

УДК 351.005.8

JEL O29

DOI <https://doi.org/10.32782/2786-765X/2026-14-21>**Некряч А.І.**

доктор політичних наук, професор,
професор кафедри міжнародних відносин та політичного консалтингу,
Інститут права та суспільних відносин
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
ORCID: <https://orcid.org/0000-0001-5058-4145>

Дабіжа В.В.

кандидат наук з державного управління, доцент,
доцент кафедри міжнародних відносин та політичного консалтингу,
Інститут права та суспільних відносин
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
ORCID: <https://orcid.org/0000-0002-7000-4635>

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ПРИ ЗАПРОВАДЖЕННІ ПРОЄКТІВ «БЕЗПЕЧНЕ МІСТО» В УКРАЇНІ

У статті досліджено особливості та перспективи використання хмарних технологій у процесі запровадження проєктів «Безпечне місто» в Україні як важливого напрямку цифрової трансформації системи публічного управління та забезпечення громадської безпеки. Обґрунтовано актуальність переходу від традиційної локальної ІТ-інфраструктури до сучасних моделей хмарних обчислень, що зумовлено стрімким зростанням обсягів даних, отриманих із систем відеоспостереження та IoT-пристроїв, необхідністю їх оперативного опрацювання, зберігання та використання для прийняття управлінських рішень. Розкрито сутність концепції Cloud Smart як комплексного підходу до використання публічних, приватних і гібридних хмарних середовищ, що дає змогу забезпечити оптимальний баланс між безпекою, гнучкістю, масштабованістю та економічною ефективністю цифрової інфраструктури. Систематизовано основні моделі хмарного обслуговування IaaS, PaaS, SaaS і XaaS, а також моделі розгортання хмарної інфраструктури: публічну, приватну, гібридну та мультихмарну. Визначено основні критерії оцінювання ефективності хмарної IoT-архітектури, зокрема техніко-експлуатаційні показники, економічну доцільність, рівень кібербезпеки, масштабованість та енергоефективність. Акцентовано увагу на безпекових ризиках централізованого зберігання даних, необхідності застосування сучасних механізмів шифрування, багатфакторної автентифікації та принципів Zero Trust. Доведено, що використання хмарних технологій у проєктах «Безпечне місто» сприяє підвищенню відмовостійкості цифрової інфраструктури, забезпечує оперативне масштабування обчислювальних ресурсів та створює умови для інтеграції технологій штучного інтелекту. Визначено стратегічні напрями подальшого розвитку, серед яких застосування хмарного штучного інтелекту для прогнозування правопорушень і управління транспортними потоками, а також формування єдиної національної платформи відеомоніторингу з інтеграцією регіональних систем «Безпечне місто».

Ключові слова: державне управління, держава, безпека, безпечне місто, інфраструктура, безпекові програми, хмарні технології.

Постановка проблеми. Запровадження комплексних систем відеонагляду та міського моніторингу в рамках загальнонаціональних і місцевих проєктів «Безпечне місто» стало одним із ключових напрямів цифровізації українських міст. Стрімке зростання обсягів відеопотоків, необхідність інтеграції аналітики штучного інтелекту та потреба у безпечній функціонуванні інфраструктури актуалізують перехід від локальних серверних рішень до сучасних моделей хмарних обчислень.

Використання хмарних технологій у проєктах «Безпечне місто» дозволить представникам місцевих органів державної влади миттєво масштабувати інфраструктуру

відеоспостереження та аналітики без необхідності обслуговувати спеціалізовані будівлі або приміщення для безпечного розміщення серверного та мережевого обладнання. Проте, головною проблемою залишається кібербезпека критичних даних в умовах військового стану. Інтеграція хмарних обчислень в інфраструктуру українських міст дозволить оцінити ефективність застосування хмарних технологій в концепті архітектури Інтернету речей (IoT) для оптимізації громадської безпеки та міського життя в режимі реального часу.

Технічні та організаційні аспекти розгортання таких інтегрованих систем моніторингу наведено обґрунтовують доцільність

об'єднання архітектури Інтернету речей (IoT), штучного інтелекту та IP-відеокамер зі вбудованою аналітикою у гнучких хмарних середовищах.

Аналіз останніх досліджень і публікацій. Теоретичні основи формування єдиного інформаційного простору в розрізі концепції «Безпечне місто» активно досліджуються як вітчизняними, так і закордонними фахівцями.

Дотримання принципу державного регулювання спрямованого на пріоритетне будьяких нових інформаційних систем в Україні, зокрема концепція Cloud First («насамперед хмарні технології»), підкреслює стратегічний вектор України на цифрову трансформацію публічного сектору [1].

Дослідженнями та оцінкою ефективності застосування хмарних технологій в архітектурі Інтернету речей активно здійснюють науковці та викладачі: В.В. Максимов, співавтор досліджень щодо показників ефективності хмарних технологій та Інтернету речей для Smart city [16], А.В. Мошинська аналізує застосування хмарних платформ для IoT-додатків [10], Б.Ю. Жураковський та І.О. Зенів розглядають класичну еталонну модель архітектури Інтернету речей (IoT) та її інтеграцію з хмарними технологіями. У цій архітектурі автори виділяють такі базові рівні:

- рівень сприйняття (Perception layer): фізичні датчики, сенсори та актуатори, що збирають дані про середовище (наприклад, температура, рух) та виконують команди;
- рівень мережі (Network layer): технології передачі даних від пристроїв до хмари, включно із бездротовими протоколами малого (Bluetooth, Wi-Fi) та великого радіусу дії (LoRaWAN, SigFox, стандарти NB-IoT);
- рівень застосунків (Application layer): безпосередня інтеграція з хмарними платформами для зберігання, обробки великих масивів інформації та управління кінцевими пристроями Інтернет-речей (IoT) (наприклад, платформа Smart Grid, сервіси Oracle) [8].

Оскільки система «Безпечне місто» оперує конфіденційними даними (розпізнавання облич, автомобільних номерів, відстежування громадян), окремий напрям публікацій присвячено проблемам інформаційної безпеки даних. Дослідження таких авторів, як І.М. Іванова, А.І. Коваленко, О.П. Лебедєв, Ю.С. Харченко та В.В. Шевченко, фокусуються на викликах і загрозах кібербезпеки в умовах хмарних обчислень [5]. Науковці наголошують на критичній необхідності використання гібридних і приватних хмарних технологій, впровадження багатофакторної автентифікації (методу захисту, який

вимагає підтвердження особи кількома різними способами), шифрування даних під час передачі та концепції Zero Trust Security («не вірити нікому і все перевіряти»). Окрім того, М.О. Щерба розглядає світові стандарти налаштування параметрів безпеки хмарних сервісів, зокрема методології Center for Internet Security (CIS) та Well-Architected Framework [11].

У переважній більшості сучасних публікацій використання хмарних технологій розглядаються або загально (для абстрактного державного сектору), або суто технічно (як інструмент збереження даних). Недостатньо висвітленими залишаються:

- оптимізація хмарної архітектури під специфічні потреби українських міст в умовах воєнного стану (відключення світла та нестабільність інтернет-зв'язку);
- створення комплексних систем захисту інформації (КСЗІ) для хмарних проєктів «Безпечне місто»;
- практичні моделі інтеграції штучного інтелекту безпосередньо у хмарні потоки міського відеоспостереження.

Метою статті визначено актуалізацію потреби у застосуванні хмарних технологій при запровадженні проєктів «Безпечне місто» в розробці комплексних архітектурних рішень для забезпечення публічного порядку та безпеки критичної міської інфраструктури в Україні.

Виклад основного матеріалу дослідження. Цифровізація публічного сектору регулюється постановами, які заохочують використання хмарних послуг для державних органів з політикою дотримання надійних стандартів захисту даних. Хмарні технології виступають аналітичною базою для технологій штучного інтелекту, розпізнавання облич, номерних знаків авто та моніторингу трафіку в реальному часі.

В Україні впровадження хмарних сервісів у інфраструктуру міст базується, в основному, на концепції Cloud Smart – це комплексна стратегія ІТ, яка заохочує організації використовувати комбінацію публічних, приватних та гібридних хмар для оптимізації робочих навантажень. Вона є еволюцією підходу Cloud First, допомагаючи збалансувати безпеку, гнучкість, масштабованість та економічну ефективність. Концепція Cloud Smart розкриває підхід до хмарної архітектури, який передбачає:

- стратегічний перехід від простого перенесення всіх даних у хмарні сервери до цілеспрямованого вибору оптимального середовища для кожного конкретного додатка;

- допомогу незалежним розробникам оптимізувати процеси, інтегруватися та надавати рішення спільно з Amazon Web Services (найпопулярніша та найширша у світі хмарна платформа, яка надає понад 200 повнофункціональних сервісів із центрів обробки даних по всьому світу);

- пропозиція українських провайдерів захищених хмарних екосистем на базі Microsoft (наприклад, SMART Cloud).

Б. Ю. Жураковський, І. О. Зенів, В. В. Максимов, А. В. Мошинська оцінюють хмарну IoT-архітектуру за такими основними метриками:

1. Техніко-експлуатаційні показники. Оцінюється затримка передачі даних (latency) між кінцевими пристроями та хмарними технологіями, пропускна здатність каналів зв'язку, надійність (наприклад, доступність сервісів AWS IoT Core чи Azure IoT) та масштабованість мережі [1; 2].

2. Економічна доцільність. Застосовують математичне й економічне моделювання для розрахунку загальної вартості володіння TCO (Total Cost of Ownership) хмарною інфраструктурою. Це дає змогу порівняти фінансову ефективність різних провайдерів за критеріями часу, бюджету та функціональності.

3. Багатокритеріальний аналіз безпеки. Оцінюється ефективність рішень керування доступом у хмарних технологіях (наприклад, впровадження політики Zero Trust), стійкість IoT-шлюзів до кібератак та захищеність транскордонних потоків даних.

4. Енергоефективність та концепція AIoT. Аналізуються енергетичний та екологічний слід складних нейромережевих архітектур у хмарних технологіях, використовуючи метрики життєвого циклу енергії (eCAL)

Для реалізації хмарних проєктів «Безпечне місто» залучаються потужності провідних українських та міжнародних хмарних провайдерів (наприклад, UCloud, GigaCloud чи Датагруп), що гарантує відмовостійкість у разі аварій.

Український розробник програмного забезпечення та інтегрованих систем безпеки «INNI» спеціалізується на об'єднанні відеонагляду, систем контролю віддаленого доступу та облікових баз даних в єдину платформу. Рішення компанії дозволяють створити ситуаційний центр для автоматизації підприємства, контролю співробітників, запобігання шахрайству та інтегруються з різними платформами:

- INNI DATA / BUSINESS (програмні модулі для аналітики, розпізнавання (автономери, обличчя) та збору даних з різних джерел);

- промислова інтеграція, тобто синхронізація відеокамер з ваг-комплексами, сканерами штрих-кодів та обліковими системами на складах і в агропромисловому комплексі;

- ПЗ інтеграції, що дозволяє отримувати, обробляти та архівувати дані з унікальних систем замовника.

Комплексне впровадження, монтаж обладнання та налаштування ПЗ INNI здійснюють офіційні сертифіковані партнери: BEZPEKA-SHOP (наприклад, для придбання програмного модуля інтеграції INNI-DC-1S-01) та дистриб'ютор та інтегратор SEC GROUP.

Компанія «Датагруп» є провідним українським оператором зв'язку та системним інтегратором комплексних рішень з IT-безпеки та кіберзахисту для державного сектору. У 2024 році «Датагруп-Volia» об'єдналася з мобільним оператором lifecell у єдину групу компаній DVL, що значно розширило можливості інтеграції конвергентних рішень кібербезпеки на стику фіксованого та мобільного зв'язку. Таким чином, компанія «Датагруп» надає комплексні послуги, об'єднуючи інфраструктуру зв'язку із захисними технологіями від провідних світових розробників.

Сучасні моделі хмарних обчислень (Cloud Computing) класифікуються за двома основними напрямками: за моделлю обслуговування (який саме тип ресурсів надається) (табл. 1) та за моделлю розгортання (хто має доступ до інфраструктури) (табл. 2). Ця концепція, дозволяє отримувати повсюдний та зручний доступ на вимогу до спільного пулу обчислювальних ресурсів через мережу.

Моделі обслуговування, які визначають рівень контролю та відповідальності між користувачем і хмарним провайдером.

У публікаціях аналітиків ринку хмарних послуг, а саме компаній GigaCloud та UCloud, детально описано, що використання моделей IaaS, PaaS та SaaS для державного сектору дозволить українським містам:

- уникнути значних капітальних витрат на купівлю та обслуговування локальних дата-центрів;

- динамічно масштабувати обсяги сховищ під тисячі міських камер;

- забезпечувати високу швидкість обробки великих масивів даних за допомогою ETL-платформ (програмне забезпечення для збору, очищення, трансформації та завантаження даних із різнорідних джерел) та хмарних аналітичних інструментів (масштабованих платформ для збору, обробки, зберігання та візуалізації даних без прив'язки до локальних серверів) [15].

Таблиця 1

Види моделей обслуговування

№п/п	Моделі	Умови обслуговування	Приклади
1	IaaS (Infrastructure as a Service – Інфраструктура як послуга)	- Оренднуються базові ІТ-ресурси: чисті віртуальні сервери, дискові сховища та мережеві компоненти. - Операційна система, база даних та додатки встановлюються й налаштовуються користувачем.	Amazon EC2 (вебсервіс, який надає масштабовані обчислювальні потужності у хмарі), Google Compute Engine, сервіси українського оператора De Novo
2	PaaS (Platform as a Service – Платформа як послуга)	- Провайдер надає готову платформу з операційною системою, середовищем розробки та інструментами керування базами даних. - Клієнт фокусується лише на написанні та розгортанні свого програмного коду.	Heroku, Google App Engine, Microsoft Azure PaaS
3	SaaS (Software as a Service – Програмне забезпечення як послуга)	- Повністю готова модель, де користувач отримує доступ до кінцевого додатку через браузер або мобільний застосунок. - Усі технічні питання – від оновлень до безпеки інфраструктури – здійснює провайдер.	Google Документи, Microsoft 365, Dropbox (безпечне хмарне сховище для синхронізації, обміну файлами та спільної роботи)
4	XaaS (Anything as a Service – Все як послуга)	Сучасний збірний термін, що включає специфічні підвиди: Serverless (безсерверні обчислення), SECaaS (безпека як послуга), DaaS (робочий стіл як послуга)	

Джерело: розроблено авторами на основі власних досліджень

Моделі розгортання (Deployment Models) вказують на те, де фізично розташоване обладнання та хто має до нього доступ.

On-Premise (локальне розгортання) – це модель, за якою вся ІТ-інфраструктура (сервери, мережеве обладнання, системи зберігання) фізично розміщується в певному дата-центрі. Обслуговуванням і налаштуванням займаються на рівні представників міської влади.

Централізоване зберігання масивів даних (у тому числі персональних) камер на комерційних серверах підвищує вразливість хмарних технологій до ворожих кібератак, тому вимагає застосування передового шифрування

та суворого дотримання політик безпеки. Обробка державних ресурсів за допомогою хмарних технологій суворо регламентована. Провайдери повинні відповідати вимогам Закону України «Про хмарні послуги» та мати сертифіковані системи захисту [1]. Стабільна робота системи повністю залежить від безперервного доступу до каналів зв'язку (високошвидкісної мережі Інтернет-з'єднання). Незважаючи на ризики, представники державних та місцевих органів влади (зокрема, у містах Київ чи Запоріжжя) поступово зпроваджують потужні хмарні відеоплатформи задля ефективного розпізнавання облич та автономерів.

Таблиця 2

Види моделей розгортання

№п/п	Моделі	Сутність
1	Публічна хмара (Public Cloud)	- Інфраструктура належить сторонньому провайдеру і використовується багатьма державними структурами одночасно. - Забезпечує високу масштабованість та оплату лише за спожиті ресурси (Pay-as-you-go).
2	Приватна хмара (Private Cloud)	- Інфраструктура призначена виключно для однієї інституції. - Може розгортатися у власному дата-центрі або на орендованому виділеному обладнанні у провайдера (Dedicated Cloud).
3	Гібридна хмара (Hybrid Cloud)	- Поеднує публічні та приватні хмари за допомогою технологій передачі даних. - Дозволяє тримати критично важливі дані в безпечній приватній хмарі, а для пікових навантажень залучати потужності публічної.
4	Мультихмара (Multi-cloud)	- Передбачає одночасне використання сервісів від кількох незалежних публічних провайдерів (наприклад, AWS та Google Cloud одночасно). - Зменшує ризик залежності від одного постачальника (vendor lock-in) та підвищує відмовостійкість системи.

Джерело: розроблено авторами на основі власних досліджень

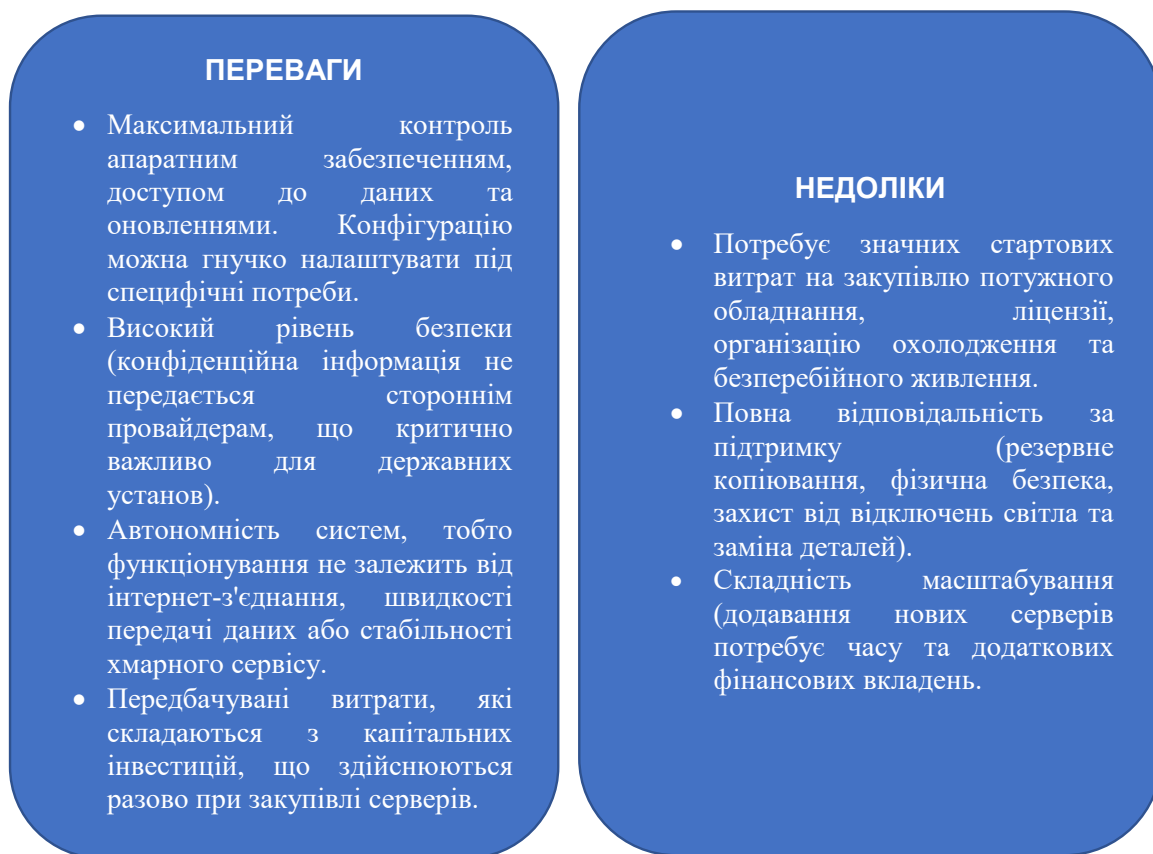


Рис. 1. Переваги та недоліки рішень локального розширення

Джерело: розроблено авторами на основі власних досліджень

Використання хмарних технологій у проєктах «Безпечне місто» в Україні забезпечує здатність системи продовжувати безперебійну роботу та зберігати функціональність навіть у разі виходу з ладу окремих компонентів, миттєве масштабування та гнучкість. Це дозволяє представникам місцевих органів влади обробляти дані з тисяч відеокamer та IoT-датчиків без масштабних інвестицій у будівництво власних локальних дата-центрів, що критично важливо в умовах воєнного стану. Закупівля хмарних обчислювальних потужностей вимагає місцевого бюджетного фінансування у резервні канали зв'язку. Проте, це компенсується відсутністю великих початкових витрат на власні сервери. У цьому випадку витрати переходять з капітальних інвестицій (на купівлю серверів) на операційні (оренда потужностей), що підвищує економічну ефективність функціонування українських міст. Нові аналітичні модулі (розпізнавання облич, номерних знаків, контроль трафіку) швидко розгортаються у хмарних технологіях за декілька днів. Навіть при пошкодженні фізичної інфраструктури в регіоні, дані зберігаються на віддалених захищених серверах. З метою забезпечення співпраці

служб наявний миттєвий доступ до інформації з єдиної платформи для представників Національної поліції України, Державної служби України з надзвичайних ситуацій та муніципальних інспекцій [9].

Стратегічними напрямками розвитку впровадження хмарних технологій в проєктах «Безпечне місто» в Україні мають стати використання хмарного штучного інтелекту для предиктивної аналітики (прогнозування правопорушень та управління трафіком) та перехід до єдиної національної платформи, яка б об'єднувала розрізнені регіональні проєкти в єдину мережу на державному рівні. Відсутність єдиних законодавчо регульованих стандартів для хмарних сервісів у муніципальному секторі ускладнює інтеграцію місцевих систем до Єдиної системи відеомоніторингу МВС України (мережа, що об'єднує десятки тисяч вуличних камер на автодорогах та у місцях скупчення людей по всій Україні з метою запобігання злочинам, пошуку зниклих осіб та безпека дорожнього руху). Таким чином, КМУ працює над створенням єдиного аналітичного інструменту для публічної безпеки, що об'єднує локальні міські системи [16–18].

Висновки. Запровадження хмарних технологій в рамках проєктів «Безпечне місто» в Україні дозволяє миттєво обробляти та надійно зберігати данні, необхідних для публічної безпеки та правопорядку.

Використання хмарних технологій забезпечує безперебійний доступ до систем відеоспостереження, аналітичних інструментів та швидке масштабування ресурсів без витрат на будівництво фізичних серверних.

Бібліографічний список

1. 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>
2. Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-IX. *База даних «Законодавство України»*. ВР України.
3. 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.
4. Блінов І. В., Кравченко Ю. В. Інтеграція хмарних рішень у муніципальні системи відеомоніторингу: безпекові аспекти. *Кібербезпека та інформаційні технології*. 2024. Т. 12, № 2. С. 45–54.
5. Григоровський В. В. Концепція “Smart City” як чинник сталого розвитку міських агломерацій в Україні. *Теорія та практика державного управління*. 2023. Вип. 3 (78). С. 112–120.
6. 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/>
7. Коваленко А. І., Шевченко В. В. Проблеми безпеки в хмарних технологіях при розгортанні критичної інфраструктури міст. *Інформаційні технології та кібербезпека*. 2025. № 15 (2). С. 45–53.
8. Лебедев О. П. Виклики та загрози кібербезпеки в умовах хмарних обчислень на муніципальному рівні. *Вісник Національної академії внутрішніх справ*. 2024. № 24 (1). С. 101–110.
9. Мартинюк О. М., Петренко С. В. Використання технологій великих даних (Big Data) та хмарних платформ у проєктах «Безпечне місто». *Сучасний захист інформації*. 2023. № 4. С. 18–26.
10. Мошинська А. В., Уривський Л. О. Декомпозиція процесів переходу від сценарію до стратегії передачі інформації у мультисервісній системі. Проблеми телекомунікацій : Дванадцята Міжнародна науково-технічна конференція, присвячена Дню науки і Всесвітньому Дню телекомунікацій (ПТ-18), 16–20 квітня 2018 р., Україна, Київ : збірник матеріалів. Київ, 2018. С. 30–32.
11. Радченко О. В. Цифрова трансформація місцевого самоврядування: від електронного врядування до розумного міста. *Публічне управління та адміністрування*. 2024. Вип. 2 (39). С. 87–93.
12. 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
13. Харченко Ю. С., Іванова І. М. Моделі забезпечення безпеки даних у хмарних середовищах інтегрованих систем спостереження. *Науковий вісник Київського університету права*. 2023. № 19 (4). С. 56–64.
14. Щерба М. О. Дослідження методів забезпечення інформаційної безпеки в хмарних обчисленнях. *Інформаційні системи та технології: матеріали наук.-практ. конф.* Харків : ХНУРЕ, 2023. С. 206–207. URL: <https://ice.nure.ua/>
15. Використання комерційних хмарних технологій для обробки даних: аналітичний звіт. Міжнародна фундація виборчих систем (IFES) в Україні, 2024. 64 с. URL: <https://www.ifesukraine.org/>
16. Єдина система відеомоніторингу стану публічної безпеки в Україні: офіційне роз’яснення МВС України. *Міністерство внутрішніх справ України*. 2024. URL: <https://mvs.gov.ua/>
17. Розумні міста України: Що таке смарт-сіті і як це працює. *Bezpeka Shop Blog*. 2022. URL: <https://www.bezpeka-shop.com/>
18. Smart city: розумні технології сучасного міста. *Kyivstar Hub*. 2021. URL: <https://hub.kyivstar.ua/>

References

1. Pro khmarni posluhy: Zakon Ukrainy vid 17.02.2022 r. № 2075-IX. [On cloud services: Law of Ukraine dated 02/17/2022 No. 2075-IX]. Vidomosti Verkhovnoi Rady Ukrainy. 2022. № 22. St. 149. Available at: <https://zakon.rada.gov.ua/go/2075-20>
2. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 01.12.2022 r. № 2807-IX [On the National Informatization Program: Law of Ukraine dated 12/01/2022 No. 2807-IX]. Baza danykh “Zakonodavstvo Ukrainy”. VR Ukrainy.
3. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII (zi zminamy ta dopovnenniamy). Baza danykh “Zakonodavstvo Ukrainy” [On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated 10/05/2017 No. 2163-VIII (as amended and supplemented). Database “Legislation of Ukraine”]. Verkhovna Rada of Ukraine.
4. Blinov I. V., Kravchenko Yu. V. (2024). Intehratsiia khmarnykh rishen u munitsypalni systemy videomonitorynhu: bezpekovi aspekty [Integration of cloud solutions into municipal video monitoring systems: security aspects]. *Kiberbezpeka ta informatsiini tekhnolohii*, vol. 12, no. 2, pp. 45–54.

5. Hryhorovsky V. V. (2023). Kontseptsiiia "Smart City" yak chynnyk staloho rozvytku miskykh ahlomeratsii v Ukraini [The concept of "Smart City" as a factor in the sustainable development of urban agglomerations in Ukraine]. *Teoriia ta praktyka derzhavnoho upravlinnia*, vol. 3 (78), pp. 112–120.
6. Dosenko A. K. (2022). Khmarni tekhnolohii: prykladni tekhnolohii suchasnykh platform [Cloud technologies: applied technologies of modern platforms]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Filolohiia. Zhurnalistyka*, vol. 33 (72), no. 1, pp. 248–253. Available at: <https://elibrary.kubg.edu.ua/42792/>
7. Kovalenko A. I., Shevchenko V. V. (2025). Problemy bezpeky v khmarnykh tekhnolohiiakh pry rozghortanni krytychnoi infrastruktury mist [Security problems in cloud technologies when deploying critical infrastructure of cities]. *Informatsiini tekhnolohii ta kiberbezpeka*, no. 15 (2), pp. 45–53.
8. Lebedev O. P. (2024). yklyky ta zahrozy kiberbezpeky v umovakh khmarnykh obchyslen na munitsypalnomu rivni [Challenges and Threats of Cybersecurity in Cloud Computing at the Municipal Level]. *Visnyk Natsionalnoi akademii vnutrishnikh sprav*, no. 24 (1), pp. 101–110.
9. Martyniuk O. M., Petrenko S. V. (2023). Vykorystannia tekhnolohii velykykh danykh (Big Data) ta khmarnykh platform u proiektakh "Bezpechne misto" [The Use of Big Data Technologies and Cloud Platforms in "Safe City" Projects]. *Suchasnyi zakhyst informatsii*, no. 4, pp. 18–26.
10. Moshynska A. V., Uryvskyi L. O. (2018) Dekompozysiiia protsesiv perekhodu vid stsenariiu do stratehii peredachi informatsii u multyservisnii systemi [Decomposition of the processes of transition from a scenario to an information transmission strategy in a multiservice system]. *Problemy telekomunikatsii : Dvanadtsiata Mizhnarodna naukovo-tekhnichna konferentsiia, prysviachena Dniu nauky i Vsesvitnomu Dniu telekomunikatsii (PT-18)*, April 16–20, 2018, Kyiv, Ukraine: Conference Proceedings. Kyiv, pp. 30–32
11. Radchenko O. V. (2024). Tsyfrova transformatsiia mistsevoho samovriaduvannia: vid elektronnoho vriaduvannia do rozumnoho mista [Digital Transformation of Local Self-Government: From E-Government to Smart City]. *Publichne upravlinnia ta administruvannia*, iss. 2 (39), pp. 87–93.
12. Tkachuk I. M. (2025). Teoretyko-pravova kharakterystyka vykorystannia khmarnykh posluh u derzhavnomu sektori Ukrainy [Theoretical and legal characteristics of the use of cloud services in the public sector of Ukraine]. *Yurydychnyi visnyk*, no. 1, pp. 134–141. Available at: https://yurvisnyk.in.ua/v1_2025/19.pdf
13. Kharchenko Yu. S., Ivanova I. M. (2023). Modeli zabezpechennia bezpeky danykh u khmarnykh seredovyshchakh intehrovanykh system sposterezhennia [Models of data security in cloud environments of integrated surveillance systems]. *Naukovyi visnyk Kyivskoho universytetu prava*, no. 19 (4), pp. 56–64.
14. Shcherba M. O. (2023). Doslidzhennia metodiv zabezpechennia informatsiinoi bezpeky v khmarnykh obchyslenniakh [Research on methods of ensuring information security in cloud computing]. *Informatsiini systemy ta tekhnolohii: materialy nauk.-prakt. konf.*. Kharkiv: KhNURE, pp. 206–207. Available at: <https://ice.nure.ua/>
15. Vykorystannia komertsiiynykh khmarnykh tekhnolohii dlia obrobky danykh: analitychnyi zvit [Using commercial cloud technologies for data processing: an analytical report]. Mizhnarodna fundatsiia vyborchykh system (IFES) v Ukraini, 2024. 64 p. Available at: <https://www.ifesukraine.org/>
16. Yedyna systema videomonitorynhu stanu publichnoi bezpeky v Ukraini: ofitsiine roziasnennia MVS Ukrainy [A unified system of video monitoring of the state of public security in Ukraine: official clarification of the Ministry of Internal Affairs of Ukraine]. Ministerstvo vnutrishnikh sprav Ukrainy, 2024. Available at: <https://mvs.gov.ua/>
17. Rozumni mista Ukrainy: Shcho take smart-siti i yak tse pratsiuie [Smart cities of Ukraine: What is a smart city and how does it work]. Bezpeka Shop Blog, 2022. Available at: <https://www.bezpeka-shop.com/>
18. Smart city: rozumni tekhnolohii suchasnoho mista [Smart city: smart technologies of a modern city]. Kyivstar Hub, 2021. Available at: <https://hub.kyivstar.ua/>

Anastasiia Nekriach

Doctor of Political Sciences, Professor,
Professor of the Department of International
Relations and Political Consulting,
Institute of Law and Public Relations
HEI "Open International University of Human Development "Ukraine"
ORCID: <https://orcid.org/0000-0001-5058-4145>

Vira Dabizha

Candidate of Science in Public Administration, Associate Professor,
Associate Professor of the Department of International
Relations and Political Consulting,
Institute of Law and Public Relations
HEI "Open International University of Human Development "Ukraine"
ORCID: <https://orcid.org/0000-0002-7000-4635>

USING CLOUD TECHNOLOGIES IN IMPLEMENTING SAFE CITY PROJECTS IN UKRAINE

The article examines the features and prospects of using cloud technologies in the implementation of Safe City projects in Ukraine as an important component of the digital transformation of public administration and public security systems. The relevance of the transition from traditional local IT infrastructure to modern cloud computing models is substantiated by the rapid growth of data generated by video surveillance systems and IoT devices, as well as the need for their efficient processing, storage, and use in public administration decision-making. The essence of the Cloud Smart concept is revealed as an integrated approach to the use of public, private, and hybrid cloud environments, which makes it possible to achieve an optimal balance between security, flexibility, scalability, and cost-effectiveness of digital infrastructure. The main cloud service models, including IaaS, PaaS, SaaS, and XaaS, as well as cloud deployment models, such as public, private, hybrid, and multi-cloud, are systematized. The key criteria for assessing the effectiveness of cloud-based IoT architecture are identified, including technical and operational performance, economic feasibility, cybersecurity, scalability, and energy efficiency. Particular attention is paid to the security risks associated with the centralized storage of data and the need to implement advanced encryption mechanisms, multi-factor authentication, and Zero Trust principles. It is established that the use of cloud technologies in Safe City projects contributes to increasing the resilience of digital infrastructure, enables rapid scaling of computing resources, and creates favorable conditions for the integration of artificial intelligence technologies. The strategic directions for further development include the use of cloud-based artificial intelligence for crime prediction and traffic management, as well as the establishment of a unified national video monitoring platform capable of integrating regional Safe City systems into a comprehensive nationwide public security network.

Keywords: public administration, state, security, safe city, infrastructure, security programs, cloud technologies.

Дата надходження статті: 05.07.2026

Дата прийняття статті до публікації: 29.07.2026

Дата публікації статті: 02.09.2026