специфіки інтеграції у наявну інфраструктуру.

Таблиця 3.7

Критерії оцінки ефективності вітчизняних програмних рішень із зарубіжними аналогами

Критерій оцінки	**Українські рішення**	**Зарубіжні аналоги**
Точність розпізнавання	Висока в специфічних умовах. Алгоритми чудово адаптовані під місцеві реалії (українські номери авто, специфіка облич, різновиди камуфляжу, типи дронів/техніки).	Стабільно висока загальна точність. Мають величезні сукупності даних для навчання, але можуть «помилятися» на специфічних локальних об’єктах.
Кібербезпека та суверенність	Максимальна. Відсутній ризик витоку даних за межі країни. Повністю контрольований код.	Залежить від вендора. Західні рішення (Milestone, Axis) безпечні, але дорогі. Азійські рішення мають санкційні ризики (наприклад, китайські Hikvision/Dahua).

Продовження табл. 3.7

Гнучкість та адаптація	Дуже висока. Вітчизняні розробники готові швидко доопрацьовувати програмне забезпечення під конкретні завдання або інтегрувати його з локальними системами управління відносинами та планування ресурсів.	Низька або помірна. Великі корпорації рідко змінюють базовий алгоритм під індивідуального замовника.
Загальна сума всіх витрат	Оптимальна. Нижча вартість ліцензій та впровадження. Відсутність митних зборів та простіша логістика підтримки.	Висока. Прив'язка до валюти, висока вартість підписки програмного забезпечення як послуги та сервісного обслуговування.

Джерело: складено автором на основі проведених досліджень

Вітчизняні рішення відеоаналітики є максимально ефективними та безальтернативними у сферах, де критично важливі національна безпека, незалежність від імпорту, захист даних та адаптація під унікальні українські реалії (табл. 3.7). У комерційному секторі рішення відеоаналітики виграють за рахунок гнучкості та ціни, хоча інколи поступаються глобальним рішенням за обсягом взаємопов'язаних каналів, інструментів, платформ, даних і партнерів, які функціонують разом, замість проведення окремих ізольованих функцій.

Для започаткування українського технологічного бізнесу рекомендуємо застосування Дія.City – це спеціальний правовий та податковий простір, який функціонує щонайменше на 25 років. Формами працевлаштування є спеціальна форма для ІТ-індустрії (Гіґ-контракти), трудові контракти відповідно до Кодексу законів про працю [34] та співпраця з ФОП (фізичними особами-підприємцями). Основні податкові форми охоплює: податок на прибуток (9% – податок на виведений капітал) або 18% на загальних підставах, 5% – податок на доходи фізичних осіб, єдиний соціальний внесок, який складає 22% від мінімальної заробітної плати, військовий збір у розмірі 5%. Частка кваліфікованого доходу щодо здійснення профільних видів ІТ-діяльності складає від 90%. Середньомісячна винагорода працівникам і гіґ-фахівцям становить від 1200 євро.

Кількість працівників та гіґ-спеціалістів – від 9 осіб. Для стартапів вимоги до кількості штату відсутні.

Однією з ключових сфер найефективнішого застосування вітчизняних рішень відеоаналітики є цивільна безпека в рамках концепції «Безпечне місто». Вітчизняні модулі розпізнавання номерних знаків (LPR), облич, фіксації порушень правил дорожнього руху та аналізу скупчень людей функціонують на рівні світових стандартів, забезпечуючи швидкий пошук у реєстрах.

Головні проблеми впровадження хмарних технологій у проєктах «Безпечне місто» полягають у відсутності масштабної сукупності структурованої бази даних, а також залежності від іноземного обладнання. Українське програмне забезпечення функціонує на виключно імпортних обчислювальних чипах та графічних процесорах, що впливає на кінцеву вартість комплексу. Для цивільних комерційних завдань великі іноземні компанії мають більше досвіду роботи з даними, через що їхні нейромережі штучного інтелекту в декілька разів швидше навчаються загальним завданням.

Основні переваги функцій хмарних технологій у проєктах «Безпечне місто» полягають у переході у формат «розумного міста» (Smart City) після повоєнного відновлення. Представники місцевих органів влади можуть швидко (за декілька днів) запускати цифрові послуги та реєстри, оскільки ресурси виділяються миттєво за запитом. Сучасні українські хмарні середовища мають офіційні атестати безпеки даних (зокрема, в Комплексній системі захисту інформації та відповідність стандартам Державного спеціального зв'язку), що, у свою чергу, мінімізує ризики втрати баз даних.

Ключові переваги хмарного підходу для повоєнного відновлення будь-якого українського міста полягають у цифровому суверенітеті та безпеці, економічній гнучкості та швидкості розгортання. У такий спосіб дані реєстрів міст захищені від фізичного знищення завдяки дублюванню на європейських хмарних серверах. Оплачується лише за реально використані хмарні потужності (модель Pay-as-you-go), уникаючи великих капітальних витрат на закупівлю серверної матеріальної бази при дефіциті бюджету. Нові сервіси та системи

моніторингу швидко запускаються, прискорюючи темпи повоєнної відбудови українських міст.

3.3. Напрями підвищення ефективності процесу управління українськими населеними пунктами із застосуванням системи «Безпечне місто»

Підвищення ефективності управління українськими населеними пунктами за допомогою інформаційно-аналітичного комплексу є ключовою складовою розвитку концепції «Безпечне місто» за стандартами «розумне місто» (Smart City) [105; 228]. У сучасних умовах проєкт трансформується з локального інструменту фіксації правопорушень в інтегрований механізм управління життєдіяльністю українських міст та виявлення національних загроз. Основними напрямами підвищення ефективності цього процесу є впровадження штучного інтелекту та інтелектуальної відеоаналітики, оптимізація міжвідомчої взаємодії та координації служб, розширення функціоналу проєкту «Безпечне місто» на житлово-комунальну сферу та нормативно-правове регулювання та залучення місцян.

Впровадження штучного інтелекту та інтелектуальної відеоаналітики забезпечує автоматичне розпізнавання об’єктів шляхом використання алгоритмів для ідентифікації номерних знаків, марок автомобілів, облич та типів транспортних засобів у реальному часі [102]. Сповіщення служб здійснюється при виявленні нетипової поведінки, скупчення людей, залишених речей, актів вандалізму або перебування осіб у заборонених зонах. Прогнозування та аналіз ризиків дозволили здійснити перехід від фіксації подій («постфактум») до моделювання та попередження загроз на основі накопичених Big Data.

Оптимізація міжвідомчої взаємодії та координації служб передбачає створення єдиного ситуаційного центру, де інтегровано дані у спільний інформаційний простір для одночасного доступу представників органів місцевого самоврядування, національної поліції, ДСНС та комунальних служб.

Автоматизація алгоритмів реагування дозволяє миттєво передати сигнал тривоги від аналітичних модулів до найближчого патруля або диспетчера відповідної служби. Усунення дублювання функцій забезпечує розмежування прав доступу та взаємообмін даними для уникнення хаотичних дій під час надзвичайних ситуацій.

Розширення функціоналу проєкту «Безпечне місто» на житлово-комунальну сфери дозволяє здійснювати контроль комунального транспорту моніторинг (роботи снігоприбиральної техніки, сміттєвозів та громадського транспорту) та керування трафіком шляхом оптимізації роботи світлофорів міста на основі аналізу щільності транспортних потоків для зменшення заторів.

Кіберзахист забезпечує здатність системи продовжувати стабільну роботу та виконувати свої функції навіть у разі виникнення збоїв, помилок або виходу з ладу окремих її компонентів міської інфраструктури. Захист каналів зв'язку здійснюється за допомогою впровадження надійних протоколів шифрування для запобігання несанкціонованому доступу до відеопотоків та баз даних.

Енергонезалежність вузлів забезпечує резервне живлення (акумулятори, сонячні панелі, генератори) для критичних камер та серверного обладнання в умовах дефіциту електроенергії шляхом застосування акумуляторів, сонячних панелей, генераторів. Локальне збереження даних може здійснюватися за допомогою використання гібридних схем запису (на внутрішню пам'ять камер та у центр обробки даних на хмарній платформі) для уникнення втрати інформації у разі обриву мережі.

Нормативно-правове регулювання передбачає стандартизацію технічних вимог, що в свою чергу, означає розробку єдиних регламентів для підключення приватних камер (торгово-розважальних центрів, заправок, об'єднання співвласників багатоповерхових будинків) до міської системи. Дотримання прав громадян в контексті чіткості правового регулювання охоплює зберігання й використання біометричних даних та відеоархівів з метою балансу між безпекою та приватністю. Створення інтерактивних карт безпеки чи мобільних застосунків

здійснюється для того, щоб мешканці могли повідомляти про небезпеку різного роду.

Трансформація розрізнених систем відеоспостереження в єдину систему відеомоніторингу стану публічної безпеки в Україні є стратегічним кроком для створення загальнодержавного механізму координації. Масштаб системи передбачає об'єднання близько 50 тисяч камер по всій країні [140]. Цей процес перетворює пасивне фіксування подій на активний аналітичний інструмент управління безпекою в реальному часі, що є критично важливим в умовах воєнного стану та повоєнного відновлення [127]. Замість великої кількості автономних локальних камер архітектурно створюється єдиний інформаційний простір, який розподіляється на три рівні:

- центральний рівень, що адмініструється Міністерством внутрішніх справ України (МВС) і є головним координаційним центром;
- місцевий рівень, що базуються на проєктах «Безпечне місто»;
- відомчий рівень, що охоплює камери підприємств, установ, організацій та об'єктів інфраструктури, що розташовані у публічних місцях.

Головна зміна функціональних систем відеоспостереження можливостей полягає у переході від простого запису до відеоаналітики з елементами штучного інтелекту. Система координує реагування за допомогою функцій:

- автоматичного розпізнавання облич, державних номерних знаків, а також ідентифікація автомобілів за маркою та кольором;
- виявлення загроз (фіксація вибухів, задимлень, спалахів, порушень периметрів безпеки чи наявності несанкціонованого залишення предметів);
- інтеграція з іншими державними реєстрами (зокрема, Єдиним демографічним реєстром) для швидкої ідентифікації осіб під час розшуку чи виявлення диверсійно-розвідувальних груп.

Державний механізм координації кібербезпеки та технологічної незалежності суворо регламентує програмне та апаратне забезпечення. Повністю виключено використання програмного забезпечення, виготовленого в Російській Федерації чи країнах, що її підтримують. Користувачами системи, насамперед є

представники Національної поліції, які отримують жорстко контрольовані права доступу. Кожен перегляд фіксується логами, а за витік інформації передбачено кримінальну відповідальність. Логами називають автоматично створені текстові або бінарні файли, які фіксують хронологію подій, операцій, помилок та стану роботи операційної системи, вебсервера чи програми.

Трансформація викликає активні суспільні дискусії щодо дотримання прав людини в рамках балансування між безпекою та приватністю. Законодавче врегулювання закріплює певні запобіжні заходи. Персональні та біометричні дані зберігатимуться не більше 15 років, після чого підлягають обов'язковому знеособленню. Громадяни мають право дізнатися, чи внесені їхні дані до системи, та вимагати їхнього оновлення чи виправлення.

Проєкти «Безпечне місто» є важливою складовою сучасного розвитку соціальної політики держави, спрямованої на місцевому рівні на захист прав та безпеки дітей, запобігання насильству, розвиток сімейних форм виховання та створення інклюзивного, дружнього до дитини середовища. Основні напрями захисту прав дітей в рамках проєктів «Безпечне місто» охоплюють цифрову та фізичну безпеку, правосуддя, підтримку містян.

Впровадження субпроєктів «Безпечна школа» та «Безпечний двір» – це ефективні інструменти для створення захищеного простору в українських містах через поєднання сучасних технологій, інфраструктурних змін та активної співпраці мешканців із правоохоронцями.

Субпроєкт «Безпечний двір» спрямований на зниження рівня злочинності (крадіжки, вандалізм), підвищення комфорту проживання та захист майна мешканців багатоквартирних будинків. Цей субпроєкт охоплює відеонагляд, фізичний бар'єр та освітлення, а також соціальний аспект. Відеонагляд передбачає перекриття камерами входів у під'їзди, дитячих майданчиків, паркінгів для автомобілів; зберігання архівів відео на хмарних платформах з доступом для мешканців та правоохоронців.

Фізичний бар'єр та освітлення означає встановлення розумних домофонів (із відеозв'язком через додаток у смартфоні), облаштування шлагбаумів або

автоматичних воріт для обмеження в'їзду стороннього транспорту та якісне LED-освітлення всієї прибудинкової території із датчиками руху. Соціальний аспект реалізації субпроєкту «Безпечний двір» має передбачати створення чатів будинку для оперативної взаємодії сусідів, залучення дільничного офіцера поліції до координації безпеки.

Головна мета реалізація субпроєкту «Безпечна школа» полягає у створенні захищеного середовища для дітей та освітян, мінімізація ризиків зовнішніх загроз та внутрішніх конфліктів (булінгу). Цифровий моніторинг безпеки охоплює заходи встановлення камер відеоспостереження на подвір'ях, у коридорах та спільних зонах, інтеграція камер із локальними ситуаційними центрами або головними управліннями та районними відділами поліції.

Контроль доступу до навчального закладу може досягатися впровадження електронних перепусток (турнікетів) для учнів та персоналу, а також запровадження автоматичного SMS або Viber сповіщення батьків про час приходу та виходу дитини з приміщення школи.

В сучасних умовах критично важливим є забезпечення цивільного захисту шляхом облаштування сучасних, сертифікованих укриттів, встановлення систем автоматичного сповіщення про тривогу, навігаційних покажчиків та оснащення «тривожними кнопками» для швидкого виклику представників охорони або поліції.

Встановлення систем відеоспостереження на вулицях і біля навчальних закладів, запровадження інноваційних систем швидкого сповіщення про зникнення дітей (наприклад, міжнародних платформ пошуку). Створення спеціальних просторів та проєктів на кшталт «Зелених кімнат» для безпечного опитування неповнолітніх, які стали жертвами або свідками насильства. Інтеграція соціальних послуг на рівні муніципалітетів, робота мультидисциплінарних команд та служба у справах дітей задля підтримки сімей у складних життєвих обставинах.

Контроль прилеглих територій навчальних закладів, захист від розповсюдження заборонених речовин та запобігання дитячому травматизму.

Опосередковано для безпеки дітей інфраструктурний фокус має бути спрямований на забезпечення відеоспостереження поблизу шкіл, дитячих садочків та дитячих майданчиків, а також на інтеграцію систем моніторингу для захисту громадських місць, де бувають діти.

Програми «Безпечне місто» зазвичай зосереджені на інфраструктурі та безпеці (відеоспостереження, аналітика), до яких залучають молодь і дітей через освітні та ігрові ініціативи [201]. Основні освітні напрями ігрових заходів для дітей і молоді можуть охоплювати пізнавальні квести «Місія: Безпечне місто» (для школярів 5–9 класів), де навчають орієнтуватися у кризових чи безпечних ситуаціях, а також тренінги з безпеки дорожнього руху та поведінки у міському просторі. Доцільним є розширення масштабів реалізації молодіжних проєктних ініціатив «Молодь в дії. Безпечне місто» у партнерствах із донорами, наприклад, UNICEF у Львові чи Полтаві. В рамках проєктів підлітки досліджують міський простір, створюють інтерактивні мапи безпечних маршрутів або планують зміни за принципами тактичного урбанізму.

Етапи впровадження субпроєктів «Безпечна школа» та «Безпечний двір»:

1. Визначення найбільш вразливих місць (де немає світла, де найчастіше збираються підозрілі особи).

2. Залучення фінансування проєктів можуть реалізовуватися через: бюджет участі міста (громадський бюджет); цільові муніципальні програми (в тому числі, програма «Безпечне місто»), співфінансування для дворів (кошти об’єднання співвласників багатоквартирного будинку та місцевий бюджет), гранти від міжнародних донорів.

3. Розробка технічного завдання та проєктування. Важливо одразу визначати обладнання, яке можна інтегрувати в єдину цифрову мережу міста.

4. Монтаж та тестування обладнання, передача прав доступу, навчання відповідальних осіб.

Створення міських координаційних рад та розробка локальних нормативно-правових актів є ключовими інструментами для інтеграції проєктів

«Безпечне місто» у місцеві бюджети, що гарантує їхнє стале фінансування та незалежність від донорських коштів.

Мета створення міських координаційних рад як консультативно-дорадчого органу при виконавчому комітеті місцевої ради полягає у об'єднанні зусиль представників органів влади, надавачів послуг, громадськості та експертів в рамках проєкту «Безпечне місто». Ініціювання створення муніципальних координаційних рад може здійснюватися в рамках проведення круглих столів або робочих зустрічей із ключовими стейкхолдерами (департаментом соціального захисту, охорони здоров'я, фінансового управління, громадських організацій).

Положення про міську координаційну раду як документ визначає мету, завдання, права та склад ради. Офіційне ухвалення та затвердження Положення та персонального складу міських координаційних рад з питань проєкту «Безпечне місто» може здійснюватися розпорядженням міського голови або рішенням виконавчого комітету міської ради. Пропонований типовий склад міської координаційної ради з питань проєкту «Безпечне місто»:

1. Голова ради (заступник голови громади з профільних питань).
2. Представники профільних управлінь (фінансів, соціального захисту, охорони здоров'я).
3. Керівники комунальних установ та закладів.
4. Представники неурядових організацій, які безпосередньо надають або адмініструють сервіси.

Щоб діяльність місцевої координаційної ради з питань проєкту «Безпечне місто» фінансувалася з місцевого бюджету, її необхідно легалізувати у правовому полі міста. Для цього здійснюється розробка пакету ключових документів місцевих нормативно-правових актів, який складається з:

1. Місцевої цільової програми (або внесення змін до чинної програми, наприклад, Програми соціально-економічного розвитку чи програми «Турбота»), що є основним документом, який обґрунтовує фінансування.

2. Сукупності правил, інструкцій або норм, що визначають порядок ведення зборів, засідань, роботу місцевої координаційної ради з питань проєкту «Безпечне місто». Чіткий опис того, хто є отримувачем доходу, яка процедура надання послуги та які критерії оцінки її якості.

3. Обґрунтування вартості послуг місцевої координаційної ради з питань проєкту «Безпечне місто» – це офіційний документ або аналітична складова (калькуляція), яка пояснює та підтверджує доцільність, структуру та розмір витрат, пов'язаних із забезпеченням діяльності або наданням послуг консультативно-дорадчими й координаційними органами на рівні міста.

Оскільки координаційні ради з питань проєкту «Безпечне місто», зазвичай, створюються як дорадчий центр при органах місцевого самоврядування та функціонуватиме на громадських засадах, обґрунтування вартості застосовується у двох випадках: у разі закупівлі послуг з організації/фасилітації роботи рад через систему Prozorro або при розрахунку бюджетних асигнувань на утримання та забезпечення діяльності ради (експертиза, технічний супровід). Розрахунок вартості базується на формуванні економічно обґрунтованих витрат (собівартості) без урахування прибутку (рентабельності).

У таблиці 3.8 наведено покроковий алгоритм дій, структуру нормативної бази та механізми забезпечення фінансової стабільності послуг міської координаційної ради з питань проєкту «Безпечне місто».

Таблиця 3.8

Етапи формування міської координаційної ради з питань проєкту «Безпечне місто»

Етап	Сутність	Результат
1	Оцінка потреб міста та картування наявних сервісів	Звіт із розрахованою вартістю сервісів
2	Створення та запуск міської координаційної ради	Розпорядження голови міста, розробка та затверджене Положення про міські координаційні ради
3	Розробка проєкту місцевої цільової програми / змін до неї	Готовий проєкт (нормативно-правовий акт із бюджетним запитом)

Продовження табл. 3.8

4	Цілеспрямований та системний процес просування та погодження проєкту в бюджетній комісії ради	Погодження профільною та бюджетною комісіями
5	Голосування на сесії місцевої ради	Рішення ради про виділення коштів з місцевого бюджету

Джерело: складено автором на основі проведених досліджень

Просте, внесення послуги до програми не гарантує автоматичного виділення коштів та забезпечення сталого фінансування. Рекомендовано задіяти інші бюджетні механізми:

1. Соціальне замовлення приховує механізм, за якого закупівля соціальних послуг відбувається на конкурсній основі серед неурядових організацій за кошти місцевого бюджету (відповідно до Закону України «Про соціальні послуги») [16].

2. Фінансова підтримка неурядових організацій шляхом виділення прямих субсидій або грантів із місцевого бюджету громадським організаціям, які виконують важливі сервісні функції для міста.

3. Створення штатної одиниці або профільного підрозділу всередині комунального некомерційного підприємства або установаи (наприклад, територіального центру соціального обслуговування чи центру надання соціальних послуг).

Децентралізація міських вузлів – це стратегія сучасного містобудування, яка передбачає відмову від класичної моделі міста з одним домінуючим центром (моноцентризм) на користь створення мережі автономних, багатофункціональних районів (поліцентризм) (табл. 3.9). Головна мета цього підходу полягає у зниженні навантаження на історичний чи діловий центр міста, рівномірно розподілити ресурси та покращити якість життя мешканців. Основні принципи децентралізації міських вузлів:

- концепція «15-хвилинного міста» означає, що усі базові потреби мешканців (робота, навчання, медицина, торгівля, відпочинок) мають бути доступні в межах 15 хвилин пішки або на велосипеді від дому;
- багатофункціональність передбачає те, що кожен міський вузол (район) поєднує житлову забудову, офіси, культурні простори та зелені зони, уникаючи появи суто «спальних» районів;
- транзитно-орієнтоване проєктування – концепція міського планування, яка передбачає максимальне збільшення кількості житлових, комерційних та відпочинкових зон у межах пішої доступності (зазвичай 400–800 метрів) від станцій громадського транспорту. Її мета полягає у зменшенні залежності містян від приватних автомобілів та популяризації громадського транспорту, велосипедні та піші прогулянки. Нові вузли розвитку формуються навколо великих центрів громадського транспорту (станцій метро, транспортно-логістичний центрів, швидкісного трамвая).

Таблиця 3.9

Порівняння моделей міської структури українських міст

Характеристика	**Моноцентричне місто (центр та околиці)**	**Децентралізоване місто (поліцентричне)**
Транспортне навантаження	Високе (маятникова міграція вранці та ввечері)	Низьке (рух розподілений рівномірно по всьому місту)
Екологічний стан	Загазованість центру, затори	Менше викидів завдяки пішохідній доступності
Інфраструктура	Концентрується переважно в центрі	Рівномірно розвинена в кожному підцентрі
Стійкість до криз	Низька (збій у центрі паралізує все місто)	Висока (райони можуть функціонувати автономно)

Джерело: складено автором на основі проведених досліджень

Децентралізація міських вузлів для мешканців має економічні, соціальні та екологічні переваги. Знижуються витрати на будівництво та ремонт надважких транспортних магістралей до центру. Розвивається локальний малий та середній бізнес. Зменшується соціальна нерівність між «престижним центром» та «занедбаними околицями». Мешканці мають однаковий доступ до культури та

послуг. Зменшення часу перебування в дорозі передбачає зниження стресу та покращення здоров'я людей, а також більш чисте повітря в місті.

Проблеми реалізації поліцентричної міської структури полягають в складності процесів управління інерцією інфраструктури та джентрифікації. Перебудувати вже існуюче моноцентричне місто надзвичайно дорого. Інерція інфраструктури – це економічний, технологічний та соціальний феномен, при якому існуючі системи штучного середовища (дороги, електромережі, будівлі, трубопроводи) чинять опір змінам і консервують старі моделі розвитку на десятиліття вперед через свою капіталомісткість та тривалий термін служби. Сучасне будівництво визначає спосіб життя, та економіку на наступні 30–50 років, навіть якщо технології та потреби суспільства кардинально зміняться.

Об'єкти інфраструктури (наприклад, залізниці чи ГЕС) високовартісні та розраховані на роботу протягом 50-100 років. Демонтувати їх раніше, ніж вони окупляться, економічно невигідно. Коли система вже побудована, усі наступні інновації доводиться адаптувати під неї. Так, в Україні важко масово перейти на водневий транспорт, якщо вся країна покрита мережею традиційних АЗС. Нормативно-правова база та державні будівельні норми, стандарти безпеки та звички обслуговуючого персоналу формуються навколо наявних технологій. Зміна цих факторів є переважно довготривалою.

Джентрифікація (табл. 3.10) – це процес реконструкції та оновлення старих або депресивних міських кварталів на новий якісний вузол, який супроводжується різким підвищенням цін на нерухомість і поступовим витісненням менш заможних корінних мешканців на більш заможних жителів.

Таблиця 3.10

Етапи розвитку джентрифікації в українських містах

Хвиля	Тенденції
Перша (піонери)	До району переїжджають митці, студенти, журналісти та молоді спеціалісти, яких приваблюють низькі ціни на житло. Вони створюють творчу атмосферу, відкривають кав'ярні та галереї.
Друга хвиля (інвестори та середній клас)	Район стає модним, з'являються девелопери, ресторани та бізнес. Житло дорожчає.
Завершення	Зростання орендної плати змушує перших мешканців та бідніші родини переїжджати в інші, дешевші райони

Джерело: складено автором на основі проведених досліджень

Інерція інфраструктури та джентрифікації потребує сильного локального самоврядування (на рівні районів) та чіткої координації з головною адміністацією.

Децентралізація міських вузлів (або створення поліцентричної міської структури) – це модель розвитку міста, яка передбачає відмову від одного домінуючого центру на користь кількох самодостатніх багатофункціональних районів (вузлів). Кожен такий вузол має власну житлову, комерційну, соціальну та культурну інфраструктуру, що дозволяє реалізувати концепцію «15-хвилинного міста». Для українських міст, особливо в контексті повоєнного відновлення та модернізації, ця модель є надзвичайно актуальною.

Таблиця 3.11

Порівняльний аналіз традиційної моноцентричної та поліцентричної моделей міст

Критерій	**Моноцентрична модель (поточна в більшості міст України)**	**Поліцентрична модель (децентралізовані вузли)**
Транспортне навантаження	Надмірне; маятникова міграція «околиця-центр» зранку та ввечері.	Рівномірне; більшість поїздок відбуваються всередині району.
Екологія та простір	Загазованість центру, занедбаність «спальних» районів.	Менше викидів, розвинені зелені зони в кожному вузлі.
Стійкість до криз	Низька; ураження центральних комунікацій чи вузлів паралізує все місто.	Висока; кожен вузол автономний і може функціонувати самостійно.
Доступ до послуг	Культурні та адміністративні послуги сконцентровані в центрі.	Рівний доступ до послуг, робочих місць та дозвілля всюди.

Джерело: складено автором на основі проведених досліджень

Переваги застосування створення поліцентричної міської структури в Україні охоплюють повоєнну відбудову та модернізацію, підвищення безпекової стійкості, транспортне розванаження та відновлення об’єктів, які втратили своє первісне призначення (табл. 3.11).

Для міст, які зазнали значних руйнувань (Маріуполь, Харків, Чернігів, Салтівка як окремий масив тощо), децентралізація вузлів – це можливість будувати «з нуля» за сучасними європейськими стандартами. Замість

відновлення застарілих радянських спальних районів можна створювати нові автономні мікроцентри.

В умовах воєнних загроз моноцентричне місто є вразливим. Розосередження критичної інфраструктури, адміністративних центрів (ЦНАПів), медичних закладів та енергетичних потужностей (мініТЕЦ, сонячні станції) між різними міськими вузлами робить населений пункт стійкішим до обстрілів та блекаутів.

Такі мегаполіси як Київ, Львів та Дніпро роками страждають від заторів через те, що бізнесактивність зосереджена в центрі, а житло – на околицях. Створення бізнесвузлів (наприклад, на базі занедбаних промзон) зменшить потребу в щоденних поїздках через усе місто.

Відновлення земельних ділянок або майданчиків із занедбаними чи старими промисловими, комерційними або сільськогосподарськими об’єктами, які раніше використовувалися і часто мають потребу в очищенні чи перепрофілюванні зон.

Українські міста мають величезні території колишніх радянських заводів, які часто розташовані близько до географічного центру (наприклад, Теличка або Промзона на Петрівці в Києві, Підзамче у Львові). Вони є ідеальними майданчиками для формування нових багатофункціональних вузлів (Smart Districts). Інтегровані міські зони можуть об’єднувати цифрові технології, сталу енергетику та IoT-інфраструктуру для покращення якості життя мешканців та оптимізації управління ресурсами (Додаток В). Вони діють як масштабовані моделі концепції «розумного міста» (Smart City), де новітні технологічні рішення тестуються на рівні окремого кварталу чи району перед впровадженням на рівні всього міста.

Децентралізація міських вузлів – це єдиний ефективний спосіб розвитку сучасних українських міст. Вона дозволяє вирішити проблеми з транспором, покращити екологію та, головне, створити безпечне і комфортне середовище для життя. Повоєнне відновлення дає Україні унікальний (хоч і вимушений) шанс

перестрибнути етап застарілого урбанізму та планово впровадити проєкт «Безпечне місто».

Перешкодою для реалізації поліцентричної міської структури є хаотичне здійснення забудови. Стратегічні керівники проєктів будівництва часто керуються миттєвим прибутком, будуючи величезні багатоповерхові житлові комплекси на сотні або тисячі квартир з надвисокою щільністю забудови без створення робочих місць чи належної соціальної інфраструктури в тому самому районі. Для зв'язку між міськими вузлами потрібен якісний швидкісний громадський транспорт (трамваї, міська електричка, метро), будівництво якого потребує великих капіталовкладень, яких бракує у місцевих бюджетах українських міст. Мешканці та підприємницькі структури міста часто за звичкою чинять супротив змінам і тяжіють до історичного центру міста як єдиного престижного місця для інвестицій та дозвілля.

Комплексна інтелектуально-аналітична система управління та безпеки, а також однойменна цільова програма може бути створена для забезпечення правопорядку, публічної безпеки та моніторингу ситуації в українських містах. Основними складовими та проявами проєкту «Безпечне місто» є інтелектуальне відеоспостереження, взаємодія через медіаресурси та спільноти. Система об'єднує тисячі камер по всьому місту. До неї інтегровано сучасні камери з функціями розпізнавання облич, автомобільних номерів та фіксації порушень ПДР. Це допомагає правоохоронцям оперативно розкривати злочини та відстежувати переміщення підозрілого транспорту. Комплекс використовується ситуаційним центром поліції українських міст для координації дій екстрених служб і моніторингу безпекової ситуації в реальному часі. Доцільним також є функціонування офіційних каналів комунікації, як YouTube-канал та Telegram-чат для оперативної взаємодії громадян з представниками органами влади, а також однойменні групи у Facebook, де публікуються кримінальні хроніки, новини правопорядку та судові вироки, які мають місце в кожному українському місті.

Безперервність державного та місцевого управління забезпечує функціонування інфраструктури, що є критично важливим для стійкості всієї держави. Наявність підземних ситуаційних центрів та альтернативних вузлів зв'язку дозволяє адміністрації міст координувати оборону навіть під час масованих обстрілів. Хмарні технології, цифровізація послуг, резервне копіювання даних та захищений документообіг гарантують те, що державні реєстри та критичні сервіси для громадян продовжують працювати.

Забезпечення базових потреб та збереження людського капіталу є головним ресурсом державної стійкості [205; 258]. Адміністрація українських міст покликана захистити життя містян та мінімізувати гуманітарну катастрофу.

Розгалужена мережа сучасних бомбосховищ та укриттів інтегрована в цивільну забудову (наприклад, станції метро, підземні паркінги), знижує рівень втрат серед цивільного населення. Знайти найближче укриття в українських містах можна за допомогою офіційних ресурсів та мобільних застосунків. Інтерактивні актуальні мапи захисних споруд можна переглянути на офіційному сайті обласних державних адміністрацій та оборонної сфери. Скористатися послугою «мапа укриттів» області для роботи офлайн дозволяє застосунок порталу «Дія». Можна завантажити мапу області, знайти найближчу адресу, переглянути стан та прокласти маршруту. Автономність систем життєзабезпечення та децентралізація енерго- та водопостачання (генератори, мобільні котельні, когенераційні установки) попереджає про влаштування блекауту і масової евакуації населення українських міст.

Таблиця 3.12

Ключові елементи безпекової інфраструктури, що формують стійкість українських міст

Елемент інфраструктури	Суть функції
Системи ППО та раннього виявлення	Фізичний захист неба над містом, виграш часу для переходу в укриття
Децентралізована енергетика	Унеможливлення повного відключення міста через ураження однієї ТЕЦ чи підстанції
Система «Безпечне місто»	Мережі розумних камер для контролю правопорядку, виявлення диверсійно-розвідувальної груп (ДРГ) та фіксації руйнувань
Резервна медицина катастроф	Автономні шпиталі із запасами крові, медикаментів та операційними в укриттях

Джерело: складено автором на основі проведених досліджень

Міська безпекова інфраструктура є фундаментом внутрішньої стійкості держави в умовах воєнного стану (табл. 3.12). Під час сучасних конфліктів міста стають головними цілями та водночас опорними пунктами оборони й життєзабезпечення всієї країни. Безпекова інфраструктура українських міст, крім захисних споруд, охоплює цифрові системи, енергетичні вузли, логістичні мережі та медичні заклади, які адаптовані до роботи під час критичних навантажень.

Стан міської інфраструктури безпосередньо впливає на ментальне здоров'я української нації та психологічна стійкість суспільства. Результати досліджень свідчать, випадки, коли громадяни переконані в чіткій роботі сирен, ППО, наявність обладнаних «Пунктів незламності» та швидке відновлення пошкоджень комунальниками, відчуття безпеки та рівень паніки знижується. Протидія дезінформації, захищені системи оповіщення та стабільний інтернет/радіозв'язок не дозволяють посіяти інформаційний вакуум та маніпулювати настроями населення країни.

Висновки до розділу 3.

У розділі 3 дисертаційного дослідження сформульовано концепцію стратегічного розвитку систем «Безпечне місто» на території України; запропоновано використання хмарних технологій в рамках підвищення рівня безпеки в містах України; визначено напрями підвищення ефективності процесу управління українськими населеними пунктами із застосуванням системи «Безпечне місто».

Розкрито напрями впровадження проєктів «Безпечне місто» (апробація світового досвіту в українських реаліях). Ключові елементи безпекової інфраструктури, що формують стійкість українських міст в умовах сучасних викликів, охоплюють комплекс інженерних, цифрових, організаційних та соціальних рішень. Вони спрямовані на захист населення, збереження критичних послуг та швидке відновлення після кризових ситуацій.

Здійснено порівняльний аналіз архітектури систем «Безпечне місто» та єдиної державної системи відеомоніторингу. Він демонструє перехід від локальних, фрагментованих рішень до централізованої загальнодержавної вертикалі. Архітектура проєкту «Безпечне місто» проєктувалася як сервісно-орієнтована модель для ЖКГ, регулювання міського трафіку, фіксації ДТП та локального правопорядку. Єдина державна система орієнтована суто на національну та публічну безпеку, розшук злочинців, протидію диверсіям та ведення оборонного контуру держави.

«Безпечне місто» діє як ізольована система. Державна система будується на регіональних комплексах, які є лише постачальниками даних для глобального аналітичного ядра МВС.

Обґрунтовано, що впровадження хмарних рішень для повоєнної відбудови українських міст за стандартами «розумного міста» (Smart City) є базовою умовою для створення гнучкої, безпечної та стійкої міської інфраструктури.

Використання хмарних технологій дозволяє відійти від застарілих локальних серверів, які є вразливими до фізичних руйнувань та кібератак.

Критично важливі дані (реєстри майна, геоінформаційні системи, демографічні дані) перенесено у захищені гібридні хмарні системи з автоматичним резервним копіюванням у безпечні дата-центри. Дані з міських відеокамер, датчиків та служб екстреної допомоги (101, 102, 103, 112) об'єднуються в єдину хмарну платформу аналітики в реальному часі для швидкого реагування на надзвичайні ситуації. Інтеграція розумних світлофорів, камер фіксації та датчиків руху в хмарну систему здійснюється для оптимізації транспортних потоків та зменшення заторів.

Запропоновано трирівневу інфраструктура масштабних національних рішень проєктів «Безпечне місто». Її основне завдання полягає у моніторингу ситуації на вулицях, дорогах та об'єктах критичної інфраструктури в режимі реального часу, автоматична первинна обробка даних та швидке інформування місцевих підрозділів поліції, ДСНС і комунальних служб.

Сформульовано критерії оцінки ефективності вітчизняних програмних рішень із зарубіжними аналогами. Вітчизняні рішення найчастіше виграють за критеріями економічної доцільності, адаптивності до локального законодавства та безпеки, тоді як глобальні зарубіжні аналоги мають перевагу в масштабності системи, передових технологічних стандартах та готовій експертизі.

Доведено, що інтелектуальні системи інтеграції відеоданих відіграють критичну роль у сучасній координації служб порятунку, забезпечуючи перехід від пасивного спостереження до проактивного реагування в режимі реального часу. Вони об'єднують потоки з тисяч камер (міських, автомобільних, камер на тілі, дронів) в єдине цифрове середовище для прийняття рішень.

Зазначено, що формування міської координаційної ради з питань проєкту «Безпечне місто» здійснюється шляхом прийняття відповідного рішення виконавчого комітету міської ради або розпорядження міського голови.

Цей орган створюється як консультативно-дорадчий для узгодження дій влади, правоохоронців, комунальних служб та громадськості у сфері розбудови інтелектуального відеоспостереження та безпекового простору.

Встановлено, що децентралізація міських вузлів – це стратегія сучасного містобудування, яка передбачає відмову від класичної моделі міста з одним домінуючим центром (моноцентризм) на користь створення мережі автономних, багатофункціональних районів (поліцентризм).

Запропоновано етапи розвитку джентрифікації в українських містах. Перетворення занепалих чи промислових районів на більш престижні та дорогі) зазвичай відбувається не за класичною західною схемою (де спочатку селяться митці та студенти), а через капіталістичну ініціативу забудовника та точкову реконструкцію.

Виділено, що традиційна моноцентрична та поліцентрична моделі міст представляють два принципово різні підходи до організації міського простору, економіки та логістики. Якщо перша фокусується навколо єдиного історичного чи ділового центру, то друга розподіляє міські функції між кількома рівнозначними вузлами. У сучасному урбанізмі більшість мегаполісів світу намагаються трансформуватися з моноцентричної моделі у поліцентричну, оскільки це єдиний спосіб забезпечити екологічну та транспортну стійкість міста в умовах перенаселення.

Доведено, що впровадження поліцентричної міської структури в населених пунктах України є одним із ключових завдань сучасного вітчизняного містобудування. Перехід від моноцентричної моделі (де всі адміністративні, культурні та бізнесові функції зосереджені в одному історичному центрі) до поліцентричної (де створюється кілька самодостатніх підцентрів) дозволяє знизити навантаження на транспортну систему, покращити екологію та забезпечити концепцію «15-хвилинного міста». Впровадження поліцентричності в Україні є безальтернативним шляхом розвитку для подолання інфраструктурної кризи великих міст, особливо в процесах повоєнного відновлення та модернізації постраждалих регіонів.

Обґрунтовано, що ключові елементи безпекової інфраструктури формують стійкість українських міст в умовах сучасних викликів, охоплюють комплекс інженерних, цифрових, організаційних та соціальних рішень. Вони спрямовані

на захист населення, збереження критичних послуг та швидке відновлення післякризових ситуацій.

Визначено, що розгалужені мережі камер відеоспостереження з функцією розпізнавання облич та автомобільних номерів, інтегровані з ситуаційними центрами Національної поліції. Функціонують автоматизовані системи раннього оповіщення про загрози (сирени, мобільні застосунки).

Захист критичних міських баз даних, хмарне резервне копіювання інформації здійснюються для запобігання втрат контролю над міською інфраструктурою. Регулярні тренінги з цивільного захисту, тактичної медицини та розгалужена мережа волонтерських організацій.

Визначено, що легітимність використання відкритих даних визначається правовими, етичними та технічними нормами, які забезпечують законність, безпеку та справедливість обробки інформації. Головний принцип полягає в тому, що дані мають бути не просто доступними, а їх використання не повинно порушувати права інших осіб чи державні інтереси.

Доведено, що розвиток безпекового простору в українських містах сьогодні базується на комплексній системі цивільного захисту, національної стійкості та концепції безбар'єрності й доступності середовища. Створення систем екстреного оповіщення з дублюванням інформації (звукові сигнали, текстові табло, жестова мова), забезпечення доступності цифрових платформ і додатків (наприклад, мапи укриттів) для людей з порушеннями зору чи слуху.

Проблеми та виклики реалізації системи проєкту «Безпечне місто» полягають у розподілі повноважень. Наявна часткова невизначеність зон відповідальності в межах проєкту «Безпечне місто» між представниками органів державної влади (МВС, Національно\поліція) та представниками органів місцевого самоврядування. З цим пов'язана необхідність остаточного затвердження та впровадження уніфікованих стандартів безпеки українських міст для оцінювання ефективності систем «Безпечне місто». Комплексний аналіз безпекового середовища в українських містах (зокрема, шляхом розробки єдиного Індексу безпеки українських міст, регіональних рейтингів Інституту

суспільно-економічних досліджень) пропонується базувати на поєднанні об’єктивних статистичних даних (від МВС, ДСНС, Національної поліції) та суб’єктивного сприйняття безпеки громадянами (що можна оцінити за допомогою результатів опитування жителів).

Виокремлено вимірювальні блоки єдиного Індексу безпеки українських міст, що базуються на адаптації провідних світових методологій оцінки міського середовища до специфіки воєнного та поствоєнного стану в Україні.

Обгрунтовано, що впровадження хмарних рішень для повоєнної відбудови Києва за стандартами «розумного міста» (Smart City) є ключовим інструментом для створення гнучкої, безпечної та сучасної міської інфраструктури.

Використання хмарних технологій дозволяє відійти від застарілих локальних серверів на користь централізованих, масштабованих та захищених систем. Резервне копіювання всіх критичних даних життєзабезпечення міста у розподілені хмарні платформи (зокрема за межами України) для захисту від фізичних та кібератак. Хмарні системи аналізують дані з камер спостереження та навігаторів для динамічного регулювання світлофорів, зменшення заторів та пріоритезації громадського транспорту. Перенесення аналітики відеопотоків на хмарні платформи для використання алгоритмів штучного інтелекту дозволяє автоматично розпізнавати обличчя, автомобільні номери, виявляти залишені предмети або фіксувати Д

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення і наведено нове вирішення важливої наукової проблеми, що полягає у розробленні та науковому обґрунтуванні теоретичних і науково-методичних підходів до обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні.

Отримані результати дослідження дозволили сформулювати такі висновки:

1. У результаті ґрунтовного аналізу сутності понять і концепцій, що проводився в межах дослідження, було узагальнено підходи щодо змістовного наповнення категорії проєкту «Безпечне місто». Визначення концепції «Безпечне місто» еволюціонувало від класичного захисту від злочинності до комплексних систем. Воно об’єднує технології, інфраструктуру та суспільну взаємодію задля безпеки громадян українських міст. Проаналізовано взаємозалежність техноцентричного та охоронного. соціально-урбаністичного, багатовимірного, правового та просторово-гендерного підходів до визначення категорії проєкту «Безпечне місто». Їх об’єднують технології, міська інфраструктура та суспільна взаємодія задля безпеки громадян українських міст.

2. Доведено, що проєкти «Безпечне місто» є базовим елементом концепції «розумне місто» (Smart City), спрямованим на створення комфортного та захищеного середовища для мешканців українських міст. Ця концепція об’єднує сучасні технології для моніторингу, оперативного реагування та запобігання надзвичайним ситуаціям. Проєкти «Безпечне місто» передбачають створення єдиного інформаційного простору для цілодобового моніторингу, оперативного реагування на надзвичайні ситуації, розшуку злочинців та управління міською інфраструктурою. Обґрунтовано доцільність доповнення класифікації проєктів «Безпечне місто» ознаками виміру безпеки, типу профілактики та режиму функціонування, а також сформовано методичні вимоги до їх запровадження за етапами – від діагностики та обґрунтування мети до щорічного оцінювання результативності.

3. Обґрунтовано, що для реалізації проєктів «Безпечне місто» в Україні

доцільно вивчити західну та східну (азійську) моделі. В рамках західної моделі (досвід ЄС та США) фокусуються на балансі безпеки та захисту приватного життя, використанні європейського/американського обладнання та залученні громадськості через прозорі муніципальні платформи. Азійська/східна модель (досвід Сінгапуру, Китаю) характеризується тотальною цифровізацією, штучним інтелектом, прогнозна аналітика та глибока інтеграція біометричних даних.

Європейський досвід реалізації проєктів «Безпечне місто» еволюціонував від простого встановлення камер спостереження до комплексних екосистем міської безпеки. Вони опираються не лише на технічні інновації, а й на інклюзивність, довіру мешканців та суворе дотримання прав людини. Ключові принципи та підходи до реалізації проєктів «Безпечне місто» в ЄС охоплює концепцію «Безпека через проєктування», яка передбачає досягнення балансування технологій та приватності даних при залученні мешканців міст.

Досліджено, що проблеми впровадження європейської моделі світового досвіду запровадження проєктів «Безпечне місто» в Україні полягають у залежності від окремих масових закордонних виробників апаратного забезпечення, недостатньому обсязі фінансування на рівні окремих міст в умовах воєнного стану, ризики порушення прав громадян на приватність через недосконаліть законодавчого поля щодо регулювання біометричних даних.

Східна (азійська) модель проєкту «Безпечне місто» базується на жорсткій державній координації, масовому впровадженні штучного інтелекту, систем розпізнавання облич, Інтернету речей (IoT) та об’єднанні всіх комунальних і правоохоронних служб у єдині централізовані ситуаційні центри реагування в реальному часі. Ключовою рисою східної (азійської) моделі є домінування централізованого державного управління та єдиних вертикальних протоколів замість ініціатив представників місцевих органів влади. Активне застосування дронів-безпілотників із панорамними камерами для ліквідації простору навколо автомобілів, які водій не може бачити через вікна чи джерела з огляду (стандартні дзеркала заднього виду) та моніторингу масових скупчень людей з повітря. Прямі канали зв’язку забезпечують миттєву передачу зашифрованого

відеопотоку на планшети патрульних поліцейських ще до їх прибуття на місце події.

Головні переваги східної моделі запровадження проєктів «Безпечне місто» полягають у миттєвому реагуванні на надзвичайні ситуації та правопорушення завдяки прогнозній аналітиці, високий рівень розкриття злочинів та профілактика правопорушень, а також повна синхронізація роботи поліції, екстрених служб і комунальної інфраструктури.

Встановлено, що європейська модель має трирівневе правове забезпечення – Загальний регламент про захист даних, Директиву (ЄС) 2016/680 щодо обробки даних поліцією та Регламент (ЄС) 2024/1689 про штучний інтелект, який з 2 лютого 2025 р. заборонив віддалену біометричну ідентифікацію «в реальному часі» в публічних місцях для правоохоронних цілей, крім вичерпно визначених випадків, – а практика Європейського суду з прав людини та національних судів формує управлінські вимоги до проєктування систем: законне визначення того, хто, де, з якою метою і як довго може застосовувати біометричні та аналітичні функції, попередня оцінка впливу, нормативні строки зберігання, журналювання доступу та незалежний аудит. Доказові дані засвідчують помірний і залежний від контексту ефект відеоспостереження, а досвід експорту східної моделі та обмежень закупівель обладнання окремих виробників у США – що вибір моделі й постачальника є питанням кібербезпеки та безпеки ланцюгів постачання. Для України, законодавство якої не передбачає обов’язкової оцінки впливу на захист даних і спеціальних правил для біометричної ідентифікації, адаптація світового досвіду полягає насамперед у перенесенні цих правових і управлінських гарантій, а не технічної архітектури тієї чи іншої моделі.

4. Визначено, що проведення комплексного аналізу ефективності міської програми «Безпечне місто» дозволяє оцінити раціональність використання бюджетних коштів, рівень зниження злочинності та реальне підвищення безпеки мешканців. Оцінити ефективність міської програми «Безпечне місто» можна через порівняння витрачених коштів із реальними результатами: кількістю розкритих злочинів за допомогою камер, зменшенням рівня злочинності на

вулицях, станом дорожнього руху та відгуками жителів українських міст.

Найвищу ефективність демонструють програми, інтегровані в довгострокові Стратегії розвитку міст, а не розроблені як відокремлені документи. Поширеним недоліком у багатьох українських містах залишається відсутність вимірюваних індикаторів ефективності, через що моніторинг часто зводиться до оцінки простого освоєння бюджетних коштів, а не реальних якісних змін для мешканців міст. Аналіз регіональних програм показує, що значна частина фінансування спрямовується на інфраструктурні об'єкти. Водночас інвестиції у відновлення людського капіталу часто ігноруються або фінансуються за залишковим принципом, проходячи етап публічного обговорення із залученням інститутів громадянського суспільства, що мають значно вищий рівень довіри та реальної результативності.

5. Проаналізовано, що методичні основи системи «Безпечне місто» необхідні для створення єдиного, захищеного та стандартизованого середовища. Вони запобігають хаотичному встановленню камер, забезпечують сумісність технологій та ефективне управління безпекою будь-якого українського міста.

Запровадження апаратно-програмного комплексу «Безпечне місто» базується на принципах системності, комплексності, законності та централізованому управлінні, об'єднуючи відеоспостереження, аналітику трафіку та координацію екстрених служб задля безпеки будь-якого українського міста.

6. Висвітлено, що людиноцентричність і партисипативність перетворюють систему «Безпечне місто» з технічного нагляду на функціонуючий простір спільної безпеки. Людиноцентричність у концепції «Безпечне місто» орієнтована на захист прав, доступність та якість життя громадян українських міст. Партисипативність як залучення громадян до управління міста охоплює такі напрями, як участь жителів міст у обговоренні розташування камер чи освітлення, локальні ініціативи для покращення безпеки районів міст, використання цифрових сервісів та додатків для швидкого реагування на проблеми та взаємодію з комунальними службами.

7. Виявлено, що соціально-орієнтований підхід до реалізації проєктів «Безпечне місто» передбачає формування системи випереджувальних заходів, спрямованих на запобігання правопорушенням до того, як вони настануть. Він ґрунтується на використанні штучного інтелекту та відеоаналітики для прогнозування ризиків, автоматизоване оповіщення профільних служб до настання критичної ситуації. Інтеграція соціальних сервісів, муніципальних варт та медичної допомоги у спільну цифрову систему з метою раннього виявлення загроз життю та здоров'ю вразливих верств населення в реальному часі.

Трансформація ролі проєкта «Безпечне місто» в соціальній політиці характеризується перехідом від реакції до попередження. Основні напрями державної та місцевої соціальної політики спрямованості полягають у допомозі вразливим категоріям. Забезпечується підтримка літніх людей та маломобільних громадян через інтеграцію соціальних служб і міських систем спостереження. Здійснюється гарантування безпеки та захист прав дітей та неповнолітніх у навчальних закладах та громадських місцях. Інклюзивний моніторинг передбачає інтеграцію камер із аналітикою для допомоги людям із порушеннями зору чи слуху.

Обґрунтовано, що теоретичним підґрунтям соціально орієнтованого підходу є концепція людської безпеки та концепція запобігання злочинності засобами середовищного проєктування, закріплена в стандарті ISO 22341:2021, у межах яких відеоспостереження доповнюється плануванням простору, освітленням і соціальними послугами, а результативність вимірюється, зокрема, індикатором 11.7.2 Цілей сталого розвитку. Встановлено, що правову основу інтеграції «Безпечного міста» із соціальною політикою становлять законодавство про запобігання домашньому насильству та соціальні послуги, Стамбульська конвенція й Конвенція про права осіб з інвалідністю, а практичними механізмами – маршрути перенаправлення через систему 112, мережа центрів життєстійкості, інститут фахівців із супроводу ветеранів і Служба освітньої безпеки. Доведено, що соціальна орієнтація потребує запобіжників для вразливих груп: мінімізації даних під час поєднання

безпекових і соціальних систем, оцінки впливу на рівність до запровадження аналітичних функцій з огляду на вищу частоту хибних збігів алгоритмів розпізнавання облич щодо жінок, людей похилого віку та дітей, а також збереження нецифрових каналів звернення за допомогою.

8. Охарактеризовано суттєвий диспропорційний розрив між великими містами-лідерами (які впроваджують інтелектуальне відеоспостереження із застосуванням штучного інтелекту) та невеликими громадами, де фінансування покриває лише базові камери без аналітики. Здійснюється слабкий рівень інтеграції, координації та оперативного обміну даними між муніципальними інфраструктурами, Національною поліцією, ДСНС та іншими силовими відомствами. Крім того, бюджетна нерівність фінансових можливостей великих та малих міст України відображається на рівні реалізації проєктів «Безпечне місто».

Попри наявність ефективно реалізованих проєктів багатьох українських міст (Тернополя, Києва, Рівного), в управлінні населеними пунктами при реалізації проєктів «Безпечне місто» часто виникають проблеми правової неврегульованості та обмеженості фінансування. Муніципальні системи працюють за локальними програмами, оскільки єдині загальнодержавні стандарти для систем відеоконтролю та захисту персональних даних із залученням штучного інтелекту потребують доопрацювання.

Встановлено, що реформа децентралізації створила інституційне підґрунтя для муніципальних проєктів, але зумовила значні відмінності в адміністративній, кадровій і фінансовій спроможності громад, поглиблені війною, а законопроєкт «Про єдину систему відеомоніторингу стану публічної безпеки» (реєстр. № 11031 від 20.02.2024) чітко не визначає кола осіб, які матимуть доступ до інформації. Запропоновано конкретизувати три рівні управління (початковий, аналітичний, інтегрований) через мінімальні правові, кадрові, технічні та кібербезпекові вимоги до кожного з них, а для громад із низькою спроможністю – мінімальний безпековий пакет, що поєднує поліцейського офіцера й офіцера-рятувальника громади, центр безпеки, базове відеоспостереження в ключових

точках, доступні укриття та оповіщення. Обґрунтовано, що державний рівень запровадження проєктів «Безпечне місто» має забезпечити законодавче визначення користувачів, цілей обробки, строків зберігання, порядку застосування біометричних функцій і незалежного нагляду, а також єдині вимоги до рівнів управління, кадрові нормативи, механізм співфінансування, включення безпекової інфраструктури до проєктів відбудови та державний моніторинг на основі показників стандартів ISO 37122 і ISO 37123 та Індексу цифрової трансформації, доповненого безпековою складовою.

9. Обґрунтовано, що впровадження хмарних рішень для повоєнної відбудови українських міст за стандартами «розумного міста» (Smart City) є базовою умовою для створення гнучкої, безпечної та стійкої міської інфраструктури. Використання хмарних технологій дозволяє відійти від застарілих локальних серверів, які є вразливими до фізичних руйнувань та кібератак.

Критично важливі дані (реєстри майна, геоінформаційні системи, демографічні дані) перенесено у захищені гібридні хмарні сховища з автоматичним резервним копіюванням у безпечні дата-центри. Дані з міських відеокамер, датчиків та служб екстреної допомоги (101, 102, 103, 112) об’єднуються в єдину хмарну платформу аналітики в реальному часі для швидкого реагування на надзвичайні ситуації. Інтеграція розумних світлофорів, камер фіксації та датчиків руху в хмарну систему здійснюється для оптимізації транспортних потоків та зменшення заторів.

10. Виділено, що традиційна моноцентрична та поліцентрична моделі міст представляють два принципово різні підходи до організації міського простору, економіки та логістики. Якщо перша фокусується навколо єдиного історичного чи ділового центру, то друга розподіляє міські функції між кількома рівнозначними вузлами. У сучасному урбанізмі більшість мегаполісів світу намагаються трансформуватися з моноцентричної моделі у поліцентричну, оскільки це єдиний спосіб забезпечити екологічну та транспортну стійкість міста в умовах перенаселення.

Впровадження поліцентричної міської структури в містах України є одним із ключових завдань сучасного вітчизняного містобудування. Перехід від моноцентричної моделі (де всі адміністративні, культурні та бізнесові функції зосереджені в одному історичному центрі) до поліцентричної (де створюється кілька самодостатніх підцентрів) дозволяє знизити навантаження на транспортну систему, покращити екологію та забезпечити концепцію «15-хвилинного міста». Впровадження поліцентричності в Україні є безальтернативним шляхом розвитку для подолання інфраструктурної кризи великих міст, особливо в процесах повоєнного відновлення та модернізації постраждалих регіонів.

11. Зазначено, що формування міської координаційної ради з питань проєкту «Безпечне місто» здійснюється шляхом прийняття відповідного рішення виконавчого комітету міської ради або розпорядження міського голови. Цей орган створюється як консультативно-дорадчий для узгодження дій влади, правоохоронців, комунальних служб та громадськості у сфері розбудови інтелектуального відеоспостереження та безпекового простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

2. Господарський кодекс України // Відомості Верховної Ради України (ВВР). 2003. №18. № 19-20. № 21-22, ст. 144. URL: https://zakon.rada.gov.ua/laws/show/436-15. Втратив чинність 28.08.2025 на підставі Закону України від 09.01.2025 № 4196-IX; наведено в редакції, чинній на час виконання дослідження.

3. Кодекс України про адміністративні правопорушення: Закон України від 07 груд. 1984 р. № 8073-X: станом на 2026 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10

4. Кодекс адміністративного судочинства України: Закон України від 06 лип. 2005 р. № 2747-IV : станом на 1 січ. 2024 р. *Відомості Верховної Ради України*. 2005. № 35/36, № 37. Ст. 446. URL: https://zakon.rada.gov.ua/laws/show/2747-15.

5. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III: [за станом на 2026 р.]. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

6. Цивільний кодекс України: Закон України від 16 січ. 2003 р. № 435-IV: станом на 2026 р. // *Відомості Верховної Ради України*. – 2003. – № 40–44. – Ст. 356. – URL: https://zakon.rada.gov.ua/laws/show/435-15

7. Цивільний процесуальний кодекс України: Закон України від 18 бер. 2004 р. № 1618-IV: станом на 2 трав. 2026 р. URL: https://zakon.rada.gov.ua/go/1618-15.

8. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.2006 № 3477-IV. URL: https://zakon.rada.gov.ua/laws/show/3477-15.

9. Про державне прогнозування та розроблення програм економічного і соціального розвитку України. Закон України від 23.03.2000 № 1602-III. URL: https://zakon.rada.gov.ua/laws/show/1602-14#Text.

10. Про державно-приватне партнерство. Закон України від 01.07.2010 № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text.

11. «Про державну підтримку інвестиційних проектів із значними інвестиціями в Україні». Закон України від 17.12.2020 № 1116-IX. URL: https://zakon.rada.gov.ua/laws/show/1116-20#Text.

12. «Про державну службу»: Закон України від 10 грудня 2015 року № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19.

13. «Про Державну службу спеціального зв'язку та захисту інформації України»: Закон України від 23 лютого 2006 року № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15.

14. Про дорожній рух: Закон України від 30.06.1993 № 3353-XII. URL: https://zakon.rada.gov.ua/laws/show/3353-12.

15. Про запобігання та протидію домашньому насильству: Закон України від 07.12.2017 № 2229-VIII. URL: https://zakon.rada.gov.ua/laws/show/2229-19.

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

17. «Про звернення громадян»: Закон України від 02.10.1996 р. URL: https://zakon2.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80.

18. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

19. «Про місцеве самоврядування»: Закон України від 21 травня 1997 року (№ 280/97-ВР). [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр.

20. «Про національну безпеку України»: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

21. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

22. «Про Національну програму інформатизації»: Закон України від 01.12.2022 р. № 2807-IX. База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2807-20.

23. «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 р. № 2163-VIII (зі змінами та доповненнями). База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

24. «Про правовий режим воєнного стану»: Закон України від 12.05.2015 No 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

25. Про ратифікацію Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами: Закон України від 20.06.2022 № 2319-IX. URL: https://zakon.rada.gov.ua/laws/show/2319-20.

26. Про систему екстреної допомоги населенню за єдиним телефонним номером 112: Закон України від 13.03.2012 № 4499-VI. URL: https://zakon.rada.gov.ua/laws/show/4499-17.

27. Про соціальні послуги: Закон України від 17.01.2019 № 2671-VIII. URL: https://zakon.rada.gov.ua/laws/show/2671-19.

28. Про стандартизацію: Закон України від 05.06.2014 № 1315-VII. URL: https://zakon.rada.gov.ua/laws/show/1315-18.

29. Про статус ветеранів війни, гарантії їх соціального захисту: Закон України від 22.10.1993 № 3551-XII. URL: https://zakon.rada.gov.ua/laws/show/3551-12.

30. «Про хмарні послуги»: Закон України від 17.02.2022 р. № 2075-IX. *Відомості Верховної Ради України*. 2022. № 22. Ст. 149. URL: https://zakon.rada.gov.ua/go/2075-20.

31. Про Цілі сталого розвитку України на період до 2030 року. Указ Президента України від 30.09.2019 р. № 722/2019. URL: https://zakon.rada.gov.ua/laws/show/722/2019#Text.

32. Про рішення Ради національної безпеки і оборони України «Про створення та забезпечення діяльності Головного ситуаційного центру України» : Указ Президента України від 28.02.2015 № 115/2015. URL: https://zakon.rada.gov.ua/laws/show/115/2015.

33. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року. Указ Президента України від 18.06.2021 № 260/2021. URL: https://www.president.gov.ua/documents/2602021-39225.

34. Про затвердження Державної стратегії регіонального розвитку на 2021- 2027 роки. Постанова Кабінету Міністрів України; Стратегія від 05.08.2020 № 695. URL: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text.

35. «Про затвердження плану заходів на 2025-2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року». Розпорядження Кабінету Міністрів України від 25 березня 2025 р. № 374-р. URL: https://zakon.rada.gov.ua/laws/show/374-2025-%D1%80.

36. Про питання реформування органів внутрішніх справ України: розпорядження Кабінету Міністрів України від 22 жовтня 2014 р. № 1118-р. URL: https://archive.khpg.org/policereform/library/rozporyadzhennya-kmu-v-d-22.10.2014-1118-r-schodo-pitannya-reform.

37. «Про схвалення Концепції Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року». Розпорядження Кабінету Міністрів України від 6лютого 2013 р. No51-р. URL: https://zakon.rada.gov.ua/laws/show/51- 2013 -%D1%-80#Text.

38. «Про схвалення Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року». Розпорядження Кабінету Міністрів України від 14 квітня 2021 р. № 366-р – URL: https://zakon.rada.gov.ua/laws/show/366-2021-%D1%80.

39. Про схвалення Концепції розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

40. Про затвердження Державної цільової програми з медичної, фізичної реабілітації та психосоціальної реадаптації постраждалих учасників Революції Гідності, учасників антитерористичної операції та осіб, які брали участь у здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації в Донецькій та Луганській областях, забезпеченні їх здійснення, на період до 2023 року: Постанова Кабінету Міністрів України від 5 грудня 2018 р. №1021 URL: http://ips.ligazakon.net/document/kp18102.

41. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки. Розпорядження Кабінету Міністрів України; План, Заходи від 12.05.2021 № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text.

42. Положення про Єдину інформаційну систему соціальної сфери: затв. постановою Кабінету Міністрів України від 14.04.2021 № 404 (в редакції постанови Кабінету Міністрів України від 27.10.2023 № 1130). URL: https://zakon.rada.gov.ua/laws/show/404-2021-%D0%BF.

43. Порядок реалізації експериментального проєкту із запровадження комплексної соціальної послуги з формування життєстійкості: затв. постановою Кабінету Міністрів України від 03.10.2023 № 1049. URL: https://zakon.rada.gov.ua/laws/show/1049-2023-%D0%BF.

44. Порядок організації діяльності та забезпечення функціонування центрів життєстійкості: затв. постановою Кабінету Міністрів України від 23.01.2024 № 83. URL: https://zakon.rada.gov.ua/laws/show/83-2024-%D0%BF.

45. Порядок забезпечення діяльності фахівців із супроводу ветеранів війни та демобілізованих осіб: затв. постановою Кабінету Міністрів України від 02.08.2024 № 881. URL: https://zakon.rada.gov.ua/laws/show/881-2024-%D0%BF.

46. Про схвалення Стратегії ветеранської політики на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2024–2027 роках : розпорядження Кабінету Міністрів України від 29.11.2024 № 1209-р. URL: https://zakon.rada.gov.ua/laws/show/1209-2024-%D1%80.

47. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: затв. наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 № 601 (зі змінами, затвердженими наказами від 12.10.2021 № 616 та від 10.07.2022 № 343). URL: https://cip.gov.ua/services/cm/api/attachment/download?id=48543.

48. Аналіз регуляторного впливу до проєкту наказу Міністерства цифрової трансформації України «Про затвердження галузевих профілів безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури». Міністерство цифрової трансформації України. URL:https://storage.thedigital.gov.ua/files/1/11/8fe88e2bce5317e72b3c5839271b4112.pdf.

49. Конвенція про захист прав людини і основоположних свобод : міжнародний договір від 04.11.1950; ратифіковано Законом України від 17.07.1997 № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004.

50. Нота Постійного представництва України при Раді Європи від 28.02.2022 № 31011/32-017-3 щодо статті 15 Конвенції про захист прав людини і основоположних свобод (відступ від зобов'язань у зв'язку із запровадженням воєнного стану). Strasbourg: Council of Europe, 2022. URL: https://rm.coe.int/1680a5b0b0.

51. Конвенція про права осіб з інвалідністю: міжнародний документ від 13.12.2006; ратифіковано Законом України від 16.12.2009 № 1767-VI. URL: https://zakon.rada.gov.ua/laws/show/995_g71.

52. Рішення Конституційного Суду України від 20.01.2012 № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської

області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12.

53. Постанова Касаційного кримінального суду у складі Верховного Суду від 08.05.2025 у справі № 207/722/23 (провадження № 51-2686км24). URL: https://reyestr.court.gov.ua/Review/127297857.

54. Справа «Пек проти Сполученого Королівства» (Peck v. the United Kingdom): рішення Європейського суду з прав людини від 28.01.2003, заява №44647/98. URL: https://hudoc.echr.coe.int/eng?i=001-60898.

55. Справа «С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom): рішення Великої палати Європейського суду з прав людини від 04.12.2008, заяви № 30562/04, 30566/04. URL: https://hudoc.echr.coe.int/eng?i=001-90051.

56. Справа «Catt v. the United Kingdom» : рішення Європейського суду з прав людини від 24.01.2019, заява № 43514/15. URL: https://hudoc.echr.coe.int/eng?i=001-189424.

57. Справа «Gaughran v. the United Kingdom»: рішення Європейського суду з прав людини від 13.02.2020, заява № 45245/15. URL: https://hudoc.echr.coe.int/eng?i=001-200817.

58. Справа «Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom): рішення Великої палати Європейського суду з прав людини від 25.05.2021, заяви № 58170/13, 62322/14, 24960/15. URL: https://hudoc.echr.coe.int/eng?i=001-210077.

59. Справа «Глухін проти Росії» (Glukhin v. Russia): рішення Європейського суду з прав людини від 04.07.2023, заява № 11519/20. URL: https://hudoc.echr.coe.int/eng?i=001-225655.

60. František Ryneš v Úřad pro ochranu osobních údajů: judgment of the Court of Justice of the European Union (Fourth Chamber) of 11.12.2014, Case C-212/13.ECLI:EU:C:2014:2428.URL:https://curia.europa.eu/juris/documents.jsf?num=C-212/13.

61. R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058: judgment of the Court of Appeal (Civil Division) of 11.08.2020. URL: https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/.

62. R (Thompson and Carlo) v Commissioner of Police of the Metropolis [2026] EWHC 915 (Admin): approved judgment of the High Court of Justice (Administrative Court) of 21.04.2026. URL: https://www.judiciary.uk/wp-content/uploads/2026/04/AC-2024-LON-001764-R-Thompson-and-Carlo-version-for-hand-down-21-04-2026.pdf.

63. The King (Shaun Thompson and Silkie Carlo) v The Commissioner of Police of the Metropolis [2026] EWHC 915 (Admin): press summary. High Court of Justice, 21.04.2026. URL: https://www.judiciary.uk/wp-content/uploads/2026/04/Summary-of-judgment-Thomson-and-Carlo-v-Metropolitan-Police-Commmissioner-AC-2024-LON-001764-21-04-2026.pdf.

64. Ухвала Першого сенату Федерального конституційного суду Німеччини від 18.12.2018 № 1 BvR 142/15 (автоматизований контроль номерних знаків). BVerfGE 150, 244. ECLI:DE:BVerfG:2018:rs20181218.1bvr014215. URL: https://www.servat.unibe.ch/Dfr/bv150244.html.

65. Рішення Першого сенату Федерального конституційного суду Німеччини від 16.02.2023 № 1 BvR 1547/19, 1 BvR 2634/20 (автоматизований аналіз даних): Press Release No. 18/2023 of 16 February 2023. URL: https://bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html.

66. Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021) (en banc): opinion of 24.06.2021, No. 20-1495. URL: https://www.aclu-md.org/app/uploads/2021/06/lbs_v_bpd_-_4th_cir_opinion_-_210624.pdf.

67. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник

Європейського Союзу. 2016. L 119. С. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

68. Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи переслідування кримінальних правопорушень або виконання кримінальних покарань, про вільний рух таких даних та про скасування Рамкового рішення Ради 2008/977/ПВД. Official Journal of the European Union. 2016. L 119. P. 89–131. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj.

69. Регламент (ЄС) 2024/1689 Європейського Парламенту і Ради від 13 червня 2024 року про встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект). Official Journal of the European Union. 2024. L series. 12.07.2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

70. Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020 / European Data Protection Board. Brussels, 2020.URL:https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.

71. John S. McCain National Defense Authorization Act for Fiscal Year 2019: Public Law 115-232 of 13.08.2018. Sec. 889. URL: https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

72. Андрієнко А.О. Упровадження концепції «Smart City» в управління великими містами України : монографія / Андрієнко А.О. Вінниця, Україна : ГО «Європейська наукова платформа», 2023. 196 с. URL: https://palsg.nmu.org.ua/ua/Sci/Monograph/Андрієнко-Е-монографія-2023.pdf.

73. Багаденко І.П., Оцел В.В. Забезпечення безпеки громадян у великих містах: досвід зарубіжних країн. URL: http://elar.naiau.kiev.ua/jspui/handle/1/13906.

74. Баглай С. Камери і муніципальні варти. Наскільки безпечне «безпечне місто»? Українська правда. 20.05.2021. URL: https://www.pravda.com.ua/columns/2021/05/20/7294137/.

75. Бараннік В.В., Комолов Д.І., Корольова Н.А. Доцільність реалізації програми «Безпечне місто» на території України. URL: https://openarchive.nure.ua/items/245cfcdf4aab17.

76. Барсукова О. МОН: Офіцери Служби освітньої безпеки вже працюють у понад 1,6 тисячі шкіл. Українська правда. Життя. 02.06.2025. URL: https://life.pravda.com.ua/society/u-mon-nazvali-kilkist-shkil-de-z-yavilis-oficeri-bezpeki-308436/.

77. Барсукова О. Скільки українців потерпали від домашнього насильства за перші 5 місяців 2025 року? Дані поліції. Українська правда. Життя. 03.07.2025. URL: https://life.pravda.com.ua/society/policiya-nazvala-kilkist-zayav-pro-domashnye-nasylstvo-za-5-rokiv-30901.

78. Бондаренко С.М., Бугас Н.В. Соціальна політика держави як основа забезпечення соціального розвитку. Державне управління: удосконалення та розвиток. 2021. №2. URL: http://www.dy.nayka.com.ua/pdf/2_2021/42.pdf.

79. Вольська О.М. Модель демократичного врядування в системі соціального розвитку міста. *Наукові перспективи*. № 1(55). 2025. С.113-121. DOI: https://doi.org/10.52058/2708-7530-2025-1(55)-113-121

80. Гарасимчук О.І., Оліярник Ю.С., Нестор А.О., Наконечний Т.І. Психологічні методи шахрайства в кіберпросторі та способи їм протидіяти. Кібербезпека: освіта, наука, техніка. 2025. № 2(30). С. 511–529. DOI: https://doi.org/10.28925/2663-4023.2025.30.990.

81. Дабіжа В.В. Розвиток соціальної політики держави в проєктах «Безпечне місто». *Актуальні проблеми інноваційної економіки та права*. 2026. №3. С. 68-72. DOI: 2026-3-11https://doi.org/10.36887/2524-0455-

82. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорон*а. 2023. № 2(60). С. 78–85. URL: https://elar.navs.edu.ua/handle/123456789/39889.

83. Досенко А.К. Хмарні технології: прикладні технології сучасних платформ. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Філологія.*

Журналістика. 2022. Т. 33 (72), № 1. С. 248–253. – URL: https://elibrary.kubg.edu.ua/42792/.

84. Дрок І.С. Система «Безпечне місто» як інструмент контролю за дотриманням законодавства на транспорті. *Науковий вісник Ужгородського Національного Університету. Серія Право*. Випуск 88: частина 2, 2025. С. 371-375. DOI: https://doi.org/10.24144/2307-3322.2025.88.2.50

85. Зінченко О. «Безпечне місто» як фактор оперативного реагування на надзвичайні ситуації // Державне управління та державна служба. URL: https://gocsri.com/index.php/GCPS/article/view/Zinchenko.

86. Кадлубович Т.І., Дабіжа В.В. Проєкт «Безпечне місто» як інструмент інтеграції інновацій у соціальну політику // *Економіка харчової промисловості*. 2026. Т.18, вип. 2. С. 66-72. DOI: https://doi.org/10.15673/fie.v18i2.3577.

87. Кириченко А. Мінцифри оцінило рівень цифровізації регіонів та громад: результати. *Економічна правда*. 13.05.2025. URL: https://epravda.com.ua/tehnologiji/mincifri-ocinilo-riven-cifrovizaciji-regioniv-ta-gromad-rezultati-806628/

88. Костенко О., Грущинська Н. Формування та реалізація кадрової політики в органах публічної влади: вітчизняний та зарубіжний досвід. *Економічний простір*. 2020. № 158. С. 77-82. https://doi.org/10.32782/2224-6282/158-13

89. Ломоносова Н. Соціальний захист у повоєнній Україні: час змінювати підходи. URL: https://cedos.org.ua/soczialnyj-zahystu-povoyennij-ukrayini-chaszminyuvaty-pidhody.

90. Матвеєва О. Мунько А. Упровадження концепції розумного міста у процеси цифрової трансформації України заради сталого розвитку. *Науковий вісник: Державне управління*, № 1(13), 2023. С.138-162 DOI: https://doi.org/10.32689/2618-0065-2023-1(13)-138-162.

91. Мозоль Н.І. Роль соціальної справедливості у забезпеченні соціальноекономічних прав людини і громадянина в українській державі: дис...

канд. юр. наук: 12.00.12; Київський Національний університет внутрішніх справ. Київ, 2009. 239 с. URL: https://nrat.ukrintei.ua/searchdoc/0410U000353.

92. Моторнюк У.І. Соціальна політика як необхідна умова функціонування соціальної держави. *Економіка та держава*. 2016. № 12. URL: http://www.economy.in.ua/pdf/12_2016/7.pdf.

93. Негребецький В. В. Впровадження інтелектуальних систем відеомоніторингу в правоохоронну діяльність України: досвід високотехнологічних країн. URL: https://doi.org/10.30525/978-9934-26-649-2-22.

94. Некряч А.І. Система «Безпечне місто» – складова механізму національної безпеки. *Вісник Хмельницького національного університету. Серія: Економічні науки.* 2026. № 4. С. 196–201. DOI: https://doi.org/10.31891/2307-5740-2026-356-27.

95. Некряч А.І. Цифрова платформа «Безпечне місто» як основа досягнення цілей сталого розвитку місцевих громад. Development of Service Industry Management. 2026. № 3. С. 292–297. DOI: https://doi.org/10.31891/dsim-2026-15(36).

96. Охріменко А. В. Інструменти публічного управління: інноваційний підхід. *Актуальні проблеми інноваційної економіки та права*, № 2, 2025. С. 11-14. DOI: https://doi.org/10.36887/2524-0455-2025-2-2.

97. Пацурія Н.Б. Впровадження технологій штучного інтелекту у забезпечення національної безпеки та обороноздатності України: проблеми та перспективи повоєнного періоду. Координата, 2023. URL: https://webcache.googleusercontent.com/searchd.

98. Пустовіт О.Б. Відеоспостереження як елемент безпеки міста у проектах «Безпечне місто». Міжнародна науково-практична конференція «Перспективи та інновації сучасної науки: теорія, практика та глобальні виклики» (м. Ізмаїл, 17 квітня 2026 р.)

99. Пустовіт О.Б. Обґрунтування необхідності впровадження систем «Безпечне місто» в умовах воєнних загроз в Україні. XIX Міжнародна науково-

практична конференція «Умови економічного зростання в країнах з ринковою економікою». (м. Переяслав, 23-24 квітня 2026 р.)

100. Пустовіт О.Б. Передумови та цілі впровадження проєктів «Безпечне місто» на державному рівні. *Актуальні проблеми інноваційної економіки та права*. 2026. №3. С. 187-191. DOI: https://doi.org/10.36887/2524-0455-2026-3-35.

101. Пустовіт О.Б. Світовий досвід впровадження моделей Smart City: можливості для України. ІІ науково-практична конференція за міжнародною участю «Проблеми управління суспільним розвитком в умовах криз та післякризового відновлення». Національний університет охорони здоров'я України імені П.Л. Шупика (м. Київ, 4 грудня 2025 року).

102. Пустовіт О.Б. Смарт-технології відеомоніторингу як елемент міської безпеки. IV Всеукраїнська науково-практична конференція молодих вчених та студентів «Транформаційні процеси соціально-економічної системи в умовах сучасних викликів». Університет Григорія Сковороди в Переяславі (м. Переяслав, 27 листопада 2025 року).

103. Пустовіт О.Б., Крилова І.І. Обґрунтування запровадження проектів «Безпечне місто» на державному рівні в Україні / О.Б. Пустовіт, І.І. Крилова // Інвестиції: практика та досвід – 2023. – № 11–С. 126–131. URL: https://www.nayka.com.ua/index.php/investplan/article/download/1645/1657/452.

104. Пустовіт О.Б. Крилова І.І. Управління ефективністю існуючих заходів. *Фаховий науковий журнал категорії Б з державного управління*. URL: http://perspectives.pp.ua/index.php/sas/article/view/9767/9820.

105. Сабурова Г. Б. Основні напрями розвитку системи публічного управління в України. *Публічне управління і адміністрування в Україні*. Вип. 21. 2021. С. 23–27. DOI: https://doi.org/10.32843/pma2663-5240- 2021.21.5

106. Савченко-Галушко Т. Як забезпечити захист кіберпростору України на тлі збройної агресії рф. Armyinform, 2022. URL: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahystkiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/.

107. Савчук О.М., Галай А.О. Кейс-менеджмент у роботі з внутрішньо переміщеними особами. *Наукові записки НаУКМА. Педагогічні, психологічні науки та соціальна робота.* 2016. 188. С. 70–74. URL: https://ekmair.ukma.edu.ua/handle/123456789/10815.

108. Світлична Т.В. Розвиток інтегрованих соціальних служб як інноваційної моделі надання соціальних послуг населенню. *Державне будівництво*. 2009. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2009_1_29.

109. Сергенюк Д. Щодо окремих напрямів формування суб'єктами публічного адміністрування безпечного середовища для населення в Україні. National law journal: teory and practice, 2018. Т. 31, № 3. С.54-57. URL: https://ibn.idsi.md/sites/default/files/imag_file/54-57_2.pdf.

110. Славкова, О., Фігурна М. Державна соціальна політика: проблеми та перспективи. Bulletin of Sumy National Agrarian University. (2021). № 2 (88). С. 48-52. DOI: https://doi.org/10.32845/bsnau.2021.2.9.

111. Смілевський М. Забезпечення громадської безпеки в місті на прикладі системи відеоспостереження «Безпечне місто Львів». Біологічні, хімічні та екологічні загрози під час війни: [колективна монографія]. Львів: ЛДУБЖД, 2025. С. 445–449. DOI: https://doi.org/10.32447/bcet.2025.32.

112. Смуш-Кулеша М., Федорова А., Мойса Б. Звіт про оцінку потреб щодо соціальних прав в Україні під час війни. URL: https://rm.coe.int/needsassessment-ua-2/1680a9b408.

113. Споришев К., Бондаренко О. Проєкт «Безпечне місто» як інструмент сучасного публічного управління. Development of Service Industry Management. 2026. № 3. С. 130–135. DOI: https://doi.org/10.31891/dsim-2026-15(15).

114. Стріха Л. О., Назаренко І. В., Гроза В. І. Стандартизація продукції та послуг: курс лекцій. Миколаїв: МНАУ, 2017. 80 с. URL: https://dspace.mnau.edu.ua:8443/jspui/bitstream/123456789/2107/1/standartyzatsiya.pdf.

115. Тимошенко Ю., Кисленко Д. Правоохоронна система в епоху діджиталізації. *Наукові праці Міжрегіональної Академії управління персоналом.*

Юридичні науки, №1 (59), 2022. С. 40-45. DOI: https://doi.org/10.32689/2522-4603.2020.1.6

116. Ткачук І. М. Теоретико-правова характеристика використання хмарних послуг у державному секторі України. *Юридичний вісник*. 2025. № 1. С. 134–141. URL:https://yurvisnyk.in.ua/v1_2025/19.pdf.

117. Федоренко Д.М. Програми «Безпечне місто» і «Розумне місто»: правове регулювання та кримінологічний аспект впровадження. Матеріали науково-практичної конференції Харківського національного університету внутрішніх справ. Харків, 2019. С. 98–101. URL: https://www.univd.edu.ua/general/publishing/konf/18_04_2019/pdf/47.pdf.

118. Шумілін О. СБУ заблокувала вебкамери, які зламали росіяни, щоб корегувати удари по Києву. Українська правда. 02.01.2024. URL: https://www.pravda.com.ua/news/2024/01/2/7435567/.

119. Щерба М. О. Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі. Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023): матеріали дев'ятої Міжнар. наук.-техн. конф., 7 груд. 2023 р. Харків: ХНУРЕ, 2023. С. 206–207. URL: https://openarchive.nure.ua/handle/document/25461.

120. Андріїв пообіцяв розвивати систему відеонагляду у місті. Слово і діло. URL: https://www.slovoidilo.ua/promise/42465.html.

121. Безпека громади в умовах воєнного стану: практикум / ДДУВС. Дніпро, 2025. URL: https://www.er.dduvs.edu.ua/bitstream/123456789/16787/5/%d0%bc%d0%b0%d0%ba%d0%b5%d1%82_%d0%9f%d1%80%d0%b0%d0%ba%d1%82%d0%b8%d0%ba%d1%83%d0%bc%20%d0%91%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b0%20%d0%b3%d1%80%d0%be%d0%bc%d0%b0%d0%b4%d0%b8%2015.09%2b_%d0%bf%d1%80%d0%b0%d0%b2%d0%ba%d0%b0.pdf.

122. Безпечне місто: використання інтелектуальних технологій для громадської безпеки. URL: https://www.unian.ua/science/10088759-bezpechne-misto-vikoristannya-intelektualnih-tehnologiy-dlya-gromadskoji-bezpeki.html.

123. В Апараті РНБО обговорили удосконалення роботи Головного ситуаційного центру. Інтерфакс-Україна. URL: https://interfax.com.ua/news/political/628446.html.

124. Визначено міста, найбільш дружні для дітей та молоді. Урядовий портал: вебсайт. URL: https://www.kmu.gov.ua/news/viznacheno-mista-najbilsh-druzhni-dlya-ditej-ta-molodi.

125. Відеоспостереження – більше, ніж просто засіб забезпечення безпеки. 2021. URL: https://bezpeka.club/videosposterezhennya-bilshe-nizh-prosto-zasib-zabezpechennya-bezpeky.

126. Відеоспостереження за українцями: де можуть з'явитися камери? Mind.ua. 2024. URL: https://mind.ua/openmind/20270305-videosposterezhennya-za-ukrayincyami-de-mozhut-zyavitisya-kameri.

127. Відновлення проєкту «Безпечне місто»: як сучасні системи відеоспостереження підвищують безпеку міст в умовах війни. URL: https://greenvision.ua/ua/blog/vidnovlennya-proyektu-bezpechne-misto-yak suchasni-systemy-videosposterezhennya-pidvyshchuyut-bezpeku-mist-v-umovakh-viyny.

128. Війна в Україні становить безпосередню загрозу для дітей. Unicef, 2022. URL: https://www.unicef.org/ukraine/donate-now.

129. Встановлення додаткових камер відеоспостереження на дорогах та у публічних місцях знизить рівень злочинності – Леонід Тимченко. Урядовий портал: вебсайт. [2024]. URL: https://www.kmu.gov.ua/news/vstanovlennia-dodatkovykh-kamer-videospoterezhennia-na-dorohakh-ta-u-publichnykh-mistsiakh-znyzyt-riven-zlochynnosti-leonid-tymchenko.

130. Глава Уряду: Досконалість влади і держави вимірюється якістю умов розвитку дитинства. Урядовий портал: вебсайт. [2018]. URL: https://www.kmu.gov.ua/news/glava-uryadu-doskonalist-vladi-vimiryuyetsya-yakistyu-umov-rozvitku-ditinstva.

131. Денис Монастирський: У кожній об'єднаній територіальній громаді має працювати поліцейський офіцер. Урядовий портал: вебсайт. [2021]. URL:

https://www.kmu.gov.ua/news/denis-monastirskij-u-kozhnij-obyednanij-teritorialnij-gromadi-maye-pracyuvati-policejskij-oficer.

132. Департамент поліції та прикордонної охорони Естонії. URL: http://www.pass.ee/index.php/pass/est/mis_on_id_kaart.

133. Відеофіксація в закладах освіти: досвід шкіл, плюси та мінуси від директорів, юридичні нюанси. URL: https://nus.org.ua/articles/dosvid-shkilnyuansy/.

134. Про схвалення Стратегії реформування державного управління України на 2026–2030 роки та затвердження операційного плану заходів з її реалізації: розпорядження Кабінету Міністрів України від 10.06.2026 № 768-р. URL: https://zakon.rada.gov.ua/laws/show/768-2026-%D1%80.

135. Дія.Цифрова громада: ще більше можливостей для цифрової трансформації регіонів та громад. Урядовий портал: вебсайт. 08.04.2025. URL: https://www.kmu.gov.ua/news/diiatsyfrova-hromada-shche-bilshe-mozhlyvostei-dlia-tsyfrovoi-transformatsii-rehioniv-ta-hromad.

136. Єврокомісія рекомендувала надати Україні статус кандидата на вступ до ЄС. Урядовий портал. 2022. URL: https://www.kmu.gov.ua/news/yevrokomisiya-rekomenduvala-nadati-ukrayini-statuskandidata-na-vstup-do-yes.

137. Івано-Франківськ, Київ та Вінниця стали лідерами рейтингу прозорості інвестиційного сектора – ТІ Україна. Інтерфакс-Україна. URL: https://interfax.com.ua/news/economic/537152.html.

138. Ігор Клименко: Заклади освіти мають стати максимально захищеними просторами для наших дітей. Урядовий портал: вебсайт. 29.01.2025. URL: https://www.kmu.gov.ua/news/ihor-klymenko-zaklady-osvity-maiut-staty-maksymalno-zakhyshchenymy-prostoramy-dlia-nashykh-ditei.

139. Ігор Клименко: МВС в Уряді Свириденко – результати, які зміцнюють стійкість країни. Головний сервісний центр МВС: офіційний вебсайт. 15.07.2026. URL: https://hsc.gov.ua/2026/07/15/igor-klimenko-mvs-v-uryadi-sviridenko-rezultati-yaki-zmitsnyuyut-stijkist-krayini/.

140. Встановлення додаткових камер відеоспостереження на дорогах та у публічних місцях знизить рівень злочинності, – Леонід Тимченко. Урядовий портал. URL: https://www.kmu.gov.ua/news/vstanovlennia-dodatkovykh-kamer-videospoterezhennia-na-dorohakh-ta-u-publichnykh-mistsiakh-znyzyt-riven-zlochynnosti-leonid-tymchenko.

141. Інформаційна довідка щодо доступності сервісних послуг для ветеранів та членів їхніх сімей / Дослідницька служба Верховної Ради України. Київ, [2025]. URL: https://research.rada.gov.ua/uploads/documents/33653.pdf.

142. Київ поділився досвідом створення системи протидії та запобігання насильству з представниками міст України. Офіційний портал Києва. URL: https://kyivcity.gov.ua/news/kiv_podilivsya_dosvidom_stvorennya_sistemi_protidi_ta_zapobigannya_nasilstvu_z_predstavnikami_mist_ukrani/.

143. Компенсація за оренду житла для ветеранів-переселенців: як отримати допомогу. Слово і діло. 30.09.2025. URL: https://www.slovoidilo.ua/2025/09/30/infografika/suspilstvo/kompensacziya-orendu-zhytla-veteraniv-pereselencziv-yak-otrymaty-dopomohu.

144. Львів витратить 4,3 млн грн на обслуговування камер відеоспостереження в громаді. Zaxid.net. 24.07.2024. URL: https://zaxid.net/lviv_vitratit_43_mln_grn_na_obslugovuvannya_kamer_videosposterezhennya_v_gromadi_n1590159.

145. Майже 60 % українців володіють базовими та просунутими цифровими навичками: результати дослідження Мінцифри. Урядовий портал: вебсайт. 2023. URL: https://www.kmu.gov.ua/news/93-ukraintsiv-volodiiut-tsyfrovymy-navychkamy-mintsyfry-prezentuvala-rezultaty-doslidzhennia-tsyfrovoi-hramotnosti-ukraintsiv.

146. Мапа безбар’єрності від Мінрозвитку та ЛУН визнана найкращою соціальною ІТ-ініціативою 2026 року. ЛУН Місто. 2026. URL: https://lun.ua/misto/barrier-free-map-2242.

147. Мінветеранів запустило єдину цифрову платформу для ветеранів «Ветеран Pro». Інтерфакс-Україна. 2025. URL: https://interfax.com.ua/news/telecom/1116157.html.

148. Мінрегіон та ЮНІСЕФ обговорили подальшу реалізацію ініціативи «Громада, дружня до дітей та молоді». Урядовий портал: вебсайт. URL: https://www.kmu.gov.ua/news/minregion-ta-yunisef-obgovorili-podalshu-realizaciyu-iniciativi-gromada-druzhnya-do-ditej-ta-molodi.

149. Мінрозвитку презентувало рейтинг міст за рівнем фізичної безбар'єрності. Міністерство розвитку громад та територій України: офіційний вебсайт. 11.06.2026. URL: https://mininfra.gov.ua/news/minrozvytku-prezentuvalo-reitynh-mist-za-rivnem-fizychnoi-bezbariernosti.

150. Мінсоцполітики та Фонд ООН у галузі народонаселення домовилися про впровадження спільних програм у сфері протидії насильству. Урядовий портал: вебсайт. URL: https://www.kmu.gov.ua/news/minsotspolityky-ta-fond-oon-u-haluzi-narodonaselennia-domovylys-pro-vprovadzhennia-spilnykh-prohram-u-sferi-protydii-nasylstvu.

151. Мінсоцполітики та Червоний Хрест України готують спільні алгоритми підтримки населення взимку. Урядовий портал. URL: https://www.kmu.gov.ua/news/minsotspolityky-ta-chervonyi-khrest-ukrainy-hotuiut-spilni-alhorytmy-pidtrymky-naselennia-vzymku.

152. Мінцифри об'єднує міністерства та регіони в єдину екосистему країни. Урядовий портал: вебсайт. 05.05.2026. URL: https://www.kmu.gov.ua/news/mintsyfry-obiednuie-ministerstva-ta-rehiony-v-iedynu-ekosystemu-krainy.

153. Мінцифри про підсумки та плани щодо цифровізації в Україні. Урядовий портал: вебсайт. 27.03.2023. URL: https://www.kmu.gov.ua/news/mintsyfry-pro-pidsumky-ta-plany-shchodo-tsyfrovizatsii-v-ukraini.

154. Мінцифри про результати цифрової трансформації в регіонах України за 2024 рік. Урядовий портал: вебсайт. 14.02.2025. URL:

https://www.kmu.gov.ua/news/mintsyfry-pro-rezultaty-tsyfrovoi-transformatsii-v-rehionakh-ukrainy-za-2024-rik.

155. На Вінниччині відбувся форум «Створюємо місцеві рішення разом: місцеві плани дій 1325». Вінницька обласна державна адміністрація. URL: https://www.vin.gov.ua/news/ostanni-novyny/62154-na-vinnychchyni-vidbuvsia-forum-stvoriuiemo-mistsevi-rishennia-razom-mistsevi-plany-dii-1325.

156. Нова ініціатива МВС – розширення мережі Центрів безпеки, які швидко та якісно надаватимуть послуги громадянам – Денис Монастирський. Урядовий портал: вебсайт. 26.08.2021. URL: https://www.kmu.gov.ua/news/nova-iniciativa-mvs-rozshirennya-merezhi-centriv-bezpeki-yaki-shvidko-ta-yakisno-nadavatimut-poslugi-gromadyanam-denis-monastirskij.

157. Номер 112 в Україні: єдина служба екстреної допомоги, яка координує порятунок. Netfreedom.org.ua. 2026. URL: https://netfreedom.org.ua/?p=20316.

158. Оглядове досьє щодо реалізації експериментальних проєктів Міністерства соціальної політики України («Електронний кейс-менеджмент», комплексна соціальна послуга з формування життєстійкості) / Дослідницька служба Верховної Ради України. Київ, [2025]. URL: https://research.rada.gov.ua/uploads/documents/33541.pdf.

159. Олег Уруський: Забезпечення оперативною інформацією Головного ситуаційного центру України – важливе завдання, яке вирішує ДКА. Урядовий портал. 17.07.2015. URL: https://www.kmu.gov.ua/news/248339643.

160. Онлайн-банкінг, Word та Excel: які цифрові навички необхідно покращити українцям. Урядовий портал: вебсайт. 23.03.2021. URL: https://www.kmu.gov.ua/news/onlajn-banking-word-ta-excel-yaki-cifrovi-navichki-neobhidno-pokrashchiti-ukrayincyam.

161. Органам місцевого самоврядування радять закрити інформацію на час війни. Офіційний сайт реформи децентралізації влади. URL: https://decentralization.gov.ua/news/14615.

162. Оцінка впливу війни на людей. UNDP Ukraine. URL: https://www.undp.org/sites/g/files/zskgke326/files/2023-09/undp-ua-hia-ukr-2.pdf.

163. Питання захисту прав дітей в умовах збройного конфлікту – на контролі Омбудсмана і громадськості [Електронний ресурс]. URL: http://www.ombudsman.gov.ua/ua/all-news/all-activity/6515-znpitannya-zaxistuprav-ditej-v-umovax-zbrojnogo-konfliktu-na-kontroli/.

164. План відновлення України. URL: https://uploads-ssl.webflow.com/625d81ec8313622a52e2f031/62c19ac16c921fc712205f03_NRC%20Ukraine%27s%20Recovery%20Plan%20blueprint_UKR.pdf.

165. Порядок денний чергового засідання Комітету Верховної Ради України з питань інтеграції України до Європейського Союзу 20 лютого 2026 р.: проєкт. URL: https://comeuroint.rada.gov.ua/uploads/documents/30682.pdf.

166. Практики реалізації програм зі створення безпечних міст для жінок і дівчат в Україні для втілення подальших дій / ООН Жінки в Україні. 2022. URL: https://ukraine.unwomen.org/en/digital-library/publications/2022/10/praktyky-realizatsiyi-prohram-zi-stvorennya-bezpechnykh-mist-dlya-zhinok-i-divchat-v-ukrayini-dlya-vtilennya-podalshykh-diy.

167. Презентовано перший україномовний мобільний застосунок для розвитку мовлення. Міністерство освіти і науки України: офіційний вебсайт. URL: https://mon.gov.ua/news/prezentovano-pershiy-ukrainomovniy-mobilniy-zastosunok-dlya-rozvitku-movlennya.

168. Проєкт «Безпечне місто» як інструмент державного управління у сфері забезпечення національної безпеки України // Вісник Хмельницького національного університету. Серія: Економічні науки. 2026. № 4. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/download/2964/3018/9137.

169. Проект Плану відновлення України Матеріали робочої групи «Державне управління». URL: https://www.kmu.gov.ua/diyalnisvijni/robochi-grupi.

170. Публічне управління та національна безпека. За заг. редакцією В.Ф. Залужного. Навчальний посібник. Прага: Publishing house Education and Science

s.r.o., 2025. 209 с. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/27879/1/Posib.pdf.

171. Розвиток інтегрованих соціальних служб для вразливих сімей і дітей. Проєкт ЄС. Звіт про результати діяльності за період 29 грудня 2006 р. – 29 березня 2007 р. / Консорціум «Кожній дитині». URL: http://archive.p4ec.org.ua/upload/library/pdf/ Progress%20Report_ukr.rar.

172. Сайт компанії «Датагруп» [Електронний ресурс]: [веб-сайт]. – URL: https://www.datagroup.ua/pro-kompaniyu.

173. СБУ заблокувала в Києві вебкамери, які «засвітили» роботу ППО. Укрінформ. 02.01.2024. URL: https://www.ukrinform.ua/rubric-kyiv/3808184-sbu-zablokuvala-v-kievi-vebkameri-aki-zasvitili-robotu-ppo.html.

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

175. Спецпроєкт МВС: 112 – єдиний номер безпеки для всієї країни. Головний сервісний центр МВС. URL: https://hsc.gov.ua/?p=58840.

176. Стан і функціональність укриттів в Україні: результати моніторингу Секретаріату Уповноваженого Верховної Ради України з прав людини. Київ, 2026. URL: https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/1-29052026-1509-stan-i-funktsionalnist-ukrittiv-v-ukraini-postorinkova-1.pdf.

177. Стенограма засідання Комітету Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій України, національних меншин і міжнаціональних відносин від 3 грудня 2025 року. URL: https://kompravlud.rada.gov.ua/uploads/documents/35056.pdf.

178. Стенограма засідання Комітету Верховної Ради України з питань цифрової трансформації від 24 липня 2024 року. URL: https://komit.rada.gov.ua/uploads/documents/31576.pdf.

179. Стратегія відновлення та розвитку економіки Сумської області на 2022- 2024 роки. URL: https://sm.gov.ua/images/docs/2023/strategia_2022-2024.pdf.

180. Стратегія розвитку штучного інтелекту в Україні: монографія. [За заг. ред. А.І.Шевченка]. Київ: ІПШІ, 2023. 305 с. URL: https://jai.in.ua/archive/2023/ai_mono.pdf.

181. Сьогодні Стамбульська конвенція набуває чинності для України. Уповноважений Верховної Ради України з прав людини: офіційний вебсайт. 01.11.2022. URL: https://www.ombudsman.gov.ua/news_details/sogodni-stambulska-konvenciya-nabuvaye-chinnosti-dlya-ukrayini.

182. Безпечне місто: єдиний інформаційний простір системи безпеки громад / «Датагруп». URL: https://www.datagroup.ua/storage/files/bezpechne-misto-ua.pdf.

183. У Києві презентували трирічну програму «Жінки, мир, безпека: місцеві потреби – місцеві рішення». АрміяInform. 25.01.2022. URL: https://armyinform.com.ua/2022/01/25/u-kyyevi-prezentuvaly-tryrichnu-programu-zhinky-myr-bezpeka-misczevi-potreby-%e2%80%92-misczevi-rishennya/.

184. У МВС прокоментували законопроєкт про відеонагляд у публічних місцях. LB.ua. 22.02.2024. URL: https://lb.ua/society/2024/02/22/599766_mvs_prokomentuvali_zakonoproiekt.html.

185. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. Офіційний портал Києва. 15.02.2019. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv/.

186. Українське суспільство в умовах війни. 2022: Колективна монографія / С. Дембіцький, О. Злобіна, Н. Костенко та ін.; за ред. член.-кор. НАН України, д. філос. н. Є. Головахи, д. соц. н. С. Макеєва. Київ: Інститут соціології НАН України, 2022. 410 с. URL: https://isnasu.org.ua/assets/files/monitoring/maket-vijna...2022dlya-tipografiivse.pdf.

187. Усміхніться, вас знімають: як відеокамери слідкують за киянами. Світовий досвід. URL: https://uain.press/articles/usmihnitsya-kyyanamy-647562

188. ₴60.7 million was spent on the construction of the «Safe City» video surveillance system over 5 years in Mykolaiv. NikVesti. 2026. URL: https://nikvesti.com/en/news/public/312989-construction-607-million-safe-city-surveillance-2026.

189. Хмельницький визнали найбезпечнішим у рейтингу міст України. ZAXID.NET.02.05.2017.URL:https://zaxid.net/hmelnitskiy_viznali_naybezpechnishim_u_reytingu_mist_ukrayini_n1424793.

190. Цифрова варта. Як IT-технології роблять українські міста безпечнішими. URL: https://techno.nv.ua/ukr/it-industry/pechne-misto-shcho-ce-take50137653.html.

191. Цифрова держава: хто її будує і як навчають лідерів цифрової трансформації. Тексти.org.ua. URL: https://texty.org.ua/fragments/117622/cyfrova-derzhava-xto-yiyi-buduye-i-yak-navchayut-lideriv-cyfrovoyi-transformaciyi/.

192. Цифровізація громад: які результати діджитал-проектів у регіонах. Урядовий портал: вебсайт. 08.01.2024. URL: https://www.kmu.gov.ua/news/tsyfrovizatsiia-hromad-iaki-rezultaty-didzhytal-proektiv-u-rehionakh.

193. Цифровізація соціальної сфери – національний проект для покращення якості надання соціальної підтримки громадянам. Урядовий портал: вебсайт. 14.04.2021. URL: https://www.kmu.gov.ua/news/cifrovizaciya-socialnoyi-sferi-nacionalnij-proekt-dlya-pokrashchennya-yakosti-nadannya-socialnoyi-pidtrimki-gromadyanam.

194. Чернівці очолили рейтинг прозорості та підзвітності з-поміж 100 міст України. Zaxid.net. 19.05.2025. URL: https://zaxid.net/chernivtsi_ocholili_reyting_prozorosti_ta_pidzvitnosti_z_pomizh_100_mist_ukrayini_n1610611/amp.

195. Як у Чернігові створили простір для підтримки ветеранів і де знайшли кошти. The Page. 2025. URL: https://thepage.ua/ua/style/life-style/yak-znajti-groshi-dlya-veteranskogo-prostoru-kejs-chernigova.

196. Які міста очолили рейтинг прозорості та підзвітності місцевої влади – Transparency International. Тексти.org.ua. [2023]. URL: https://texty.org.ua/fragments/109392/yaki-mista-ocholyly-rejtynh-prozorosti-ta-pidzvitnosti-miscevoyi-vlady-transparency-international.

197. 5 things to know about Virtual Singapore. Government Technology Agency of Singapore (GovTech). URL: https://www.tech.gov.sg/technews/5-things-to-know-about-virtual-singapore/.

198. Akimov, O., Troschinsky, V., Karpa, M., Ventsel, V., & Akimova, L. (2020) International experience of public administration in the area of national security. *Journal of Legal, Ethical and Regulatory Issues*, Volume 23, Issue 3, 2020. URL: https://www.abacademies.org/articles/international-experience-of-public-administration-in-the-area-of-national-security-9307.html.

199. Andros, S., Akimov, O., Akimova, L., Chang, S., & Gupta, S. K. (2021). Scenario Analysis of the Expected Integral Economic Effect from an Innovative Project. Marketing and Management of Innovations 3, 237-251. DOI: https://doi.org/10.21272/mmi.2021.3-20.

200. Angelidou M., Gountaras N., Tarani P. Engaging digital services for the creation of urban knowledge ecosystems: the case of Thermi, Greece. *International Journal of Knowledge-Based Development*, 2012. Vol. 3, № 4, P. 331-350. DOI: https://doi.org/10.1504/IJKBD.2012.050090

201. Angelidou M., Psaltoglou A. Social innovation, games and urban planning: an analysis of current approaches. International Journal of Electronic Governance, 2019. Vol. 11. № 1. P. 5-22. DOI: https://doi.org/10.1504/IJEG.2019.098807

202. Angelidoua M., Karachalioua E., Stylianidisa E. Encouraging urban planning and development practice to contribute to sustainable development. A methodology and a use case. International Journal of Real Estate and Land Planning, 2018. Vol. 1. P. 322-330. URL: https://scholar.archive.org/work/zr237nxyivgntit7b26jbd2awy/access/wayback/https://ejournals.lib.auth.gr/reland/article/download/6488/6231.

203. ANPR: один з ключових елементів розумного міста. 2023. URL: https://bezpeka.club/anpr-klyuchovyjelement-rozumnogo-mista.

204. Barker R. The social work dictionary. [5th ed.]. Washington, DC: NASW Press, 2003. 493 p. ISBN 0-87101-355-X.

205. Becker Gary S. Human Capital: A Theoretical and Empirical Analysis, with Special Reference to Education, University of Chicago Press, 1994, 412 c. ISBN 0-226-04119-0. URL: https://www.nber.org/books-and-chapters/human-capital-theoretical-and-empirical-analysis-special-reference-education-third-edition.

206. Brian Lee-Archer, Effects of digitalization on the human centricity of social security administration and services [Електронний ресурс]: робочі документи. – URL: https://www.ilo.org/static/english/intserv/workingpapers/wp087/index.html.

207. Building safer cities with AI: Machine learning model enhances urban resilience against liquefaction. PreventionWeb (UNDRR). 2024. URL: https://www.preventionweb.net/news/building-safer-cities-ai-machine-learning-model-enhances-urban-resilience-against-liquefaction.

208. Buzan B. People, States and Fear: The National Security Problem in International Relations. Brighton: Wheatsheaf Books, 1983. 262 p. ISBN 0-7108-0106-8.

209. Carr J. B., Doleac J. L. The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using ShotSpotter Data. Washington: Brookings Institution, 2016. URL: https://www.brookings.edu/articles/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/.

210. Chalfin A., Hansen B., Lerner J., Parker L. Reducing Crime Through Environmental Design: Evidence from a Randomized Experiment of Street Lighting in New York City. Journal of Quantitative Criminology. 2022. Vol. 38, No. 1. P. 127–157. URL: https://www.nber.org/papers/w25798.

211. City of Chicago Office of Inspector General. The Chicago Police Department's Use of ShotSpotter Technology: report. Chicago, 2021. URL: https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-

evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

212. Connect Birmingham: program page. Birmingham Police Department (Alabama, USA). URL: https://police.birminghamal.gov/connectbirmingham/.

213. Doris Pasha, E-Governance and the Importance of Personal Data Protection [Електронний ресурс]: доповідь. URL: https://www.dcaf.ch/sites/default/files/imce/ECA/D.Pasha-YoungFaces2022.pdf.

214. Drone Program: Drone as First Responder (DFR). Chula Vista Police Department (California, USA). URL: https://chulavistaca.gov/departments/police-department/programs/uas-drone-program.

215. FCC Adds All Foreign-Made UAS and UAS Critical Components to Covered List: client alert. Akin Gump Strauss Hauer & Feld LLP. 31.12.2025. URL: https://www.akingump.com/en/insights/alerts/fcc-adds-all-foreign-made-uas-and-uas-critical-components-to-covered-list.

216. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects: NISTIR 8280. Gaithersburg: National Institute of Standards and Technology, 2019. 81 p. DOI: https://doi.org/10.6028/NIST.IR.8280.

217. High Court backs Live Facial Recognition, with clear legal limits. DWF. 02.06.2026. URL: https://dwfgroup.com/en/news-and-insights/insights/2026/6/high-court-backs-live-facial-recognition-with-clear-legal-limits.

218. Hillman J. E., McCalpin M. Watching Huawei's "Safe Cities": CSIS Brief. Washington: Center for Strategic and International Studies, 2019. URL: https://www.csis.org/analysis/watching-huaweis-safe-cities.

219. How Japan's 'opt-in' smart city could change urban living. World Economic Forum. 2021. URL: https://www.weforum.org/stories/forum-institutional/japanese-smart-city-residents-privacy-protection-data/.

220. HTX Ground Robot on trial at Toa Payoh Central to support Public Officers in enhancing public health and safety: joint media release. Singapore Food Agency. 2021. URL: https://sfa.gov.sg/newsroom/press-releases/joint-media-release--

-htx-ground-robot-on-trial-at-toa-payoh-central-to-support-public-officers-in-enhancing-public-health-and-safety.

221. ISO 22341:2021. Security and resilience – Protective security – Guidelines for crime prevention through environmental design. Geneva: ISO, 2021. 23 p. URL: https://www.iso.org/standard/50078.html.

222. ISO 37122:2019. Sustainable cities and communities – Indicators for smart cities. Geneva: ISO, 2019. URL: https://www.evs.ee/en/iso-37122-2019.

223. ISO 37123:2019. Sustainable cities and communities – Indicators for resilient cities. Geneva: ISO, 2019. URL: https://www.evs.ee/en/iso-37123-2019.

224. Japan Smart Cities: Market Intelligence. International Trade Administration (USA). URL: https://www.trade.gov/market-intelligence/japan-smart-cities.

225. Kitchin R. Urban Data Power: Capitalism, Governance, Ethics, and Justice. Data Power in Action, 2023. P. 21-41. DOI: https://doi.org/10.51952/9781529233551.ch002.

226. Kitchin R., Coletta C., McArdle G. Governmentality and urban control. The Routledge Companion to Smart Cities, 2020. P. 109-122. DOI: https://doi.org/10.4324/9781315178387-9.

227. Levine E. S., Tisch J., Tasso A., Joy M. The New York City Police Department's Domain Awareness System. Interfaces. 2017. Vol. 47, No. 1. DOI: https://doi.org/10.1287/inte.2016.0860.

228. Liudmyla Antonova, Dmytro Havrychenko, Roman Primush, Vitalii Kropyvnytskyi, Violeta Tohobytska. Modern Aspects of SMART-Management of the Region in the Context of the Development of Public Administration. IJCSNS.International Journal of Computer Science and Network Security. 2022. Vol. 22. №5, pp. 469–474. DOI: https://doi.org/10.22937/IJCSNS.2022.22.5.66

229. London cops bring live facial recognition to West End. The Register. 2026. URL: https://www.theregister.com/a/5261031.

230. Ministry of Land, Infrastructure, and Transport Announcement No. 2024-129: 2024 Sector-specific Smart City Regulatory Sandbox (crime prevention and disaster prevention). Smart City Korea. URL: https://smartcity.go.kr/en/?p=37374.

231. Nabatchi T., Gastil J., Weiksner G. M., Leighninger M. «The Many Faces of Public Participation: Towards a Theoretical Typology». Journal of Public Administration Research and Theory, 22(3), 506-526. 2012. DOI: https://doi.org/10.1093/jopart/mur047.

232. NEC-led consortium awarded the Singapore Safe City Test Bed Project: press release. NEC Corporation. 29.05.2013. URL: https://www.nec.com/en/press/201305/global_20130529_04.html.

233. New York City Police Department. Domain Awareness System (DAS): Impact and Use Policy. Updated February 4, 2026. URL: https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/Domain-Awareness-System-NYPD-Impact-and-Use-Policy-2.4.26-FINAL.pdf.

234. OECD. Rebuilding Ukraine by Reinforcing Regional and Municipal Governance. OECD Multi-level Governance Studies. Paris: OECD Publishing, 2022. 338 p. ISBN 978-92-64-45152-0 (PDF). URL: https://www.oecd.org/en/publications/rebuilding-ukraine-by-reinforcing-regional-and-municipal-governance_63a6b479-en/full-report.html.

235. Piza E. L., Welsh B. C., Farrington D. P., Thomas A. L. CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology & Public Policy. 2019. Vol. 18, No. 1. P. 135–159. DOI: https://doi.org/10.1111/1745-9133.12419

236. Policy Task: About Smart Seoul. Seoul Metropolitan Government. URL: https://smart.seoul.go.kr/en/content/view/EN01030000.do.

237. Project PLATEAU: The Initiative of Digital Twin in Japan. Ministry of Land, Infrastructure, Transport and Tourism of Japan (MLIT). URL: https://www.mlit.go.jp/plateau/en/.

238. Regional and municipal authorities key to Ukraine's resilience: press release. OECD. 02.12.2022. URL: https://www.oecd.org/en/about/news/press-releases/2022/12/regional-and-municipal-authorities-key-to-ukraine-s-resilience.html.

239. Richmond Soft Launches Real Time Crime Center press release. City of Richmond (Virginia, USA). 20.12.2023. URL: https://rva.gov/press-releases-and-announcements/news/richmond-soft-launches-real-time-crime-center.

240. Safe Cities and Safe Public Spaces Programme Overview. UN Women Virtual Knowledge Centre to End Violence against Women and Girls. URL: https://www.endvawnow.org/en/initiatives-articles/42-safe-cities-and-safe-public-spaces-programme-overview.html.

241. Safer Cities through Information Sharing: NEC Innovation Series. NEC Corporation, 2014. URL: https://sa.nec.com/en_SA/en/global/solutions/safety/InterAgency/pdf/SaferCities_through_information_sharing.pdf.

242. Smart City Integrated Platform. Korea's Smart City Solutions: Best Practices & Technologies. Smart City Korea. 2023. URL: https://smartcity.go.kr/wp-content/uploads/2023/10/EN01.Smart-City-Integrated-Platform.pdf.

243. Step 16: Study the journey to crime. Center for Problem-Oriented Policing. URL: https://www.popcenter.org/node/3652.

244. Stronger cities for the future: a new set of International Standards just out. ISO News. [2019]. URL: https://www.iso.org/news/ref2305.html.

245. Surveillance Camera Code of Practice: amended November 2021. London: Home Office, 2021. 18 p. ISBN 978-1-5286-2983-6. URL: https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf.

246. Sustainable Smart Town Provides Better Lifestyles as the Entire Town: Fujisawa SST. Panasonic Holdings Corporation. URL: https://holdings.panasonic/global/corporate/sustainability/sdgs/case-tudy/case01.html.

247. The Smart Nation vision. Smart Nation Singapore: Ministry of Digital Development and Information. URL: https://smartnation.gov.sg/about/our-vision/smart-nation-vision.

248. Ukraine Fifth Rapid Damage and Needs Assessment (RDNA5): February 2022 – December 2025 / World Bank, Government of Ukraine, European Union, United Nations. 2026. URL: https://euneighbourseast.eu/wp-content/uploads/2026/09/ukraine fifth_rapid_damage_and_needs_assessment.pdf.pdf.

249. UNDP. Human Development Report 1994: New Dimensions of Human Security. New York: United Nations Development Programme, 1994. URL: https://hdr.undp.org/en/reports/global/hdr1994.

250. UN-Habitat. 11.7 Public space. URL: https://unhabitat.org/11-7-public-space.

251. United Nations System-wide Guidelines on Safer Cities and Human Settlements. Nairobi: UN-Habitat, 2020. 34 p. URL: https://unhabitat.org/sites/default/files/2020/03/un_systemwide_guidelines_on_safer_cities_and_human_settlements.pdf.

252. Updated Ukraine Recovery and Reconstruction Needs Assessment Released: press release. World Bank. 23.02.2026. URL: https://www.worldbank.org/en/news/press-release/2026/02/23/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.

253. UrbSecurity. Planning safer cities: URBACT Action Planning Network (2020–2022). URBACT. URL: https://urbact.eu/networks/urbsecurity.

254. Welsh B. C., Farrington D. P. Effects of Improved Street Lighting on Crime. Campbell Systematic Reviews. 2008. Vol. 4, No. 1. P. 1–51. DOI: https://doi.org/10.4073/csr.2008.13.

255. What is ShotSpotter? What to know after city decides to not renew contract to use controversial technology. NBC Chicago. 2024. URL: https://nbcchicago.com/news/local/what-is-shotspotter-what-know-after-city-decides-to-not-renew-contract-to-use-controversial-technology/3355645.

256. Özdemir A., Kourtit K., & Nijkamp P. Social policy in smart cities: the forgotten dimension. Smart Cities in the Post-algorithmic Era. Edward Elgar Publishing, 2019. P. 235-261. DOI: https://doi.org/10.4337/9781789907056.00020

257. Pattoni L. Strengths-based approaches for working with individuals. IRISS Insights. Institute for Research and Innovation in Social Services. 2012. No. 16. URL: https://www.iriss.org.uk/sites/default/files/iriss-insight-16.pdf.

258. Schultz Theodore W. Investing in People: The Economics of Population Quality, University of California Press, 2020, 188 c. URL: https://www.ucpress.edu/flyer/books/investing-in-people/paper.

259. Tunggal A.T. Why is Cybersecurity Important? Abi Tyas Tunggal. UpGuard. 2021. – Режим доступу: https://www.upguard.com/blog/cybersecurity-important.

ДОДАТКИ

Додаток А

Напрями впровадження хмарних рішень для повоєнної відбудови інфраструктури міста Києва за стандартами «розумного міста» (Smart City)

Напрям	Технологія	Суть впровадження	Практичне застосування
Єдиний міський масштабний державний цифровий проєкт	Розширення на хмарній платформі інтегрованого міського інформаційно-комунікаційного центру	Замість відбудови локальних серверних кімнат у комунальних установах, які є вразливими до обстрілів, використовуються розподілені хмарні платформи	Створення цифрових двійників інфраструктури. На хмарну платформу завантажуються 3D-моделі руйнувань, підземних комунікацій (водопостачання, тепломережі) та транспортних розв'язок.
Нейровідеоаналітика та хмарна безпека (Safe City)	Хмарні платформи обробки відеопотоків із функціями штучного інтелекту	Перенесення Ситуаційного центру міста та систем відеоспостереження на хмарну платформу. Фізичне знищення камери або локального реєстратора не призводить до втрати критично важливих даних	Камери фіксують дорожню ситуацію, надзвичайні події чи руйнування інфраструктури. Хмарна ШІ-система безпосередньо аналізує потік даних, миттєво сповіщаючи рятувальні та комунальні служби про завали, пожежі або ДТП для ситуаційного реагування.
Мобільність та система сервісів для киян	Хмарні SaaS-рішення (програмне забезпечення як сервіс)	Консолідація всіх муніципальних служб (транспорт, медицина, ЦНАП, ЖКГ) в єдину хмарну систему, доступну через чат-боти та застосунки	Автоматизована система диспетчерської служби «1562» повністю функціонує на хмарній платформі, реєструючи та розподіляючи заявки на ремонт пошкодженої інфраструктури. Чат-бот «Твій дім» на хмарній платформі обробляє запити щодо пошкодженого майна, виплати компенсацій та надання медичної або гуманітарної допомоги ВПО

Джерело: складено автором на основі проведених досліджень

Додаток Б

Трирівнева інфраструктура масштабних національних рішень проєктів «Безпечне місто»

Рівень	Компоненти	Функції	Технології
Моніторинг та збір даних	IoT-датчики, камери відеобереження, GPS-трекери, smart-лічильники, кінцеві пристрої користувачів (смартфони), локальні сервери	• фіксація фізичних чи цифрових показників (температура, трафік, біометричні дані, транзакції); • первинна фільтрація та агрегація даних на місцях (щоб не перевантажувати мережу непотрібним трафіком); • шифрування даних безпосередньо на пристрої перед відправкою	Протоколи зв'язку – MQTT, CoAP, HTTPS, 5G/6G, LoRaWAN
Обробка, аналіз та зберігання даних	кластери серверів, системи розподіленого зберігання, аналітичні платформи, штучний інтелект та машинні навчання	• аналіз критично важливих даних у режимі реального часу (наприклад, виявлення кібератак чи аварій на критичній інфраструктурі); • пакетний аналіз великих масивів історичних даних для виявлення трендів та довгострокового планування; • зберігання та структурування даних у захищених базах для швидкого доступу та забезпечення суворої відповідності законодавству про захист персональних даних [16] • візуалізація поточної ситуації в країні або галузі для керівництва (KPI, карти ризиків, графіки)	Apache Kafka, Spark, Hadoop, SQL/NoSQL бази даних (PostgreSQL, Cassandra), прогнозування за допомогою штучного інтелекту
Управління та прийняття рішень	ситуаційні центри, диспетчерські пульти, інтерактивні дашборди (BI-системи), автоматизовані системи керування, мобільні застосунки для	• автоматичне керування шляхом надсилання зворотних команд на рівень моніторингу (наприклад, автоматичне перекриття засувки на газопроводі у разі витоку або зміна фаз світлофорів для розвантаження доріг);	Tableau, PowerBI, системи ERP/CRM, API-шлюзи для інтеграції, шини обміну даними

	посадовців чи громадян	• координація взаємодії між різними державними відомствами на основі єдиного джерела даних	

Джерело: складено автором на основі проведених досліджень [81]

Додаток В

Напрями потенційного впровадження поліцентричної міської структури в містах України

Джерело: складено автором на основі проведених досліджень

Додаток Г

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

1. Пустовіт О. Б., Крилова І. І. Обґрунтування запровадження проектів «Безпечне місто» на державному рівні в Україні. *Інвестиції: практика та досвід.* 2023. № 11. С. 126-131. DOI: https://doi.org/10.32702/2306-6814.2023.11.126 *(Крилова І. І. – здійснено систематизацію вітчизняного та зарубіжного досвіду цифрової трансформації муніципальної інфраструктури й виокремлено організаційно-правові передумови централізації безпекових проєктів. Пустовіт О. Б. – обґрунтовано необхідність переходу від локальних ініціатив до загальнодержавного рівня задля цифрової трансформації публічного адміністрування).*

2. Пустовіт О. Б., Крилова І. І. Управління ефективністю існуючих заходів забезпечення безпеки міст. *Науковий журнал «Успіхи та досягнення в науці».* 2024. № 1 (1). С. 258-266. DOI: https://doi.org/10.52058/3041-1254-2024-1(1)-258-266. (*Крилова І. І. – розроблено аналітичний підхід до оцінювання результативності превентивних заходів та структуровано взаємодію екстрених служб у єдиному інформаційному просторі міст. Пустовіт О. Б. – розкрито аналіз наявних інструментів забезпечення публічного порядку й безпеки життєдіяльності в містах України зокрема в умовах воєнного стану та адаптації до повоєнного відновлення).*

3. Пустовіт О. Б., Крилова І. І. Оцінка ефективності існуючих заходів забезпечення безпеки міст. *Науковий журнал «Успіхи та досягнення в науці».* 2024. № 2 (2). С. DOI: https://doi.org/10.52058/3041-1254-2024-2(2)-196-204 *(Крилова І. І. – описано методології оцінювання того, як органи публічної влади керують безпековими ризиками, координують дії екстрених служб і впроваджують превентивні заходи. Пустовіт О .Б. – описано методології*

оцінювання того, як органи публічної влади керують безпековими ризиками, координують дії екстрених служб і впроваджують превентивні заходи)

4. Пустовіт О. Б. Передумови та цілі впровадження проєктів «Безпечне місто» на державному рівні. *Актуальні проблеми інноваційної економіки та права.* 2026. №3. С. 187-191. DOI: https://doi.org/10.36887/2524-0455-2026-3-35 .

5. Пустовіт О. Б. Проєкт «Безпечне місто» як інструмент державного управління у сфері забезпечення національної безпеки України. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С. 389-397. DOI: https://doi.org/10.31891/2307-5740-2026-356-52.

Тези наукових доповідей

6. Пустовіт О. Б. Проекти «Безпечне місто»: запровадження на державному рівні в Україні. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : матеріали І Міжнар. наук.-практ. конф. (2 черв. 2023 р.) / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 220-223.

7. Пустовіт О. Б. Значення проектів «Безпечне місто» на державному рівні в Україні. *Складові національної безпеки в умовах воєнного стану* : матеріали наук.-практ. конф. з міжнар. участю (м. Київ, 09-11 серп. 2023 р.) / за заг. ред. З. В. Гбур. Кам'янець-Подільський : Друкарня Рута, 2023. С. 413-418.

8. Пустовіт О. Б. Обгрунтування запровадження проектів «Безпечне місто». *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : матеріали ІІ Міжнар. наук.-практ. конф. (27 жовт. 2023 р.) / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 188–191.

9. Пустовіт О. Б. Потенціал впровадження проектів «Безпечне місто в Україні». *Національна безпека України в умовах воєнного стану* : матеріали І наук.-практ. конф. з міжнар. участю (м. Чернігів, 06-08 берез. 2024 р.) / за заг. ред. З. В. Гбур. Чернігів : ІПТ, 2024. С. 208-211.

10. Пустовіт О. Б. Оцінка ефективності існуючих заходів забезпечення безпеки міст. *Тренди сталого розвитку для України* : зб. тез І наук.-практ. конф. за міжнар. участю (м. Чернігів – м. Київ, 10 лип. 2024 р.). Чернігів : УТМ, 2024.

С. 77–80.

11. Пустовіт О. Б. Державне управління процесом реалізації програми «Безпечне місто» в умовах цифрової трансформації. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : зб. наук. пр. з матеріалами VII Міжнар. наук. конф. (м. Харків, 31 лип. 2026 р.) / Міжнар. центр наук. досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 59–61.

Довідки про впровадження

Додаток Д

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№13/3-271 від 02 вересня 2026р.

ДОВІДКА

Видана здобувачу освіти **Пустовіту Олексію Борисовичу** про те, що він у ході виконання дисертаційного дослідження на тему **«Обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні»** приймав участь у виконанні науково-дослідної теми кафедри міжнародних відносин та політичного консалтингу «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322).

Директор Інституту права та суспільних відносин **Тетяна ФЕДОРЕНКО**

Додаток Е

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№ 1243-270 від 02 жовтня 2026 р.

Довідка

про впровадження

результатів наукового дослідження у навчальний процес

видана **Пустовіту Олексію Борисовичу** про те, що результати його дисертаційного дослідження на здобуття наукового ступеня доктора філософії на тему ««**Обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні**»» за спеціальністю 281 «Публічне управління та адміністрування» були використані при розробці робочих програм, силабусів, а також під час викладання таких навчальних дисциплін як «Громадські об'єднання в Україні» за програмою підготовки фахівців освітнього рівня «бакалавр», «Міжнародна та національна безпека» за програмою підготовки фахівців освітнього рівня «магістр».

Завідувач кафедри міжнародних відносин
та політичного консалтингу
Інституту права та суспільних відносин
ЗВО «Відкритий міжнародний університет
розвитку людини «Україна»
к.пол.н., доцент **Тетяна КАДЛУБОВИЧ**

Додаток Ж

Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів вул. Бориса Грінченка, 1, 2-й поверх, м. Київ, 01001

№ 02-34/2026 від 21. 09 2026 р.

ДОВІДКА

про впровадження результатів дисертаційного дослідження **Пустовіта Олексія Борисовича** на тему **«Обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні»** на здобуття наукового ступеня докора філософії в галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування»

видано Пустовіту Олексію Борисовичу, здобувачу ступеня доктора філософії, про те, що положення та результати його дисертаційного дослідження на тему «Обґрунтування запровадження проєктів «Безпечне місто» на державному рівні в Україні», виконаного на кафедрі міжнародних відносин та політичного консалтингу у ЗВО «Відкритий міжнародний університет розвитку людини «Україна», становлять практичний інтерес для діяльності Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, у частині вдосконалення інформаційно-аналітичного забезпечення, розвитку цифрових інструментів оброблення інформації та організації міжвідомчої інформаційної взаємодії.

Зокрема, практичне значення мають такі науково-практичні положення та рекомендації дисертаційного дослідження: рекомендації щодо використання хмарних технологій та інтелектуальної аналітики даних, спрямовані на вдосконалення процесів оброблення, систематизації та захищеного зберігання інформації, підвищення ефективності інформаційно-аналітичного забезпечення та підтримки прийняття управлінських рішень; пропозиції щодо інтеграції інформаційних систем та стандартизації цифрових рішень, які передбачають забезпечення технологічної сумісності інформаційних ресурсів, організацію захищеного інформаційного обміну, дотримання вимог інформаційної безпеки та захисту персональних даних.

Зазначені положення та рекомендації адаптовані до потреб інформаційно-аналітичної діяльності Управління виявлення та розшуку активів, зокрема під час опрацювання інформації з різних джерел, удосконалення міжвідомчої інформаційної взаємодії та розвитку цифрових інструментів забезпечення управлінських процесів.

Практичне значення результатів дисертаційного дослідження полягає у використанні запропонованих організаційних і технологічних підходів для підвищення ефективності інформаційно-аналітичної діяльності, забезпечення надійності та захищеності інформаційних ресурсів, а також удосконалення інформаційного забезпечення діяльності у сфері виявлення та розшуку активів.

Начальник Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів **Ніна МИРОНЮК**

Начальник
Управління персоналу