МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Навчально-науковий інститут неперервної освіти
Кафедра публічного управління та адміністрування

ДОПУСТИТИ ДО ЗАХИСТУ
В.о.завідувача кафедри
Кожина Алла Василівна

_____

“__ __” _____ 2024р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ “МАГІСТР”
спеціальності 281 “Публічне управління та адміністрування” освітньо-професійної програми «Менеджмент в органах публічного управління»

Тема: “ЗАСТОСУВАННЯ SMART-ТЕХНОЛОГІЙ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ МІСТ-МЕГАПОЛІСІВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ”

Електронний підпис
Кумиков Ігор Вадимович
Ідентифікаційний код
3423415916
Підписано у Вчасно

Виконавець: студент групи М-281-23-1-МУ Кумиков Ігор Вадимович

Електронний підпис
ГЕЛИЧ АЛЛА ОЛЕКСАНДРІВНА
Ідентифікаційний код
2869021966
Підписано у Вчасно

Керівник: к.ю.н., доцент Гелич Алла Олександрівна

Нормоконтролер: _____ Гелич А. О.

Електронний підпис
Кожина Алла Василівна
Ідентифікаційний код
2686200868
Підписано у Вчасно

Київ 2024

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Навчально-науковий інститут неперервної освіти
Кафедра публічного управління та адміністрування
Спеціальність 281Публічне управління та адміністрування

ЗАТВЕРДЖУЮ:
В.о. завідувача кафедри
_____Алла КОЖИНА
«_____»_____2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи (проєкту)

Кумикова Ігоря Вадимовича

1. Тема кваліфікаційної роботи (проєкту): «ЗАСТОСУВАННЯ SMART-ТЕХНОЛОГІЙ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ МІСТ-МЕГАПОЛІСІВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ» затверджена наказом ректора від 15.10.2024 року № 2241/ст.

2. Термін виконання роботи (проєкту): з 15.10.2024 р. по 25.11.2024 р.

3. Вихідні дані по роботі (проєкту):

- Застосування Smart-технологій для посилення безпеки міст-мегаполісів.

- Аналіз використання Smart-технологій для посилення безпеки міст-мегаполісів в Україні.

- Перспективи удосконалення використання застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні.

4. Зміст пояснювальної записки: Здійснено оцінку наукових праць, інформаційних, аналітичних джерел та статистичних даних. Проведено дослідження застосування Smart-технологій для посилення безпеки міст-

мегаполісів. Проаналізовано використання Smart-технологій для посилення безпеки міст-мегаполісів в Україні.. Розглянуто перспективи удосконалення використання застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:- .

6. Календарний план-графік:

№ з/п	Графік виконання роботи	Строк виконання	Фактичне виконання
1.	Розроблення детального плану роботи	17.10.2024	17.10.2024
2.	Підготовка Розділу 1	27.10.2024	27.10.2024
3.	Підготовка Розділу 2	10.11.2024	10.11.2024
4.	Підготовка Розділу 3	18.11.2024	18.11.2024
5.	Підготовка Вступу, Висновків та Анотації	24.11.2024	24.11.2024
6.	Надання завершеної роботи науковому керівнику для перевірки	25.11.2024	25.11.2024

7. Дата видачі завдання: «15» жовтня 2024 р.

Керівник кваліфікаційної роботи (проєкту): _____ Гелич А.О.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання: Кумиков І.В.
(підпис здобувача вищої освіти) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні»: 84 с., 59 літературних джерел.

Об’єкт дослідження: міста-мегаполіси в умовах воєнного стану в Україні.

Мета роботи: теоретичне обґрунтування та розробка практичних рекомендацій щодо застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні.

Методи дослідження: проведення аналізу наукових праць, порівняльного аналізу, метод моделювання, прогнозування, узагальнення та систематизація.

Результати магістерської роботи рекомендується використовувати під час проведення наукових досліджень та в практичній діяльності фахівців з публічного управління та адміністрування.

SMART-ТЕХНОЛОГІЇ, БЕЗПЕКА, МЕГАПОЛІС, ВОЄННИЙ СТАН, ПОСИЛЕННЯ БЕЗПЕКИ.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність магістерської дипломної роботи на тему «Застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні» є надзвичайно високою через сучасні виклики, з якими стикається Україна, зокрема у контексті воєнних дій та гібридних загроз. Безпека громадян і критичної інфраструктури є ключовим аспектом у функціонуванні міст, особливо мегаполісів, які є стратегічно важливими об'єктами. Smart-технології пропонують інноваційні рішення для підвищення ефективності управління, моніторингу та реагування на надзвичайні ситуації.

У сучасних умовах війни, традиційні системи безпеки потребують адаптації та посилення через використання технологічних інструментів. Інтернет речей (IoT), великі дані (Big Data), штучний інтелект (AI) та відеоспостереження з елементами аналітики дозволяють оперативно виявляти загрози, координувати дії екстрених служб та попереджати громадян про можливі небезпеки. Це важливо як для захисту цивільного населення, так і для забезпечення функціонування критичної інфраструктури, включаючи транспортні мережі, енергопостачання та зв'язок.

Крім того, мегаполіси є основними центрами управління та концентрації населення, що робить їх потенційними цілями для атак як фізичного, так і кібератак. Застосування Smart-технологій у таких містах надає можливість покращити координацію між різними державними та муніципальними службами, забезпечуючи більш швидке та ефективне реагування на надзвичайні ситуації. Такі технології можуть використовуватися для виявлення підозрілих дій, моніторингу громадських місць, а також забезпечення кібербезпеки міської інфраструктури.

Окрім безпеки, використання Smart-технологій сприяє підвищенню рівня комунікації між владою та громадянами. Мобільні додатки та онлайн-платформи дозволяють мешканцям швидко повідомляти про проблеми або

загрози, а також отримувати інформацію про поточну ситуацію у місті. Це є особливо важливим в умовах воєнного стану, коли швидкість та точність передачі інформації можуть мати вирішальне значення для збереження життя та здоров'я громадян.

Таким чином, магістерська робота на тему застосування Smart-технологій для посилення безпеки міст в умовах воєнного стану має високу практичну значимість. Вона спрямована на розробку інноваційних підходів до забезпечення безпеки в умовах постійних викликів та загроз. Інтеграція сучасних технологій в управлінські процеси може значно підвищити рівень захисту населення та інфраструктури, а також сприяти швидшому відновленню міст після кризових ситуацій.

З огляду на досвід міст, що вже впроваджують Smart-технології для підвищення рівня безпеки, таких як Київ, де створено систему відеонагляду та моніторингу громадських місць з елементами штучного інтелекту, можна стверджувати, що подібні ініціативи є ефективними та мають велике значення для посилення безпеки. Такі рішення допомагають органам місцевого самоврядування оперативніше реагувати на загрози, координувати свої дії з екстреними службами та забезпечувати громадський порядок.

В умовах воєнного стану технологічний прогрес стає необхідністю для забезпечення стійкості міст до зовнішніх і внутрішніх загроз. Магістерська робота, присвячена цій темі, дозволяє досліджувати можливості інтеграції Smart-технологій у системи безпеки міст-мегаполісів, визначати перспективи та ризики, пов'язані з їх впровадженням, а також розробляти рекомендації для підвищення ефективності їх використання.

Таким чином, актуальність дослідження полягає у тому, що воно не тільки допомагає зрозуміти роль Smart-технологій у сучасному публічному управлінні, але й пропонує практичні рішення для захисту міст в умовах надзвичайних ситуацій та воєнного стану.

Мета і завдання кваліфікаційної магістерської роботи.

Мета роботи – теоретичне обґрунтування та розробка практичних рекомендацій щодо застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні.

Досягнення поставленої мети обумовлює необхідність вирішення таких *завдань*:

- Розкрити сутність Smart-технологій в контексті забезпечення громадської безпеки.
- Дослідити актуальні стратегії використання Smart-технологій у містах-мегаполісах світу.
- Проаналізувати правове регулювання застосування Smart-технологій у сфері безпеки.
- Провести порівняльний аналіз досвіду країн, що використовують Smart-рішення.
- Розробити рекомендації щодо інтеграції Smart-технологій у системи міського управління безпекою.
- Визначити перспективи подальшого розвитку Smart-технологій у контексті зміцнення національної безпеки.

Об'єкт кваліфікаційної магістерської роботи – міста-мегаполіси в умовах воєнного стану в Україні.

Предмет кваліфікаційної магістерської роботи – Smart-технології для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні.

Методи дослідження. У роботі для дослідження застосовані так загальнонаукові та специфічні методи наукового пізнання: аналіз, синтез, бібліографічний аналіз, моделювання (якісна модель, описова) та інші.

Наукова новизна одержаних результатів полягає у. науковому обґрунтуванні шляхів забезпечення єдності громадянського суспільства і політичної еліти в умовах воєнного стану та у воєнний період в Україні.

Практичне значення одержаних результатів полягає в тому, що напрацьовані пропозиції можуть бути використані органами виконавчої влади,

що розробляють та реалізують державну політику у впровадження Smart-технологій для посилення безпеки міст-мегаполісів.

Структура кваліфікаційної роботи. Робота складається з трьох розділів, вступу, висновків та списку використаних джерел, який налічує 59 позицій.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ SMART-ТЕХНОЛОГІЙ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ МІСТ-МЕГАПОЛІСІВ

1.1. Сутність Smart-технологій та їх характерні риси

«Smart-технології» — це комплекс сучасних інформаційно-комунікаційних технологій, що включають використання штучного інтелекту (AI), Інтернету речей (IoT), обробку великих даних (Big Data), а також автоматизацію процесів для підвищення ефективності управління [42, с. 36]. Вони спрямовані на забезпечення швидкого доступу до інформації, зниження витрат ресурсів, прозорість і підвищення якості надання послуг. У публічному управлінні це стосується різних сфер: від управління містами до автоматизації надання адміністративних послуг населенню.

Використання Smart-технологій дозволяє суттєво підвищити ефективність управління громадськими послугами, а також поліпшити умови життя громадян. Ці технології забезпечують інтеграцію різних інформаційних систем, що сприяє швидкій обробці даних та прийняттю рішень на основі реальних показників. Однією з головних переваг є можливість автоматизації рутинних процесів, що знижує кількість помилок і витрат часу на виконання завдань.

Як відзначає О. Бобровський, Smart-технології включають використання широкого спектру інструментів для поліпшення публічних послуг [10, с. 15]. Це включає, зокрема, електронне урядування, системи моніторингу стану інфраструктури та інші технологічні рішення, що дозволяють оптимізувати використання ресурсів.

В публічному управлінні Smart-технології виконують ряд ключових функцій, спрямованих на підвищення ефективності та якості публічних послуг. Одна з основних — це автоматизація процесів. Це дозволяє зменшити

людський фактор і прискорити надання послуг громадянам. Наприклад, через електронні платформи можна швидко отримувати адміністративні послуги без фізичної присутності.

Іншою важливою функцією є забезпечення прозорості управлінських процесів. Smart-технології надають можливість онлайн-моніторингу рішень, бюджету, проєктів і стану надання публічних послуг, що робить управлінську діяльність відкритою для громадян. Як зазначає Д. Перелі, прозорість допомагає підвищити довіру населення до органів влади і стимулює до активної участі громадян у прийнятті рішень [39, с. 142-143].

Третя функція Smart-технологій — це підвищення комунікації між громадянами та органами влади. Використання цифрових інструментів, таких як портали для обробки звернень, платформи для голосування або участі у прийнятті рішень, сприяє активній взаємодії громадян з владою. Це знижує бюрократичні бар'єри та сприяє швидшій реакції на запити громадян.

В Україні використання Smart-технологій стає дедалі актуальнішим, особливо у сфері міського управління. Розвиток концепції «Smart City» дозволяє ефективніше використовувати міські ресурси, зменшувати витрати на комунальні послуги, покращувати стан інфраструктури і надавати нові можливості для взаємодії влади з громадянами. На прикладі Києва та Львова, де вже впроваджуються різні цифрові платформи для надання публічних послуг, можна побачити суттєве зменшення часу обробки заявок та підвищення рівня комунікації між мешканцями та владою.

Також варто зазначити, що важливу роль відіграють цифрові платформи для управління даними та оптимізації надання послуг, такі як системи моніторингу комунального господарства, транспортні системи і системи енергозбереження. Наприклад, вітчизняні вчені відзначають, що впровадження Smart-систем для моніторингу споживання енергії в муніципальних установах дозволяє зменшити витрати на 10-20% [42, с. 36-37].

Попри всі переваги, впровадження Smart-технологій у публічне управління не є безпроблемним. Основний виклик полягає у фінансових

витратах, необхідних для розробки та підтримки цифрових систем. Багато територіальних громад не мають достатніх ресурсів для фінансування таких інноваційних рішень, що обмежує їхній доступ до технологічних досягнень.

Іншою проблемою є низька цифрова грамотність серед населення, особливо в сільських районах. Це створює труднощі з використанням цифрових інструментів для отримання публічних послуг. Також необхідність інтеграції великих масивів даних вимагає надійних механізмів кібербезпеки для захисту персональних даних громадян, що додає ще одну складність для органів управління.

Незважаючи на виклики, перспективи впровадження Smart-технологій у публічному управлінні є досить позитивними. Впровадження таких рішень дозволить знизити навантаження на державні органи, підвищити якість надання послуг, а також зробить процеси управління більш прозорими і доступними для громадян. Використання штучного інтелекту і автоматизації відкриває нові можливості для оптимізації процесів, а інтеграція електронних систем управління дозволить створити єдину базу даних, що значно прискорить обробку інформації.

Smart-технології також відіграють важливу роль у розвитку систем електронного урядування. Як зазначає Т. Шестаковська, впровадження систем e-government дозволяє значно скоротити терміни надання публічних послуг, а також сприяє взаємодії між різними органами влади, що підвищує ефективність управління [57, с. 10-11].

Smart-технології є важливою складовою сучасного публічного управління. Їх впровадження дозволяє оптимізувати процеси управління, підвищити якість надання послуг і зробити їх доступнішими для громадян. Попри виклики, пов'язані з фінансуванням і рівнем цифрової грамотності, розвиток Smart-технологій відкриває нові перспективи для підвищення ефективності управління в Україні.

Smart-технології є невід'ємною частиною сучасного управління, зокрема у контексті Smart City. Їх ключові характеристики — автономність, інтеграція,

масштабованість та адаптивність — дозволяють створювати ефективні системи управління, що здатні вирішувати складні міські проблеми.

Автономність — це здатність систем самостійно приймати рішення та діяти без людського втручання. Автономні системи використовують штучний інтелект для обробки великих масивів даних, що дозволяє здійснювати управління в реальному часі [25, с. 92-93]. Наприклад, автономні системи можуть керувати міським трафіком або забезпечувати роботу енергомереж, що значно підвищує ефективність використання ресурсів та знижує рівень людської помилки.

Інтеграція є важливою складовою Smart-технологій, оскільки вона передбачає об'єднання різних систем та платформ в єдину мережу, що полегшує управління ресурсами та процесами. Як відзначають експерти Центру Разумкова, нтеграція дозволяє зв'язувати між собою транспортну, енергетичну, комунальну та інші системи, що створює більш комплексний та взаємозалежний підхід до міського управління [32, с. 57-59]. Це сприяє ефективному обміну даними та оперативному вирішенню проблем, пов'язаних з ресурсами міста.

Ще однією важливою характеристикою є масштабованість, тобто здатність технологій до розширення або зменшення обсягів своїх функцій відповідно до потреб. Це дозволяє містам впроваджувати Smart-рішення поступово, не вимагаючи одномоментних великих капіталовкладень. Як відзначають вітчизняні науковці, масштабованість особливо важлива в умовах зростаючого навантаження на міську інфраструктуру та збільшення чисельності населення [41, с. 47-48]. Технології, здатні масштабуватися, дозволяють містам адаптуватися до зміни вимог та завдань, що стоять перед ними.

Нарешті, адаптивність є ще однією характеристикою Smart-технологій, яка полягає в їх здатності адаптуватися до змін у зовнішньому середовищі. Як наголошують науковці, адаптивні технології дозволяють міським системам гнучко реагувати на зміни, такі як погодні умови, зміна поведінки громадян або

надзвичайні ситуації [17, с. 295-296]. Наприклад, адаптивні системи можуть автоматично змінювати режими роботи вуличного освітлення в залежності від рівня освітленості або змінювати маршрути транспорту у випадку заторів.

Важливою умовою успішного впровадження Smart-технологій є не тільки їх технічні характеристики, але й готовність міських органів до їх інтеграції у системи управління [28, с. 12-14]. Використання цих технологій вимагає також розуміння принципів їх роботи та навчання персоналу.

Таким чином, ключові характеристики Smart-технологій, такі як автономність, інтеграція, масштабованість та адаптивність, дозволяють містам стати більш ефективними, стійкими та безпечними. Ці технології забезпечують не тільки підвищення якості життя громадян, але й значну оптимізацію процесів управління міською інфраструктурою, що є критично важливим в умовах сучасного світу.

Концепція «Smart City» базується на застосуванні технологій для ефективного управління міськими ресурсами та покращення якості життя. Основні риси включають інтеграцію Інтернету речей (IoT), аналіз великих даних (Big Data), штучний інтелект (AI) та хмарні технології [25, с. 92-93]. Це дозволяє забезпечити автоматизоване управління інфраструктурою.

Однією з важливих характеристик Smart City є інтелектуальні мережі [34, с. 149-150]. Це інтегровані системи, що об’єднують різні міські підсистеми — від транспорту до енергетики. Системи збирають дані в режимі реального часу для підвищення ефективності, наприклад, інтелектуальне управління трафіком зменшує затори.

Іншим ключовим елементом **є** Інтернет речей (IoT)**,** що дозволяє сенсорам моніторити екологічні показники, рівень води та забезпечувати безпеку в містах [41, с. 47-49]. Це значно покращує координацію міських процесів.

Застосування штучного інтелекту (AI) допомагає автоматизувати управління міськими службами та процеси прийняття рішень [25, с. 91-92]. AI аналізує великі обсяги даних для передбачення ризиків та їх попередження. Це робить міське управління більш передбачуваним і безпечним.

Як зазначають дослідники, важливим аспектом є прозорість і відкритість даних для громадян [34, с. 149-150]. Відкриті дані та електронні платформи дозволяють громадянам брати активну участь в управлінні містом. Такі платформи надають доступ до різних публічних послуг, зменшуючи бюрократію та покращуючи зручність.

Ще однією важливою рисою Smart City є екологічність [17, с. 295-296]. Використання смарт-технологій дозволяє оптимізувати споживання ресурсів та знижувати негативний вплив на довкілля. Наприклад, застосування розумних систем енергозбереження скорочує використання електроенергії, допомагає переходити на відновлювані джерела енергії.

Крім того, урбаністичне планування має велике значення для успішної реалізації Smart City. Впровадження нових технологій сприяє розвитку інфраструктури, що дозволяє містам бути більш сталими та зручними для життя [17, с. 296-297].

Безпека є ще однією сферою, де смарт-технології можуть відігравати ключову роль [41, с. 47-48]. Інтелектуальні системи відеоспостереження та попередження злочинів використовують штучний інтелект та великі дані для аналізу та передбачення потенційних загроз, що дозволяє оперативно реагувати на виклики.

Як зазначають вітчизняні науковці, важливим фактором успішного впровадження Smart City є співпраця між владою, бізнесом та громадянами [25, с. 92-93]. Це забезпечує стійке управління ресурсами та покращує рівень комунікації між різними сторонами. Також це сприяє кращій координації та залученню громадян до прийняття рішень.

Таким чином, впровадження смарт-технологій дозволяє містам стати більш ефективними, екологічними та безпечними. Smart-технології не тільки покращують якість життя громадян, але й створюють нові можливості для сталого розвитку міст та підвищення безпеки.

1.2. Особливості застосування Smart-технологій в сучасних умовах глобалізованого світу

Smart-технології активно використовуються в публічному управлінні для покращення якості управлінських рішень і оптимізації процесів. Їх ключова роль полягає у створенні «розумних» систем, що дозволяють підвищити ефективність та прозорість функціонування державних органів.

Однією з найважливіших особливостей застосування Smart-технологій в публічному управлінні є штучний інтелект. Використання ШІ дозволяє автоматизувати багато аспектів управлінських процесів, таких як обробка великих масивів даних, прогнозування розвитку подій та моделювання сценаріїв [28, с. 27-29]. Це не лише підвищує точність ухвалених рішень, але й забезпечує ефективніше реагування на виклики, з якими стикаються державні органи, особливо в умовах кризових ситуацій.

Другою важливою характеристикою Smart-технологій є цифровізація адміністративних послуг**.** Завдяки впровадженню електронних платформ громадяни отримують можливість взаємодіяти з органами влади швидше та зручніше. Як відзначають науковці, створення електронних урядів та порталів для надання публічних послуг сприяє значному спрощенню адміністративних процедур, зменшенню рівня корупції та підвищенню прозорості у державному секторі [29, с. 180-181].

Інтеграція технологій в систему управління є ще однією важливою особливістю застосування Smart-технологій. Системи «розумного міста» дозволяють інтегрувати різноманітні аспекти міської інфраструктури — від управління транспортом до моніторингу екологічного стану. Це сприяє підвищенню загальної ефективності міського управління та дає можливість оперативно реагувати на зміни в міському середовищі. Як зазначають вітчизняні вчені, інтелектуальні системи на базі датчиків та сенсорів дозволяють збирати дані в реальному часі та аналізувати їх для прийняття управлінських рішень [33, с. 11-12].

Ще одним важливим аспектом є адаптивність і гнучкість Smart-технологій**.** Ці технології здатні підлаштовуватися під зміни в оточуючому середовищі, що робить їх особливо ефективними для використання в умовах невизначеності та швидкої зміни ситуацій. Наприклад, під час пандемії COVID-19 багато міст застосовували Smart-рішення для контролю дотримання карантинних обмежень та моніторингу стану здоров'я громадян через спеціальні мобільні додатки та датчики. Вітчизняні вчені зазначають, що така адаптивність технологій дозволяє органам влади гнучко реагувати на нові виклики та забезпечувати стабільну роботу інфраструктури навіть у кризових умовах [40, с. 140-141].

Однією з важливих рис впровадження Smart-технологій в публічне управління є зменшення навантаження на державний апарат. Використання автоматизованих систем дозволяє скоротити кількість паперових процесів, що у свою чергу знижує витрати на адміністрування та підвищує ефективність державних органів. Дослідники відзначають, що Smart-технології сприяють тому, що державні структури можуть виконувати більше завдань з меншою кількістю ресурсів, що є важливим в умовах обмеженого бюджету [42, с. 39-40].

Важливо також зазначити, що впровадження Smart-технологій потребує налагодження співпраці між різними рівнями влади та приватним сектором. Для створення ефективних розумних міст необхідна взаємодія як між державними структурами, так і з бізнесом та науковими установами, що займаються розробкою технологій. Відсутність цієї співпраці може призвести до затримок у впровадженні технологій або їх неефективного використання.

Таким чином, Smart-технології відіграють ключову роль у трансформації публічного управління, забезпечуючи підвищення ефективності, прозорості та гнучкості в державному секторі. Використання таких технологій стає важливою складовою сучасної системи управління, що дозволяє не лише поліпшити якість життя громадян, але й забезпечити стійкий розвиток міст та громад.

Водночас, сучасна глобалізація відкриває нові можливості для впровадження Smart-рішень, але водночас породжує численні виклики та

ризики. Smart-технології мають потенціал для трансформації публічного управління, підвищення ефективності, прозорості, та якості послуг, однак їх застосування стикається з кількома значущими проблемами:

1. Ризик кіберзагроз та безпеки даних. Одним із найважливіших викликів є загроза кібербезпеці та захисту даних. У світі, де цифрові системи все більше інтегруються в публічне управління, питання безпеки персональних даних набуває критичного значення. Smart-системи можуть бути вразливими до кібератак, що ставить під загрозу як дані громадян, так і національну безпеку. Як зазначають Н. Максімцева та М. Максімцев, у разі втручання в систему ШІ, що керує процесами публічного управління, можна легко маніпулювати управлінськими процесами або навіть дестабілізувати їх [28, с. 25-26].

2. Проблеми технологічної нерівності. Ще однією загрозою є технологічна нерівність між регіонами. Багато міст та регіонів, особливо в країнах, що розвиваються, не мають достатніх ресурсів для впровадження Smart-рішень. Це призводить до цифрового розриву між мегаполісами, де впроваджуються передові технології, та менш розвиненими регіонами. Як зазначає О. Малюков, така нерівність може призвести до збільшення соціальної напруженості та дискримінації, оскільки частина населення може залишатися відрізаною від сучасних можливостей і доступу до публічних послуг [29, с. 182-183].

3. Виклики щодо адаптації законодавства. Застосування новітніх технологій потребує адаптації законодавчої бази. Технологічний розвиток відбувається набагато швидше, ніж оновлюються регуляторні рамки. Це створює правову невизначеність, що може стати перешкодою для впровадження інноваційних Smart-рішень. У багатьох випадках, як зазначає Д. Перелі, законодавство відстає від технологічних інновацій, що ускладнює забезпечення правового регулювання діяльності в цифровому середовищі [40, с. 137-138].

4. Фінансові ризики та інвестиційна привабливість. Інший виклик пов'язаний з фінансуванням проектів Smart-технологій. Їх впровадження

потребує значних інвестицій як на етапі розробки, так і на етапі реалізації. Багато міст стикаються з проблемами фінансових обмежень, що робить неможливим реалізацію повномасштабних проектів. Крім того, проекти можуть не відповідати очікуванням інвесторів щодо окупності. Як зазначають такі дослідники, як М. Попов, І. Комаровський, В.Яценко, економічна доцільність і довгострокова стабільність проектів залежать від правильної стратегії їх реалізації та залучення приватного капіталу [40, с. 36-37].

5. Технологічна залежність та вплив глобальних компаній. Важливий виклик для багатьох країн, зокрема й України, полягає в технологічній залежності від глобальних корпорацій, які контролюють ринок Smart-технологій. Впровадження інновацій часто пов'язане із співпрацею з такими гігантами як Google, Microsoft, Amazon, що створює залежність від їхніх платформ та продуктів. Як зазначає Т. Шестаковська, така залежність може обмежити можливості національного розвитку в галузі технологій та призвести до втрати контролю над ключовими інфраструктурними рішеннями [57, с. 10-11].

6. Етичні проблеми та питання конфіденційності. Впровадження технологій, таких як штучний інтелект, ставить під загрозу конфіденційність даних громадян та порушує питання етики. Smart-системи здатні збирати великі обсяги інформації про поведінку, звички та пересування громадян. Це викликає занепокоєння щодо неправомірного використання цих даних та порушення прав людини. Українські вчені підкреслюють, що існує загроза використання технологій для маніпуляцій та контролю за громадянами без їхнього відома [28, с. 29-30].

7. Екологічні ризики. Впровадження Smart-рішень також має певні екологічні виклики. Хоча мета технологій полягає у зменшенні споживання ресурсів і підвищенні екологічної стійкості, сам процес їх реалізації потребує великих ресурсів. Інфраструктура для функціонування Smart-технологій включає в себе мережі датчиків, сервісні центри та інші елементи, що вимагають значного споживання енергії. Крім того, впровадження нових

технологій породжує проблему утилізації старих електронних компонентів, що створює екологічне навантаження на довкілля.

8. Культурні та соціальні бар'єри. Один з останніх, але не менш важливих викликів – це соціально-культурні бар'єри на шляху впровадження новітніх рішень. Люди можуть бути не готові або навіть вороже ставитися до впровадження технологій, що змінюють звичні процеси та соціальну взаємодію. Це може створювати опір з боку певних верств населення або ж викликати проблеми у комунікації між владою та громадянами.

Таким чином, впровадження Smart-технологій у сучасних умовах глобалізації, хоча й несе великий потенціал для розвитку суспільства, стикається з низкою викликів. Вирішення цих проблем вимагає узгоджених зусиль на національному та міжнародному рівнях, а також уваги до питань безпеки, етики та соціальної рівності.

1.3. Теоретичні засади посилення безпеки міст-мегаполісів

Міста-мегаполіси стикаються з унікальними викликами в питаннях безпеки через високу щільність населення, інтенсивну урбанізацію та розвиток технологій. Сучасна концепція безпеки охоплює три основні виміри: фізичну, кібернетичну та соціальну безпеку.

Фізична безпека передбачає захист громадян та інфраструктури від загроз, пов’язаних із злочинністю, тероризмом, техногенними та природними катастрофами. Основні заходи з фізичної безпеки включають створення надійних правоохоронних органів, розвиток відеоспостереження, контролю доступу та інших інструментів запобігання небезпекам. У мегаполісах ці заходи зосереджуються не лише на зменшенні злочинності, а й на зниженні ризиків катастроф, як-от повені або пожежі. Як зазначає Ю. Романовська, використання Smart-технологій, таких як відеокамери з системами розпізнавання обличь або аналітичне програмне забезпечення для моніторингу публічних місць, стало невід'ємною частиною забезпечення безпеки великих міст [45, с. 84-85].

Кібербезпека стає одним із ключових аспектів міської безпеки у зв’язку з постійним ростом цифрових технологій. Сучасні міста активно використовують технології для керування транспортними системами, енергопостачанням, водопостачанням та іншими критичними інфраструктурами. Це створює нові вразливості, адже кібератаки на такі системи можуть призвести до серйозних наслідків. Кібербезпека міст включає захист систем управління, збереження персональних даних громадян та моніторинг кіберзагроз. Як підкреслює низка українських вчених, таких як А. Шлапак, Іващенко О., Никонюк К., розвиток кіберзагроз вимагає посилення заходів кібернетичної безпеки, які б охоплювали як технічний, так і організаційний рівні захисту міської інфраструктури [58, с. 4-5].

Соціальна безпека передбачає забезпечення сталого соціального порядку, запобігання конфліктам та забезпечення довіри громадян до органів влади. Цей аспект є особливо важливим у великих містах, де соціальна нерівність та різноманітність населення можуть спричиняти соціальні напруження. Як зазначає Д. Балашова, безпека у мегаполісах є комплексним явищем, яке залежить не лише від інфраструктурних рішень, але й від соціальної згуртованості та участі громадян у міському житті [9]. Наприклад, наявність публічних просторів та програм інтеграції мігрантів може сприяти зменшенню соціальної напруги.

Також забезпечення безпеки в мегаполісах вимагає інтеграції фізичних, кібернетичних та соціальних аспектів. У сучасних умовах глобалізації та цифровізації ці три компоненти безпеки дедалі більше взаємопов'язані. Наприклад, фізична безпека може бути підтримана через використання кіберінструментів, таких як системи моніторингу та прогнозування злочинності, а соціальна безпека може покращуватися через застосування цифрових платформ для зв’язку між громадянами та владою. Як зазначає Платформа розвитку міст, важливим є також інтеграція безпекових стратегій у загальну стратегію розвитку міста, що охоплює не лише технологічні аспекти, але й соціальні ініціативи [1].

Сучасні міста все частіше звертаються до Smart-технологій для покращення безпеки. Ці технології дозволяють зібрати та аналізувати великі обсяги даних про місто та його мешканців, що допомагає прогнозувати ризики та швидко реагувати на загрози. Наприклад, інтелектуальні системи моніторингу можуть виявляти незвичну активність на вулицях і сповіщати правоохоронців про можливі загрози. Водночас кіберсистеми дозволяють захищати міську інфраструктуру від атак, забезпечуючи стабільне функціонування критично важливих служб. Як зазначає М. Карповець, такі системи не лише підвищують рівень безпеки, але й забезпечують економічну ефективність управління безпекою міста [22, с. 127-128]/

Отже, структура безпеки мегаполісів охоплює три ключові компоненти – фізичну, кібернетичну та соціальну безпеку, кожен з яких є взаємопов'язаним і потребує інтеграції у загальну стратегію розвитку міста. Інноваційні технології, зокрема Smart-рішення, стають важливим інструментом для досягнення цієї мети.

В умовах воєнного стану та сучасних конфліктів мегаполіси стають особливо вразливими до різних загроз. Розглянемо ключові небезпеки, з якими стикаються сучасні міста:

1. Фізичні загрози. Однією з найбільших загроз є фізичні атаки, зокрема ракетні удари, терористичні акти, бомбардування або інші форми насильства, спрямовані на важливі об'єкти інфраструктури, наприклад, енергетичні станції, мости, аеропорти. Ці атаки не лише завдають значних руйнувань інфраструктурі, але й створюють паніку серед населення, що ускладнює процеси евакуації та надання допомоги. Як зазначає Ю Романовська, міста в умовах воєнного стану потребують ефективної системи захисту, яка включає укриття, зони для евакуації, а також надійні комунікаційні канали для оповіщення населення про загрозу [45, с. 85-86].

2. Кіберзагрози**.** Зростаюча залежність мегаполісів від інформаційних технологій робить їх вразливими до кібернетичних атак, особливо в умовах воєнного стану. Злочинці можуть використовувати кібератаки для дестабілізації

функціонування міської інфраструктури, наприклад, зламати системи управління енергетикою, водопостачанням або транспортом. Це призводить до зупинки критично важливих служб, що збільшує паніку серед населення та створює хаос. Вітчизняні вчені підкреслюють, що кібербезпека є одним із ключових елементів сучасної безпеки міст, адже втрата контролю над системами може мати катастрофічні наслідки [58, с. 4].

3. Соціальні конфлікти та зростання злочинності. В умовах воєнного стану або конфліктів соціальна стабільність мегаполісів опиняється під загрозою через зростання соціальної напруги, економічну нестабільність та збільшення рівня злочинності. Групи населення, які залишилися без роботи або домівок, можуть спричиняти зростання випадків насильства, пограбувань, мародерства. Це підсилюється відсутністю доступу до основних послуг, таких як охорона здоров'я, продовольство або безпека. Важливо, щоб у таких умовах влада мала можливість реагувати на загрози, впроваджуючи ефективні стратегії для збереження соціального порядку [9].

4. Техногенні та природні катастрофи. Крім загроз, пов'язаних із конфліктами, мегаполіси також вразливі до техногенних катастроф, таких як аварії на промислових підприємствах, витоки хімічних речовин, а також природні катастрофи, як-от землетруси або повені. У випадку війни інфраструктура, що відповідає за запобігання або реагування на такі катастрофи, може бути зруйнованою, що значно збільшує ризик великих втрат серед населення. Згідно з поглядами експертів, мегаполіси повинні мати плани екстреного реагування на такі події, зокрема задіюючи резерви та мобільні групи для швидкої ліквідації наслідків [1].

5. Міграційні потоки та перенаселеність. Під час воєнних дій значна частина населення може переміщатися до мегаполісів, шукаючи захисту або гуманітарної допомоги. Це спричиняє перенаселеність міст, яка веде до додаткового тиску на ресурси, інфраструктуру та системи забезпечення. Зростання міграційних потоків може також створювати нові соціальні конфлікти, оскільки ресурси обмежені, а влада не завжди встигає належним

чином організувати процеси адаптації переселенців. Як зазначає М. Карповець, важливим аспектом у таких умовах є забезпечення рівного доступу до ресурсів та послуг для всіх груп населення [22, с. 165-166].

6. Політична та економічна нестабільність. В умовах воєнного стану економіка міст зазнає значних потрясінь. Це може виражатися у вигляді зростання безробіття, зупинки бізнесу, інфляції, а також браку інвестицій. Політична нестабільність також впливає на здатність міської влади ухвалювати рішення та ефективно координувати заходи з безпеки. У Національному інституті стратегічних досліджень наголошують на тому, що для зменшення впливу цих факторів необхідно зміцнювати інституційні можливості влади та створювати резерви, які можуть використовуватися в критичні моменти [4, с. 14-15].

Отже, безпека мегаполісів у сучасних умовах залежить від здатності ефективно протистояти фізичним, кібернетичним та соціальним загрозам, що виникають під час воєнних дій.

У сучасних умовах урбанізації й зростання загроз для міського населення, використання Smart-технологій набуває ключового значення в забезпеченні безпеки міст. Вони дозволяють втілювати як превентивні, так і реактивні заходи для зменшення ризиків і підвищення захищеності міських систем.

Превентивні заходи у безпеці міста спрямовані на запобігання загрозам до того, як вони реалізуються. Smart-технології допомагають інтегрувати такі заходи у всі сфери міського управління. Наприклад, впровадження систем моніторингу, таких як відеонагляд, здатних відстежувати підозрілу активність у режимі реального часу, є важливою частиною превентивних рішень. Дані з цих систем автоматично аналізуються штучним інтелектом для виявлення аномалій та інформування відповідних служб безпеки.

Smart City-підходи включають у себе й створення передових мереж сенсорів, що дозволяють стежити за якістю повітря, трафіком і станом інфраструктури. Як відзначають у Центрі Разумкова, ці рішення допомагають

швидко реагувати на небезпечні зміни, тим самим попереджаючи загрози для населення [32, с. 245].

Коли загрози вже реалізовані, наприклад, під час стихійних лих, терористичних атак або соціальних заворушень, роль Smart-технологій полягає в прискореній реакції на ці події. Завдяки інтеграції міських систем із комунікаційними технологіями, влада може швидко реагувати на надзвичайні ситуації, координуючи ресурси й приймаючи рішення в режимі реального часу. Важливу роль тут відіграють системи управління кризовими ситуаціями, що забезпечують миттєве повідомлення жителів міста про загрози й шляхи їх уникнення [2].

Основною рисою Smart-технологій є їх інтеграція у всі аспекти міського життя. Це стосується як побутових рішень, що підвищують комфорт жителів, так і складних систем управління міськими ресурсами. Наприклад, транспортні системи Smart Cities дозволяють не тільки керувати потоком трафіку, але й реагувати на аварії або інші інциденти, спрямовуючи ресурси для їх вирішення. Як зазначають українські науковці, інтеграція штучного інтелекту та аналітики великих даних допомагає передбачати загрози й ефективно їх нейтралізувати [23, с. 52-53].

У концепції Smart City важливим є створення єдиної інформаційної платформи, що збирає дані з різних джерел, таких як системи моніторингу, соціальні мережі та погодні прогнози. Це дозволяє органам влади мати повну картину ситуації у місті та швидко реагувати на зміни. Така інтеграція є ключовою для забезпечення ефективного управління безпекою міста [23, с. 53-54].

Незважаючи на значні переваги, впровадження Smart-технологій також пов'язане з певними викликами. По-перше, це висока вартість впровадження таких технологій, що потребує значних інвестицій з боку міської влади. По-друге, для ефективного функціонування Smart-рішень необхідна висока кваліфікація персоналу, який буде обслуговувати ці системи. Також варто враховувати можливість кіберзагроз, адже централізація даних та інтеграція

систем можуть стати об'єктами атак хакерів. Це підтверджується в дослідженні Центру Разумкова, де наголошується на важливості захисту інформаційних систем міста [32, с. 301-302].

Крім того, важливою проблемою є недосконаліть законодавчої бази, яка не завжди відповідає сучасним вимогам для впровадження таких рішень. Це створює правові вакууми, які можуть призвести до затримки у впровадженні Smart City рішень.

З кожним роком технології Smart City стають все більш доступними та необхідними для сучасних мегаполісів. Вони здатні підвищити якість життя мешканців, забезпечуючи безпечні умови для проживання, роботи та відпочинку. Розвиток штучного інтелекту та інтернету речей (IoT) дозволить ще більш точно передбачати й запобігати загрозам, роблячи міста стійкими до різних кризових ситуацій. Нові технології дозволять містам бути більш автономними та адаптивними до нових викликів [2].

Таким чином, Smart-технології відіграють важливу роль у забезпеченні безпеки міст, дозволяючи не тільки ефективно реагувати на загрози, але й запобігати їм. Розвиток таких рішень є невід'ємною частиною сучасної урбанізації, що дозволяє підвищувати якість життя та забезпечувати стабільність міських систем у періоди кризи.

Висновки до розділу 1

Smart-технології є важливою складовою концепції сучасних мегаполісів, які прагнуть забезпечити безпеку своїх громадян. Їхнє застосування дозволяє підвищувати ефективність управління міськими системами через інтеграцію інтелектуальних рішень. Розробка й використання таких технологій знижують загрози, пов'язані з урбанізацією, завдяки можливості моніторингу й оперативної реакції на кризові ситуації. Водночас, глобалізаційні процеси накладають нові виклики для безпеки міст, що вимагає адаптивних

технологічних рішень. Концепція безпеки міст повинна враховувати всі основні компоненти – фізичну, соціальну й кібербезпеку.

Smart-технології мають кілька характерних рис, що роблять їх унікальними для застосування в умовах сучасного мегаполісу. В першу чергу, це їхня здатність до автономної роботи завдяки використанню штучного інтелекту та великих даних. Smart-технології інтегрують численні інформаційні потоки, що дозволяє оперативно відстежувати події в місті. Важливою рисою є масштабованість цих технологій, що дозволяє адаптувати їх під потреби різних міст. Вони також мають високу адаптивність, що дозволяє оперативно реагувати на зміни в умовах глобалізованого світу, покращуючи управління міськими процесами й підвищуючи безпеку.

У контексті глобалізації, роль Smart-технологій полягає не тільки в локальному забезпеченні безпеки, але й у створенні взаємопов'язаних інфраструктур, здатних реагувати на глобальні загрози. Це включає в себе кібербезпеку, управління транспортом, контроль за екологічними ризиками та моніторинг соціальних загроз. Глобальні виклики вимагають тісної інтеграції Smart-технологій на рівні міст, країн і навіть міжнародних мереж. Використання таких технологій дозволяє підвищити рівень адаптивності міст і зменшити залежність від традиційних ресурсів управління. Крім того, глобальні тенденції до зростання населення мегаполісів вимагають впровадження інноваційних рішень для уникнення соціальних і екологічних криз.

Посилення безпеки міст-мегаполісів вимагає інтегрованого підходу, що включає фізичну, кібернетичну та соціальну безпеку. Smart-технології стають інструментом, який дозволяє інтегрувати всі ці елементи в єдину систему, що працює в режимі реального часу. Це дозволяє знизити ризики терористичних атак, соціальних заворушень або техногенних катастроф. Основні підходи до підвищення безпеки базуються на системному аналізі ризиків та їхньому попередженні за допомогою інтелектуальних систем моніторингу. Крім того, важливою складовою є кібербезпека, яка забезпечує захист від атак на критичну

інфраструктуру, що є особливо актуальним в умовах глобалізації та цифровізації.

Smart-технології відіграють ключову роль у сучасному публічному управлінні безпекою мегаполісів, забезпечуючи інноваційні рішення для різних аспектів міського життя. Їхня інтеграція дозволяє створювати ефективні інструменти для моніторингу, аналізу та управління ризиками, пов'язаними з урбанізацією, тероризмом, екологічними та кіберзагрозами. Впровадження цих технологій сприяє не лише підвищенню рівня безпеки, але й оптимізації використання міських ресурсів, що відповідає сучасним тенденціям розвитку «розумних міст».

РОЗДІЛ 2 РОЗБУДОВА ВИКОРИСТАННЯ SMART-ТЕХНОЛОГІЙ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ МІСТ-МЕГАПОЛІСІВ В УКРАЇНІ

2.1. Сучасний стан та динаміка використання Smart-технологій для посилення безпеки міст-мегаполісів в Україні

Впровадження Smart-рішень у великих містах України є важливим напрямом розвитку для підвищення ефективності міського управління, безпеки та якості життя населення. Українські міста активно переймають світовий досвід у використанні цифрових технологій для вирішення питань інфраструктури, безпеки, транспорту, екології та управління ресурсами. Одним із ключових аспектів впровадження таких рішень є концепція «розумного міста», що передбачає інтеграцію інформаційно-комунікаційних технологій (ІКТ) у всі сфери міського життя.

Як зазначають вітчизняні дослідники, впровадження Smart-технологій у містах, таких як Київ, Харків та Львів, сприяє підвищенню ефективності муніципальних послуг [38, с. 93-94]. Особлива увага приділяється безпеці, де запроваджуються системи відеоспостереження, аналізу даних та автоматизованого управління транспортом. Крім того, впровадження цифрових сервісів дозволяє зменшити витрати та підвищити прозорість в управлінні міськими ресурсами.

Одним із прикладів успішного застосування Smart-рішень є використання системи «Kyiv Smart City», яка об'єднує платформи для громадського транспорту, паркування, моніторингу екології та безпеки громадян. Як зазначає О. Кривоніс, ця платформа забезпечує ефективний контроль за інфраструктурою міста та знижує ризики, пов'язані з аваріями чи злочинами інтегрує електронні послуги для зручності громадян, що дозволяє покращити взаємодію між населенням та владою [26].

У Харкові також активно розвиваються Smart-технології, спрямовані на підвищення безпеки та екологічної стійкості. Відповідно до досліджень українських науковців, місто впровадило системи відеомоніторингу, управління дорожнім рухом та енергетичними ресурсами [7, с. 102-103]. Особливо важливою є роль таких технологій під час надзвичайних ситуацій або кризових умов, що дозволяє забезпечити швидку реакцію служб на загрози.

Одним із важливих аспектів є адаптація Smart-рішень до умов воєнного стану. В сучасних умовах українські міста активно використовують цифрові технології для захисту інфраструктури та безпеки громадян. Як підкреслює С. Ткач, впровадження автоматизованих систем моніторингу та управління ресурсами дозволяє забезпечити безперебійність роботи критичних об'єктів інфраструктури під час бойових дій або інших кризових ситуацій [50, с. 94-95].

Таким чином, Smart-рішення, впроваджені у великих містах України, забезпечують значний прогрес у сфері управління містами, покращують безпеку та якість життя громадян, а також дозволяють швидко реагувати на виклики, зокрема в умовах воєнного стану.

В Україні застосування Smart-технологій для підвищення безпеки міст є важливою складовою сучасного урбаністичного розвитку. Успішні кейси втілення таких технологій демонструють, як цифрові інновації сприяють захисту громадян і критичної інфраструктури.

Одним із успішних прикладів є проєкт «Безпечне місто», реалізований у місті Ладижин, Вінницької області. Як зазначають мас-медіа, система на основі відеоспостереження дозволяє поліції швидко реагувати на інциденти, контролювати транспортні потоки та знижувати рівень злочинності [15]. Це дає змогу моніторити події в реальному часі, що сприяє оперативнішому прийняттю рішень.

Ще одним вдалим кейсом є проєкт «Kyiv Smart City». Цей проєкт, як зазнає Transparency International Ukraine, інтегрує різноманітні системи для забезпечення громадської безпеки, включаючи автоматизовані системи контролю доступу, відеомоніторинг і аналітику на основі великих даних [44].

Ці рішення дозволяють не лише підвищити рівень захищеності міста, а й поліпшити якість муніципальних послуг та взаємодію між громадянами і міською владою.

Успішний досвід Харкова також варто зазначити, де застосовуються Smart-рішення для управління безпекою дорожнього руху. За даними [52], використання інтелектуальних систем моніторингу дозволяє суттєво знизити кількість аварій на дорогах завдяки автоматизованим камерам контролю швидкості та управління сигналами світлофорів. Це сприяє зменшенню навантаження на дорожню інфраструктуру та підвищенню загальної безпеки.

Крім того, у Львові впроваджено систему «Безпечне місто», яка дозволяє моніторити вулиці міста за допомогою численних камер спостереження. Як зазначають в Національному транспортному університеті, система спрямована на запобігання терористичним атакам, зниження рівня злочинності, а також підвищення рівня загальної безпеки громадян [52]. Аналітика відеоспостереження допомагає правоохоронним органам виявляти потенційні загрози та своєчасно на них реагувати.

Кейс впровадження Smart-рішень у Вінниці заслуговує окремої уваги. Як відзначає А. Андрієнко, у місті функціонує інтегрована система моніторингу, що дозволяє контролювати ситуацію на дорогах, забезпечувати безпеку громадян та управління інфраструктурними об’єктами [6, с. 74-75]. Відеоспостереження, аналіз даних і автоматизовані повідомлення дозволяють швидко виявляти та реагувати на аварії або надзвичайні ситуації, підвищуючи тим самим безпеку мешканців міста.

Таким чином, впровадження Smart-технологій у великих містах України є ключовим елементом для підвищення рівня безпеки та ефективності міського управління. Використання інтелектуальних систем моніторингу, відеоспостереження та аналізу даних дозволяє міським органам влади оперативно реагувати на загрози, що виникають, та забезпечувати захист населення.

Порівняння українського досвіду застосування Smart-технологій із міжнародними практиками є важливим аспектом аналізу урбаністичних інновацій. В Україні розпочато інтеграцію рішень на зразок систем відеомоніторингу та управління транспортом, що схоже на практики, які успішно застосовуються в таких містах, як Барселона та Сінгапур. Однак українські міста, зокрема Київ і Вінниця, стикаються з унікальними викликами, пов'язаними з воєнним станом, що відрізняє їх від західних міст.

Одним із яскравих прикладів міжнародного досвіду є Барселона, де широко використовуються сенсори для відстеження параметрів навколишнього середовища, автоматизація систем освітлення та розумне управління водними ресурсами. У Києві ж впровадження інноваційних рішень також спрямоване на безпеку та зниження злочинності через комплексну систему відеонагляду та аналітику даних, але акцент робиться на адаптацію технологій до поточних загроз війни. Як зазначають в Transparency International Ukraine , система «Kyiv Smart City» інтегрує різні інструменти для підвищення безпеки та покращення взаємодії громадян із владою [44].

На відміну від західних міст, де ключовими завданнями є екологічна стійкість та розумне управління інфраструктурою, українські міста більше сфокусовані на безпеці населення. Наприклад, система відеомоніторингу в Харкові допомагає контролювати транспортні потоки та реагувати на загрози терористичних атак, що характерно для ситуації з війною [51, с. 62-63].

На міжнародному рівні, Сінгапур також виступає прикладом розвиненого Smart-міста, де ключовими елементами є аналітика великих даних та цифрові рішення для ефективного управління. Зокрема, використання алгоритмів штучного інтелекту допомагає прогнозувати можливі загрози, що дозволяє уникати інцидентів і забезпечувати високий рівень безпеки. Водночас, як зазначає А. Андрієнко, в Україні впровадження подібних рішень знаходиться на етапі активного розвитку, і ключовою відмінністю є те, що вітчизняні міста мають фокус на інтеграцію безпеки в контексті воєнного стану [6, с. 96].

Участь України у форумах та конференціях, присвячених темі Smart-рішень, сприяє обміну досвідом з міжнародними партнерами. Наприклад, у березні 2024 року на форумі Smart City обговорювались можливості адаптації закордонних практик у контексті українських реалій [52]. Зокрема, йшлося про інноваційні рішення для підвищення ефективності міського управління та безпеки, а також їх адаптацію до умов постійної загрози збройних конфліктів.

Таким чином, український досвід впровадження Smart-технологій демонструє активний розвиток у напрямку інтеграції передових світових практик, проте суттєво відрізняється через унікальні виклики, з якими стикаються українські міста в умовах воєнного стану.

Розвиток Smart-технологій для міської безпеки стикається з низкою проблем і перешкод, які впливають на їх ефективність та впровадження. Однією з основних проблем є висока вартість таких рішень, яка обмежує можливості їх повного розгортання у всіх містах. Також виникають труднощі з нормативно-правовим регулюванням та інтеграцією різних компонентів у єдину систему, що часто затримує впровадження нових технологій.

Фінансова складова розвитку Smart-рішень є ключовим викликом. Вартість встановлення сучасних систем, таких як відеоспостереження, аналіз даних і сенсорні технології, значно перевищує бюджетні можливості багатьох українських міст. Наприклад, у Вінниці реалізація комплексних Smart-систем для підвищення безпеки потребує значних інвестицій, що обмежує масштаб впровадження та модернізації систем [15].

Іншою важливою перешкодою є проблема координації та інтеграції. Різні елементи інфраструктури часто належать до різних управлінських структур, що ускладнює синхронізацію між ними. Наприклад, технології для моніторингу транспорту можуть бути несумісні з іншими системами міської безпеки, що потребує значних зусиль для їх інтеграції [6, с. 126-127].

Нормативно-правове регулювання також створює проблеми. Хоча українське законодавство поступово адаптується до нових реалій, часто виникають прогалини у регулюванні використання сучасних Smart-технологій

для безпеки. Це стосується особливо питань конфіденційності даних і прав людини, що ускладнює впровадження автоматизованих систем спостереження та моніторингу громадських просторів [44].

Технологічні виклики також відіграють важливу роль. Не всі міста мають належну технічну базу для ефективної реалізації Smart-рішень, що потребує додаткових інвестицій у модернізацію інфраструктури. Крім того, як відзначають українські вчені, постійний розвиток технологій створює нові виклики для підтримки сумісності старих і нових систем, що вимагає постійного оновлення та покращення рішень [51, с. 61-62].

2.2 Нормативно-правове регулювання Smart-технологій для посилення безпеки міст-мегаполісів в Україні під час воєнного стану

Аналіз законодавчої бази використання Smart-технологій під час воєнного стану є важливим аспектом сучасного розвитку державного управління, особливо в умовах кризи. Використання розумних технологій не лише дозволяє підвищити рівень безпеки і комфорту в містах, але й сприяє ефективнішому управлінню ресурсами та швидкому реагуванню на виклики, пов’язані з воєнним станом. Ця тема актуальна для України, де впровадження інноваційних технологій стало ключовим напрямом розвитку національної інфраструктури.

Перш за все, необхідно зазначити, що впровадження Smart-технологій, або так званих «розумних» технологій, в умовах війни вимагає спеціальної правової бази, яка гарантує безпеку та конфіденційність даних, а також ефективне управління інфраструктурними об’єктами. Розумні міста стають основою для нових форм управління територіями, зокрема у питаннях безпеки, моніторингу та швидкого реагування на загрози. Серед ключових елементів таких міст Transparency International Ukraine називає системи відеоспостереження, управління трафіком, енергозбереження та забезпечення громадської безпеки [44].

Український досвід впровадження розумних технологій під час воєнного стану показав, що системи Smart Building і Smart City можуть стати ефективним інструментом у забезпеченні безпеки населення. Наприклад, форум Smart Building Forum, який відбувся в Києві, наголосив на необхідності впровадження технологій, що забезпечують комфорт та безпеку в умовах екстремальних ситуацій [52].

Законодавче регулювання впровадження розумних технологій під час воєнного стану має свої особливості. Існуючі правові акти України передбачають можливість використання технологій моніторингу та відеоспостереження для забезпечення громадської безпеки. Водночас, як наголошує А. Андрієнко, необхідно вдосконалювати норми, що регулюють використання таких технологій в умовах воєнного стану, зокрема, з огляду на конфіденційність даних і захист персональних даних громадян [6, с. 157-158].

Розвиток нормативно-правової бази для впровадження Smart-технологій в Україні пов'язаний також із міжнародними стандартами, які сприяють інтеграції інноваційних рішень у сфері безпеки. Наприклад, у законодавстві інших країн передбачено окремі положення, які забезпечують ефективну координацію роботи між державними органами і приватним сектором, що забезпечує стійкість інфраструктури під час кризових ситуацій [51, с. 65-66].

Зокрема, важливою складовою є правовий контроль за обміном даними між різними структурами. Використання розумних технологій вимагає чіткого правового регулювання з метою уникнення можливих загроз інформаційної безпеки. Законодавчі ініціативи повинні враховувати не тільки воєнні загрози, але й можливі кіберзагрози, що можуть виникнути при використанні мережевих технологій у сфері державного управління.

Правоохоронні органи в умовах воєнного стану активно використовують розумні технології для забезпечення громадської безпеки. Наприклад, вже згадана презентована у місті Ладижин система «Безпека майбутнього» [15]. Це демонструє приклад того, як технології можуть бути використані для зміцнення безпеки громадян в умовах війни.

Важливо також зазначити, що впровадження таких технологій потребує постійного оновлення та підтримки з боку законодавчої влади. Системи моніторингу повинні відповідати не тільки вимогам конфіденційності, але й забезпечувати максимальну ефективність в умовах зростання рівня загроз.

Для успішного впровадження Smart-технологій необхідна інституційна підтримка на рівні держави та місцевих органів влади. Наприклад, у дослідженні українських науковців підкреслюється, що децентралізація дозволяє ефективніше впроваджувати розумні технології на рівні місцевих громад, що сприяє розвитку інфраструктури та підвищенню якості надання публічних послуг [41, с. 49-50].

Законодавчі ініціативи в цій сфері повинні враховувати особливості місцевого самоврядування та забезпечувати механізми фінансування, які дозволять реалізувати проєкти Smart City на місцевому рівні. Досвід країн ЄС показує, що законодавча підтримка ініціатив місцевих органів влади є критично важливою для успішної реалізації таких проєктів.

З огляду на швидкий розвиток технологій, подальші перспективи впровадження Smart-рішень в Україні будуть значною мірою залежати від гнучкості законодавства і здатності державних органів швидко адаптуватися до нових умов. Впровадження розумних технологій під час воєнного стану повинно враховувати не лише технологічні аспекти, але й соціальні і правові вимоги, які дозволять забезпечити безпеку і добробут громадян [37, с. 164-165].

У підсумку, ефективне використання Smart-технологій в умовах воєнного стану можливе лише за умови існування чіткої законодавчої бази, яка гарантує прозорість, безпеку та відповідність міжнародним стандартам. Україні необхідно продовжувати вдосконалювати правові механізми з огляду на виклики, пов'язані з воєнними загрозами та цифровізацією державного управління.

Воєнний стан в Україні викликає необхідність оперативної адаптації нормативно-правових актів для забезпечення ефективного функціонування державних структур, суспільної безпеки та підтримки громадянського

суспільства в умовах кризи. Актуалізація законодавства в умовах війни пов'язана із запровадженням нових правил, змін у вже існуючих актах та розвитком інституцій, які допомагають реалізовувати ці норми на практиці.

Одним із ключових напрямів адаптації нормативно-правових актів у період воєнного стану є безпека громадян і територій. Сучасні загрози потребують нових підходів до забезпечення безпеки, зокрема через використання інноваційних технологій. Впровадження Smart-технологій у міському управлінні стає важливим елементом для підвищення рівня захисту та забезпечення комфорту громадян в умовах надзвичайних ситуацій. Зокрема, концепція розумних міст передбачає використання автоматизованих систем відеоспостереження та моніторингу, що підвищують швидкість реагування на загрози [44].

Воєнний стан також вплинув на необхідність перегляду законодавства, що стосується захисту персональних даних. Використання сучасних технологій, таких як розумні камери та мережеві системи, викликає нові ризики для конфіденційності інформації. У таких умовах актуалізація законодавчих норм, які регулюють обробку та захист даних, стає одним із пріоритетів для забезпечення безпеки як фізичної, так і інформаційної.

Оновлення правової бази у цій сфері передбачає вдосконалення норм щодо зберігання даних, управління інформаційними ресурсами, а також посилення контролю за доступом до конфіденційної інформації. Як відзначає А. Андрієнко, важливим елементом є також захист даних громадян, які використовуються для підтримки оперативного моніторингу ситуації в країні [6, с. 137-138].

В умовах воєнного стану суттєво змінюється підхід до надання публічних послуг. Зокрема, адаптація правової бази спрямована на спрощення доступу до цих послуг для населення, а також на впровадження нових форм їх надання через цифрові платформи. Використання цифрових сервісів, таких як «Дія», стає ключовим елементом, що дозволяє забезпечити безперебійний доступ до адміністративних послуг навіть в умовах військових дій.

Важливо, щоб законодавство враховувало особливості використання цифрових платформ в умовах надзвичайних ситуацій. Як зазначають українські науковці, під час війни доступність та безпека цих сервісів стає питанням першочергового значення, тому держава має адаптувати нормативні акти, що стосуються роботи таких платформ, щоб вони могли функціонувати в умовах обмеженої інфраструктури та можливих загроз кібербезпеки [51, с. 71-72].

Під час воєнного стану правоохоронні органи відіграють ключову роль у забезпеченні порядку та безпеки. У зв'язку з цим відбувається адаптація законодавства, що регулює діяльність поліції та інших силових структур. Одним із прикладів є впровадження розумних систем моніторингу та відеоспостереження для швидкого реагування на кримінальні загрози та вищезгадана презентація у місті Ладижин проєкту «Безпека майбутнього» [15].

Крім того, актуалізуються нормативні акти, що стосуються оперативного управління кризовими ситуаціями. Для цього вносяться зміни до існуючих законів і постанов, які надають правоохоронцям розширені повноваження щодо контролю за ситуацією в умовах війни. Ці зміни допомагають ефективніше реагувати на загрози та підтримувати порядок у складних умовах.

Успішна адаптація законодавства під час воєнного стану потребує також інституційної підтримки на всіх рівнях управління. Дослідження показують, що децентралізація влади в Україні сприяє швидшому впровадженню змін на місцевому рівні. Наприклад, територіальні громади відіграють важливу роль у забезпеченні публічних послуг і безпеки населення, тому законодавчі ініціативи повинні враховувати їх потреби та можливості [41, с. 48-49].

Адаптація нормативно-правових актів на місцевому рівні дозволяє оперативно реагувати на виклики воєнного стану, зокрема в контексті управління ресурсами та координації дій між різними структурами. Законодавчі ініціативи повинні підтримувати розвиток місцевих інституцій, надаючи їм достатньо повноважень для швидкого прийняття рішень.

Попри успіхи у зміні законодавства, воєнний стан вимагає постійної актуалізації правових норм. Виклики, пов'язані з війною, зокрема загроза

кібербезпеці, обмеженість ресурсів і складні гуманітарні умови, вимагають нових підходів до правового регулювання. Водночас необхідно забезпечити стабільність правової системи, щоб уникнути хаосу у державному управлінні.

Перспективи адаптації законодавства пов'язані із здатністю державних інституцій швидко реагувати на нові виклики. Це стосується як цифровізації державних процесів, так і впровадження нових норм у сфері безпеки та надання публічних послуг. Подальший розвиток законодавчої бази також залежить від ефективної взаємодії між різними рівнями влади та приватним сектором, що дозволить інтегрувати нові технології та рішення для забезпечення безпеки й добробуту населення [37, с. 164-165].

Водночас, у сучасному світі забезпечення національної безпеки неможливе без активної взаємодії між державними структурами та приватним бізнесом. Це співробітництво дозволяє не тільки розвивати інноваційні технології, але й адаптувати їх для практичного використання у сфері безпеки. В Україні такий підхід особливо актуальний в умовах війни та постійних загроз, коли державні ресурси потребують ефективної підтримки приватного сектору для швидкого й результативного впровадження технологій безпеки.

Взаємодія держави з бізнесом у сфері безпеки відкриває низку можливостей для підвищення ефективності захисту національних інтересів. Перш за все, приватний сектор є джерелом інновацій та технологій, які можуть бути швидко інтегровані у державні системи. Такі технології включають системи відеоспостереження, аналітику великих даних, кібербезпеку, а також інструменти для управління кризовими ситуаціями.

Досвід багатьох країн свідчить про те, що участь бізнесу у впровадженні технологій безпеки дозволяє державі економити ресурси, зменшувати час на розробку нових рішень і оперативно реагувати на загрози. Як відзначає А. Андрієнко, у процесі цифровізації України, бізнес активно підтримує ініціативи, спрямовані на підвищення національної безпеки шляхом впровадження нових цифрових рішень [6, с. 54-55].

Одним із найважливіших напрямів співпраці держави та бізнесу є цифрова трансформація у сфері безпеки. У сучасних умовах технології, що базуються на аналізі великих даних, штучному інтелекті та блокчейні, мають значний потенціал для підвищення ефективності державних структур. Наприклад, українські науковці відзначають, що технології автоматизованого моніторингу та аналізу відеоданих дозволяють швидко виявляти загрози, а також оперативно надавати необхідну інформацію правоохоронним органам [51, с. 74-75].

Цифрова трансформація також сприяє розвитку кібербезпеки, яка стає одним із ключових факторів у забезпеченні захисту держави. Український досвід показує, що співпраця між державними структурами та бізнесом у цьому напрямі дозволяє захистити критичну інфраструктуру від кібератак та гарантувати безперервність функціонування важливих державних систем. Зокрема, кібербезпека стала пріоритетом після 2014 року, коли Україна зіткнулася з масштабними кіберзагрозами. У цих умовах, на думку А. Мунько, приватний сектор став важливим партнером у розробці та впровадженні технологічних рішень для забезпечення захисту державних інформаційних систем [37, с. 162-163].

Іншим важливим аспектом співпраці держави та бізнесу є реалізація спільних проєктів у сфері безпеки. В Україні існують численні приклади таких проєктів, коли приватні компанії надають технологічні рішення для потреб державних структур. Один із таких прикладів – програми розумних міст (Smart City), де бізнес інвестує у розробку та впровадження систем моніторингу, освітлення, контролю доступу та інших технологій, які підвищують рівень безпеки на вулицях міст і сприяють запобіганню злочинності [37, с. 164-165].

Спільні проєкти охоплюють не лише сфери фізичної безпеки, але й кібербезпеку, управління кризовими ситуаціями та моніторинг інфраструктури. Важливим аспектом цієї співпраці є те, що держава може користуватися досвідом і ресурсами бізнесу для розробки спеціалізованих рішень, а також забезпечувати їх швидке впровадження. На думку Г. Швець, це дозволяє

зменшити витрати та покращити ефективність управління у кризових ситуаціях, зокрема під час воєнних дій або інших загроз [56].

Водночас, попри очевидні переваги, співпраця між державними структурами та бізнесом у сфері безпеки не позбавлена викликів. Одним із найбільших є питання регулювання правових аспектів такої співпраці, зокрема щодо захисту персональних даних, управління інформаційними потоками та дотримання конфіденційності. Держава, на думку експертів, повинна забезпечити відповідне законодавче підґрунтя, яке б дозволяло бізнесу ефективно інтегрувати свої рішення у державні системи, водночас захищаючи права громадян [12].

Ще одним викликом є забезпечення надійності та безпеки самих технологій. Оскільки багато інноваційних рішень залежить від підключення до інтернету та використання великих даних, кібербезпека стає основним питанням. Взаємодія державних і приватних структур має враховувати необхідність створення надійних протоколів для захисту від зовнішніх загроз і можливих збоїв у системах безпеки.

Крім внутрішньої співпраці, важливим аспектом впровадження технологій безпеки є взаємодія з міжнародними партнерами. Багато міжнародних організацій та компаній надають підтримку Україні у сфері розробки та впровадження технологічних рішень для підвищення рівня безпеки. Наприклад, Європейський Союз та США надають Україні технічну допомогу для розвитку кібербезпеки, а також підтримують розвиток інновацій у сфері управління кризовими ситуаціями [47].

Міжнародна співпраця дозволяє Україні не тільки отримувати технологічну підтримку, але й обмінюватися досвідом з іншими країнами. Це сприяє розвитку нових підходів до забезпечення безпеки, які можуть бути адаптовані до українських реалій. Також міжнародні партнери допомагають впроваджувати стандарти кібербезпеки, що підвищують стійкість державних систем до зовнішніх загроз.

Співпраця державних структур із бізнесом у впровадженні технологій безпеки є важливим елементом забезпечення національної безпеки України. Ця взаємодія дозволяє інтегрувати інноваційні рішення у державні системи, підвищуючи ефективність управління безпекою та захистом національних інтересів. Однак для успішної співпраці необхідно подолати виклики, пов'язані із законодавчим регулюванням, кібербезпекою та захистом даних. Міжнародна підтримка відіграє ключову роль у розвитку технологій безпеки та їхньому впровадженні в Україні.

2.3. Організаційно-економічні механізми використання Smart-технологій для посилення безпеки міст-мегаполісів в сучасних умовах України

У сучасних умовах, коли українські міста, зокрема мегаполіси, стикаються з численними викликами, зумовленими війною, урбанізацією, економічною нестабільністю та зростанням злочинності, актуальним питанням стає впровадження Smart-технологій для підвищення безпеки. Smart-технології дозволяють ефективно вирішувати проблеми управління міськими системами, забезпечуючи комплексний підхід до безпеки. Однак, успішне впровадження цих технологій вимагає наявності чітко структурованих організаційно-економічних механізмів, що регулюють процес їх впровадження та використання.

Smart-технології є інноваційними інструментами для вирішення широкого спектра проблем у мегаполісах, включаючи питання безпеки. Вони включають використання інтелектуальних систем спостереження, управління трафіком, моніторинг стану інфраструктури та швидке реагування на надзвичайні ситуації. Особливе значення, на думку А. Андрієнко, мають системи відеоспостереження, що дозволяють оперативно виявляти та реагувати на загрози громадській безпеці, а також автоматизовані системи оповіщення

про надзвичайні ситуації, які забезпечують своєчасне інформування населення [6, с. 164-165].

У сучасній Україні безпека мегаполісів є важливим аспектом не лише для забезпечення нормального функціонування міської інфраструктури, а й для підтримки стабільності та відновлення після воєнних дій. Технологічні рішення мають забезпечити комплексний підхід до безпеки: від моніторингу громадських місць до управління кризовими ситуаціями та забезпечення кібербезпеки.

Для того щоб Smart-технології ефективно працювали в умовах мегаполісів, необхідно створити надійну організаційно-економічну систему їх впровадження та управління. Ця система повинна забезпечити гармонійне поєднання інтересів держави, приватного сектору та громадськості. Основними елементами цієї системи виступають фінансові механізми. Кожен із них має свої переваги та недоліки, залежно від економічної ситуації міста, обсягу інвестицій та специфіки технологій, які впроваджуються.

Традиційно, значна частина проектів у сфері безпеки фінансується державою. Державне фінансування Smart-проєктів передбачає використання бюджету для покриття витрат на розробку, впровадження та обслуговування систем безпеки. В Україні держава активно бере участь у фінансуванні таких проєктів через державні програми модернізації та цифровізації. На думку А. Андрієнко, це дозволяє забезпечити стабільне фінансування критично важливих проєктів, особливо у сфері громадської безпеки та кібербезпеки [6, с. 167-168].

Державне фінансування також забезпечує контроль з боку держави за стратегічними рішеннями, що дозволяє краще координувати ініціативи. Водночас цей підхід може бути обмежений через нестачу коштів, особливо у кризові часи, як-от у період воєнного стану.

Приватно-державне партнерство (PPP) є однією з найефективніших моделей фінансування Smart-проєктів. У рамках цього підходу, приватні компанії беруть на себе частину фінансового навантаження, інвестуючи в

розробку та впровадження технологій. У свою чергу, на думку українських вчених, держава надає доступ до інфраструктури, законодавчі гарантії та підтримує проєкти на рівні нормативно-правового регулювання [51, с. 59].

PPP є вигідним як для держави, так і для бізнесу, оскільки дозволяє залучити додаткові ресурси, зменшити навантаження на бюджет і, водночас, забезпечити високий рівень інновацій. Наприклад, в Україні такі проєкти активно реалізуються у сфері кібербезпеки, де бізнес надає технологічні рішення, а держава інтегрує їх у свої структури [37, с. 162-163].

Міжнародні організації та фінансові інституції відіграють важливу роль у фінансуванні Smart-проєктів для безпеки міст. Європейський Союз, ООН, Світовий банк та інші організації надають гранти на впровадження інноваційних технологій у сфері громадської безпеки. Це особливо важливо для країн, що розвиваються, де доступ до фінансових ресурсів обмежений [37, с. 163-164].

Гранти дозволяють фінансувати масштабні проєкти, такі як системи відеоспостереження, «розумні» вулиці та інші технології, які підвищують безпеку громадян. В Україні міжнародні організації активно підтримують Smart-проєкти, зокрема у контексті реформ децентралізації та цифровізації громад [56].

Ще одним сучасним інструментом фінансування Smart-проєктів є краудфандинг. Це підхід, який передбачає збір коштів від громадян, бізнесу та інших зацікавлених осіб для реалізації конкретних проєктів. Наприклад, як відзначають експерти, міські громади можуть організовувати збори коштів для впровадження систем відеоспостереження або розумного освітлення в районах, де рівень злочинності є підвищеним [12].

Краудфандинг дозволяє підвищити рівень громадської участі у вирішенні проблем безпеки та забезпечити додаткове фінансування для реалізації проєктів, які не можуть бути покриті державними ресурсами. Успіх цього підходу залежить від активності громадян і прозорості використання зібраних коштів.

Міські ради та інші органи місцевого самоврядування відіграють важливу роль у впровадженні Smart-технологій. Муніципальні ініціативи, спрямовані на поліпшення безпеки, можуть включати інвестиції в інфраструктуру для відеоспостереження, системи «розумного» освітлення та інші технології, що сприяють підвищенню рівня безпеки на вулицях мегаполісів [59].

Зокрема, муніципалітети можуть ініціювати впровадження локальних систем моніторингу, що дозволяють виявляти загрози на ранній стадії та оперативно реагувати на них. Це підвищує рівень безпеки громадян і сприяє створенню комфортного середовища для життя.

Smart-технології значно підвищують рівень безпеки в мегаполісах, надаючи можливості для швидкого реагування на надзвичайні ситуації, зменшення рівня злочинності та ефективного управління міськими ресурсами. Наприклад, системи «розумного» моніторингу дозволяють контролювати ключові точки міста, забезпечуючи своєчасне виявлення загроз і швидке реагування поліції чи інших служб.

Також технології автоматизованого управління транспортом можуть суттєво знизити рівень аварійності, покращити трафік та забезпечити безпеку на дорогах мегаполісів. Це досягається через використання датчиків, відеокамер та систем штучного інтелекту, що аналізують трафік у режимі реального часу та вносять корективи до управління транспортними потоками.

Одним із успішних прикладів фінансування Smart-проєктів є проєкт «Smart City» у Києві, який передбачає впровадження технологій для моніторингу громадської безпеки, управління транспортом та енергетикою. Важливим елементом фінансування цього проєкту стало приватно-державне партнерство, де бізнес взяв на себе частину витрат на розробку та впровадження технологій, а держава забезпечила нормативно-правове регулювання та інтеграцію рішень у міські системи [47].

Ще одним прикладом є проєкти відеоспостереження, впроваджені у Львові та Харкові. Вони дозволяють оперативно виявляти загрози та реагувати на надзвичайні ситуації, що підвищує рівень безпеки мешканців міст.

Фінансування цих проєктів здійснювалося за допомогою міжнародних грантів та державного фінансування, що дозволило зменшити фінансове навантаження на місцеві бюджети.

Вибір моделі фінансування значною мірою визначає успішність впровадження Smart-проєктів для безпеки міст. Державне фінансування забезпечує стабільність і контроль з боку держави, але обмежене бюджетними можливостями. Приватно-державне партнерство дозволяє залучити інновації та ресурси бізнесу, але потребує складного законодавчого регулювання та прозорості. Міжнародна допомога та гранти можуть стати вирішальними для впровадження великих проєктів, але залежать від міжнародної підтримки. Краудфандинг дозволяє громаді активно брати участь у вирішенні проблем безпеки, але потребує довіри з боку громадян.

Загалом, ефективне фінансування Smart-проєктів для безпеки міст вимагає комплексного підходу, який включає поєднання різних джерел фінансування, зокрема державного бюджету, приватних інвестицій, міжнародної допомоги та громадських ініціатив. Це дозволить не лише впроваджувати інноваційні рішення, але й забезпечувати їхню стійкість та ефективність на довгострокову перспективу.

Фінансування Smart-проєктів для безпеки міст є складним, але необхідним процесом для забезпечення сучасної інфраструктури та безпеки громадян. Важливо вибирати правильні моделі фінансування залежно від конкретних умов та можливостей

Попри всі переваги, існують певні виклики у впровадженні Smart-технологій. До них можна віднести високу вартість впровадження, необхідність у технічному обслуговуванні та модернізації систем, а також ризики, пов'язані з кіберзагрозами. В умовах війни в Україні, на думку експертів, ці виклики стають ще більш актуальними, оскільки ресурси для реалізації технологічних проєктів можуть бути обмеженими [35].

Також важливою проблемою є необхідність розробки чіткої нормативно-правової бази, яка б регулювала використання Smart-технологій, зокрема у сфері громадської безпеки. Ці технології потребують

Smart-технології для безпеки міст стали невід'ємною частиною сучасної урбаністичної інфраструктури. Їх впровадження дозволяє підвищити ефективність управління міським простором, покращити громадську безпеку та реагування на надзвичайні ситуації. Однак, однією з ключових проблем є фінансування таких проєктів, оскільки впровадження технологічних рішень вимагає значних інвестицій, що потребує розробки спеціальних моделей фінансування.

Висновки до розділу 2

Розбудова використання Smart-технологій для підвищення безпеки в українських містах-мегаполісах є одним із важливих кроків у вирішенні сучасних викликів безпеки та ефективного управління міським середовищем. Після детального аналізу сучасного стану розвитку та нормативно-правових аспектів впровадження таких технологій можна зробити кілька ключових висновків щодо їх значення, перспектив та проблем впровадження.

Однією з ключових тенденцій розвитку Smart-технологій у сучасних умовах є активне впровадження інтелектуальних систем відеоспостереження, моніторингу та управління транспортними потоками. На сьогодні у більшості великих міст України, таких як Київ, Харків, Дніпро та Одеса, впроваджуються технології для контролю за громадським порядком і трафіком, а також системи оповіщення про надзвичайні ситуації. Важливо зазначити, що такі технології активно використовуються не лише для запобігання злочинам, але й для підвищення ефективності управління міськими системами в умовах надзвичайних ситуацій, зокрема під час воєнних дій.

Сучасний стан розвитку Smart-технологій можна охарактеризувати як фазу активного становлення. Незважаючи на певні успіхи в інтеграції окремих

елементів інтелектуальних систем, загальна картина залишається нерівномірною, що зумовлено кількома факторами. По-перше, впровадження таких систем потребує значних фінансових ресурсів, які обмежені через воєнні дії та економічну нестабільність в країні. По-друге, технології потребують високого рівня кваліфікації як з боку інженерів, так і з боку муніципальних управлінців, що вимагає додаткового навчання кадрів.

Також важливо відзначити тенденції співпраці між державними установами та приватними компаніями. Приватно-державне партнерство (PPP) стає все більш поширеним методом для фінансування та впровадження Smart-технологій. Це дозволяє значно зменшити фінансове навантаження на міські бюджети та водночас впроваджувати найсучасніші рішення на основі інновацій приватного сектору. Іншою позитивною тенденцією є залучення міжнародних грантів, які сприяють впровадженню технологій в умовах воєнного часу.

Загалом, динаміка розвитку Smart-технологій в Україні свідчить про поступове збільшення їхнього використання, хоча існує ряд факторів, що обмежують темпи впровадження. Серед них можна виділити обмеженість фінансових ресурсів, необхідність розробки відповідних законодавчих актів та потребу в розвитку професійних компетенцій серед муніципальних служб.

В умовах воєнного стану питання нормативно-правового регулювання використання Smart-технологій для безпеки набуває особливого значення. По-перше, необхідно чітко визначити правові рамки, в яких здійснюватиметься моніторинг та обробка персональних даних громадян. Smart-технології передбачають активне використання систем відеоспостереження, датчиків та інших інструментів, що збирають дані про пересування громадян, трафік та інші аспекти міського життя. Відповідно, виникає потреба в захисті конфіденційності та особистих даних мешканців міст.

На сьогодні в Україні вже існують певні законодавчі ініціативи, спрямовані на регулювання використання таких технологій. Однак, загальний правовий механізм залишається ще недосконалим. Зокрема, чинне законодавство не завжди враховує специфіку використання Smart-систем в

умовах воєнного часу. Необхідним є оновлення нормативно-правової бази, зокрема з урахуванням воєнного стану та можливих кіберзагроз, що стають більш актуальними під час військових конфліктів.

Існує також проблема адаптації міжнародних стандартів до українських реалій. Наприклад, багато західних країн мають чітко визначені правові норми щодо використання технологій відеоспостереження в громадських місцях, а також щодо кібербезпеки. Для України важливим є не лише створення власних законодавчих актів, але й адаптація найкращих міжнародних практик з метою ефективного захисту прав громадян і забезпечення безпеки мегаполісів.

Під час воєнного стану актуальним є також питання залучення міжнародних організацій та фінансових інституцій для підтримки впровадження Smart-технологій. Наприклад, організації, як Європейський Союз та ООН, можуть надавати як фінансову, так і технічну підтримку у впровадженні систем кібербезпеки та інтелектуальних систем управління міськими інфраструктурами. Це дозволяє не лише покращити загальний рівень безпеки в містах, але й адаптувати міські системи до нових викликів, таких як зростання кіберзагроз.

Іншим важливим аспектом правового регулювання є питання відповідальності за функціонування таких систем. З огляду на складність і комплексність Smart-технологій, необхідним є чітке розподілення відповідальності між державними органами, приватними компаніями та міжнародними організаціями, які можуть бути залучені до процесу впровадження та управління такими системами.

Впровадження Smart-технологій для підвищення безпеки в українських містах-мегаполісах є складним процесом, що потребує ефективних організаційно-економічних механізмів. Поєднання цих механізмів забезпечує не лише технологічну інтеграцію інтелектуальних систем, але й гарантує фінансову стійкість, ефективність управління та підтримку сталого розвитку безпекових ініціатив.

Основною складовою організаційного механізму є тісна співпраця між державними структурами, муніципалітетами та приватним сектором. Успішне впровадження Smart-технологій неможливе без залучення приватного бізнесу та міжнародних організацій, які можуть надавати не тільки фінансування, а й технологічну експертизу. Приватно-державні партнерства (PPP) відіграють ключову роль, дозволяючи об'єднати ресурси для масштабних проєктів. Зокрема, у таких містах, як Київ, Харків та Одеса, приватні компанії активно беруть участь у впровадженні систем відеоспостереження, аналітики даних та контролю доступу.

Економічний механізм впровадження Smart-технологій базується на оптимізації фінансових потоків та залученні альтернативних джерел фінансування, таких як міжнародні гранти та кредити від міжнародних фінансових інституцій. В умовах економічних викликів, пов'язаних із воєнним станом, міста мають змогу залучати кошти від донорів, таких як Європейський Союз, ООН та інші міжнародні партнери. Крім того, важливим є використання сучасних моделей фінансування, таких як краудфандинг та залучення інвестицій через механізми соціального впливу (Social Impact Bonds).

Ще однією ключовою особливістю економічних механізмів є необхідність забезпечення ефективного управління ресурсами. Впровадження Smart-технологій вимагає значних капіталовкладень на початковому етапі, але у довгостроковій перспективі забезпечує економію коштів через оптимізацію ресурсів, зменшення витрат на енергетику та підвищення ефективності управління міськими інфраструктурами. Використання датчиків, інтелектуальних систем управління трафіком та інших технологій дозволяє суттєво скоротити витрати на експлуатацію та обслуговування інфраструктури.

Крім того, нормативно-правова база для впровадження таких механізмів потребує оновлення та адаптації до сучасних реалій. Зокрема, важливо впроваджувати міжнародні стандарти та адаптувати їх до українського законодавства, враховуючи специфіку використання таких технологій в умовах підвищеного ризику для безпеки.

Таким чином, організаційно-економічні механізми впровадження Smart-технологій для посилення безпеки міст-мегаполісів в Україні є комплексною системою, що поєднує тісну співпрацю між державою, бізнесом та міжнародними партнерами. Ця система потребує подальшого розвитку як на рівні фінансування, так і на рівні управління ресурсами для забезпечення стійкості й ефективності в довгостроковій перспективі.

Загалом, у другому розділі було розглянуто ключові аспекти впровадження та розвитку Smart-технологій для підвищення безпеки в українських мегаполісах. Аналіз сучасного стану показав, що впровадження цих технологій є необхідним кроком для забезпечення громадського порядку, ефективного управління міськими системами та протидії зростанню злочинності в умовах міських агломерацій. Основними перевагами є можливість швидкого реагування на загрози, зменшення ризику надзвичайних ситуацій, а також підвищення ефективності управління міською інфраструктурою.

Водночас, для ефективного функціонування цих систем необхідно подолати ряд викликів, серед яких фінансові обмеження, недостатня розвиненість нормативно-правової бази та потреба в підвищенні кваліфікації муніципальних кадрів. Також важливим є залучення міжнародного досвіду та фінансування для забезпечення стійкості таких систем в умовах війни.

Питання нормативно-правового регулювання є ключовим аспектом для забезпечення належного функціонування Smart-технологій. Необхідно розробити комплексну правову базу, що враховуватиме специфіку використання таких технологій в умовах війни та підвищених ризиків для кібербезпеки. Крім того, важливим є захист прав громадян у контексті використання персональних даних, що також потребує додаткової уваги законодавців.

РОЗДІЛ 3 ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ ВИКОРИСТАННЯ ЗАСТОСУВАННЯ SMART-ТЕХНОЛОГІЙ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ МІСТ-МЕГАПОЛІСІВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

3.1. Рекомендації щодо застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні на законодавчому рівні

В умовах воєнного стану, який Україна переживає через військову агресію Російської Федерації, впровадження Smart-технологій для посилення безпеки міст-мегаполісів стає ключовим напрямом державної політики. Сучасні технології забезпечують ефективний контроль над безпекою, управління критичною інфраструктурою, координацію дій під час надзвичайних ситуацій та попередження загроз. Успішне використання цих технологій потребує чіткого та своєчасного правового регулювання, тому законодавчі ініціативи мають відігравати провідну роль у забезпеченні нормативної бази для впровадження Smart-рішень.

1. Створення правового підґрунтя для застосування Smart-технологій. Перш за все, для ефективного застосування Smart-технологій на державному рівні необхідно удосконалити існуючу нормативно-правову базу. Законодавчі акти мають охоплювати всі аспекти використання Smart-рішень, від захисту персональних даних до фінансування інноваційних проєктів. Для цього слід оновити закони, які регулюють інформаційну безпеку, кіберзахист, а також створити нові положення щодо використання технологій штучного інтелекту, Інтернету речей (IoT) і великих даних (Big Data).

Законодавчі ініціативи повинні передбачати адаптацію існуючих нормативних актів до сучасних викликів, які постають перед Україною в умовах війни. Це включає оновлення Закону України «Про основи національної безпеки» та Закону «Про захист критичної інфраструктури». Вони мають

враховувати нові загрози, які виникають через використання сучасних технологій для терористичних та військових цілей.

В умовах воєнного стану важливо також ввести жорсткіші вимоги щодо захисту міської інфраструктури, що використовує Smart-рішення, та закріпити відповідні норми на законодавчому рівні. Наприклад, міста повинні мати право тимчасово обмежувати доступ до певних технологій для запобігання їх несанкціонованого використання в умовах воєнних дій або загрози терористичних актів.

2. Забезпечення кібербезпеки та захисту даних. Smart-технології базуються на величезних масивах даних, включаючи особисту інформацію громадян, відомості про міську інфраструктуру та критичні об'єкти. З огляду на це, критично важливо впровадити на законодавчому рівні ефективні механізми кіберзахисту. Нормативні акти повинні забезпечувати суворий контроль за зберіганням і обробкою даних, а також передбачати чіткі протоколи дій у разі кіберзагроз або витоку інформації.

Державні структури мають надавати пріоритетність удосконаленню законодавства у сфері кібербезпеки та захисту даних, зокрема через оновлення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону «Про електронні комунікації». Такі зміни дозволять більш ефективно регулювати питання, пов'язані з кібербезпекою в контексті використання Smart-технологій для посилення безпеки.

Також важливо на законодавчому рівні закріпити механізми обміну інформацією між державними органами та приватними компаніями, які володіють критично важливими даними. Це забезпечить своєчасне реагування на загрози та забезпечить комплексний підхід до захисту національних інтересів в умовах воєнного стану.

3. Законодавча підтримка приватно-державного партнерства. Одним із найважливіших аспектів впровадження Smart-технологій є залучення приватного сектора до процесу розробки та використання таких рішень. Приватно-державне партнерство (PPP) дозволяє не лише залучати інвестиції у

проєкти підвищення безпеки міст, але й забезпечує більш гнучкий підхід до розробки та реалізації таких ініціатив.

Законодавство повинно сприяти розвитку PPP через спрощення процедур укладення договорів між державою та приватними компаніями. Для цього необхідно удосконалити Закон України «Про публічно-приватне партнерство», враховуючи специфіку впровадження Smart-технологій. Крім того, важливо передбачити механізми податкових пільг та субсидій для компаній, які займаються впровадженням технологій безпеки.

Також законодавче регулювання в цій сфері має бути удосконалене з метою залучення приватних інвестицій у розвиток безпекової інфраструктури та інноваційних рішень для міст шляхом розробки законопроекту про стимулювання публічно-приватного партнерства у сфері безпеки міст повинен передбачати:

- Спрощення процедур укладення договорів між державними органами та приватними компаніями;
- Введення податкових пільг для компаній, які інвестують у проєкти Smart-безпеки;
- Запровадження механізмів компенсації витрат на дослідження та розробки у сфері інноваційних технологій;
- Створення державних грантових програм для підтримки стартапів, які працюють над розробкою технологій безпеки.

Такі зміни в законодавстві дозволять більш активно залучати приватний сектор до розв'язання проблем безпеки міст, а також стимулюватимуть інноваційний розвиток у цій сфері.

На законодавчому рівні також необхідно створити умови для залучення іноземних інвестицій, зокрема через міжнародні фонди та грантові програми. Це дозволить розширити можливості фінансування проектів та прискорити їх впровадження.

4. Гармонізація національних законодавчих норм із міжнародними стандартами. Україна повинна активно інтегруватися в міжнародну систему

правового регулювання використання Smart-технологій. Законодавство, що регулює впровадження Smart-рішень, має бути гармонізоване з міжнародними нормами і стандартами. Це стосується таких питань, як захист персональних даних, кібербезпека, використання хмарних технологій та штучного інтелекту.

Особливу увагу слід приділити адаптації українського законодавства до стандартів Європейського Союзу, що є важливим етапом у контексті євроінтеграційних прагнень України. Зокрема, Україна має адаптувати національні нормативно-правові акти до вимог Загального регламенту захисту даних ЄС (GDPR), що стане гарантією безпеки персональних даних у процесі впровадження Smart-технологій.

5. Законодавче обґрунтування впровадження Smart-технологій для безпеки міст. Першим кроком у цьому напрямі має бути розробка та прийняття спеціалізованого закону, який регулюватиме впровадження Smart-технологій для посилення безпеки міст-мегаполісів. Такий законопроект повинен встановлювати чіткі рамки щодо використання інноваційних технологій у сфері громадської безпеки, управління критичною інфраструктурою, моніторингу та попередження надзвичайних ситуацій.

Основні положення цього закону мають охоплювати:

- Визначення основних термінів та понять, пов'язаних із Smart-технологіями;
- Норми щодо захисту персональних даних під час використання технологій збору та обробки інформації;
- Вимоги до кібербезпеки та захисту інформаційних систем;
- Положення щодо інтеграції інноваційних рішень у міську інфраструктуру;
- Стимулювання приватно-державного партнерства для залучення інвестицій у сфері безпеки.

Такий законопроект не лише сприятиме впровадженню новітніх технологій, але й забезпечить правову основу для їх використання, що важливо в умовах воєнного стану, коли питання безпеки стають пріоритетними.

6. Розробка стратегії цифрової трансформації для посилення безпеки міст. Верховна Рада має затвердити загальнонаціональну стратегію цифрової трансформації для посилення безпеки міст і мегаполісів. Ця стратегія повинна бути узгоджена з вже існуючими програмами цифровізації та національної безпеки і передбачати конкретні кроки щодо впровадження Smart-рішень у міську інфраструктуру.

Ключовими напрямами стратегії мають бути:

- Визначення пріоритетних напрямів використання Smart-технологій для безпеки;
- Інтеграція цифрових рішень у системи управління критичною інфраструктурою міст;
- Розвиток систем моніторингу та аналітики для попередження загроз і реагування на надзвичайні ситуації;
- Створення єдиної інформаційної платформи для обміну даними між державними органами, приватними компаніями та громадянами;
- Підвищення рівня цифрової грамотності серед працівників державного сектору, які займаються безпекою.

Важливим компонентом стратегії повинні стати заходи з кібербезпеки, оскільки більшість Smart-технологій пов'язані з великими даними, управлінням інформаційними потоками та доступом до цифрової інфраструктури.

7. Забезпечення на законодавчому рівні захисту критичної інфраструктури. Одним із ключових аспектів підвищення безпеки міст є захист критичної інфраструктури. Верховна Рада має прийняти законопроект, який регулюватиме захист об'єктів критичної інфраструктури в умовах використання Smart-технологій. Це включає не лише фізичний захист об'єктів, але й забезпечення кібербезпеки та стійкості інформаційних систем.

Основні положення такого закону повинні охоплювати:

- Визначення критеріїв для класифікації об'єктів як критичної інфраструктури;
- Вимоги до кіберзахисту та управління ризиками;

- Запровадження механізмів моніторингу та швидкого реагування на загрози;
- Встановлення правил щодо доступу до інформації, пов'язаної з критичною інфраструктурою, та її захисту;
- Зобов'язання щодо регулярного аудиту безпеки таких об'єктів.

Цей законопроект допоможе посилити захист ключових міських об'єктів, таких як енергетичні системи, водопостачання, транспорт та зв'язок, що є критично важливими для функціонування міст у надзвичайних умовах.

8. Розробка стандартів кібербезпеки для міських інфраструктур. Одним із головних викликів при впровадженні Smart-технологій для безпеки міст є питання кібербезпеки. Верховна Рада має прийняти законопроекти, які б регулювали захист інформаційних систем та мереж, що використовуються для управління міською інфраструктурою. Такі законодавчі ініціативи мають включати стандарти безпеки для різних видів інфраструктури, а також вимоги щодо захисту даних і механізмів швидкого реагування на кіберзагрози.

Основні положення законопроектів з кібербезпеки повинні включати:

- Встановлення обов'язкових вимог щодо захисту інформаційних систем міських об'єктів;
- Регулювання діяльності компаній, що надають послуги в сфері кібербезпеки;
- Введення штрафів за порушення стандартів кібербезпеки;
- Розробку національних стандартів для управління інформаційною безпекою;
- Створення державних сертифікаційних центрів, які будуть перевіряти відповідність технологій вимогам безпеки.

Важливим аспектом цих законопроектів має бути також забезпечення навчання та сертифікації спеціалістів у галузі кібербезпеки для роботи з міськими Smart-системами.

9. Законодавчі ініціативи для залучення міжнародної допомоги. В умовах воєнного стану Україна має використовувати всі можливості для залучення

міжнародної допомоги та інвестицій у розвиток Smart-технологій. Верховна Рада повинна прийняти законопроекти, які сприятимуть співпраці з міжнародними організаціями та донорами. Це може бути законопроект про спрощення процедур залучення іноземних інвестицій у проєкти з безпеки, а також введення спеціальних умов для міжнародних компаній, які готові інвестувати у розвиток українських міст.

Основні положення таких законопроектів мають передбачати:

- Створення пільгових умов для міжнародних інвесторів;
- Спрощення реєстраційних процедур для іноземних компаній;
- Розробку міжнародних програм співфінансування проєктів безпеки;
- Введення механізмів контролю та моніторингу за використанням іноземних коштів.

10. Розробка законодавчих ініціатив у сфері інноваційних технологій. Для забезпечення ефективного впровадження Smart-технологій важливо створити законодавчу базу для стимулювання розвитку інноваційних технологій в Україні. Зокрема, це стосується таких напрямів, як штучний інтелект, блокчейн, Інтернет речей та великі дані. На сьогоднішній день у законодавстві України відсутні чіткі положення, які б регулювали розвиток цих технологій.

11. Розробка комплексного законодавчого акту впровадження та використання Smart-технологій для безпеки в містах. Одна з головних проблем полягає в тому, що Україна наразі не має єдиного комплексного законодавчого акту, який би регулював впровадження та використання Smart-технологій для безпеки в містах. Існуючі нормативні акти мають фрагментарний характер і не охоплюють усі аспекти взаємодії таких технологій із системами національної безпеки. Наприклад, регулювання окремих компонентів, таких як відеоспостереження чи системи управління дорожнім рухом, існує, але комплексний підхід до їх інтеграції та координації з іншими елементами міських систем безпеки відсутній.

Крім того, участь України в міжнародних організаціях, таких як Міжнародний союз електрозв'язку (ITU) та Організація економічного

співробітництва і розвитку (OECD), дозволить використовувати найкращі світові практики у сфері регулювання Smart-технологій.

12. Створення чітких регуляторних норм для екстрених ситуацій. Окрему увагу слід приділити відсутності законодавчих норм, які б спеціально регулювали застосування Smart-технологій під час надзвичайних або воєнних ситуацій. Наприклад, у багатьох країнах існують спеціальні положення, що дозволяють оперативним службам отримувати доступ до міських інфраструктурних даних у випадку надзвичайної ситуації. В Україні такі механізми часто не врегульовані належним чином, що ускладнює їх оперативне використання. В умовах воєнного стану це може призводити до затримок або неефективного використання технологій для захисту громадян.

Загалом запровадження правового регулювання у сфері інновацій дозволить сприяти активному розвитку стартапів та залученню міжнародних компаній для впровадження нових технологій у міську інфраструктуру. Важливим кроком є розробка законопроектів, які передбачатимуть механізми фінансування стартапів через державні гранти та інноваційні фонди.

Законодавчі ініціативи також повинні стимулювати дослідження і розробки (R&D) у сфері Smart-технологій, надаючи державну підтримку університетам та науково-дослідним установам. Це створить основу для розвитку науково-технічного потенціалу країни і дозволить впроваджувати новітні рішення у сфері безпеки міст.

Загалом, чинне законодавство не відповідає вимогам сучасних безпекових викликів. Для ефективного використання цих технологій необхідне створення єдиного законодавчого акту, гармонізація із міжнародними стандартами, удосконалення механізмів регулювання збору і обробки даних, а також встановлення чітких норм щодо їх використання в умовах надзвичайних ситуацій. Також важливо забезпечити державну підтримку для розвитку Smart-технологій і створити стимули для приватного сектору.

Можна підсумувати, що застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні потребує чіткого

законодавчого регулювання. Важливими кроками є оновлення нормативно-правової бази, забезпечення кібербезпеки, стимулювання приватно-державного партнерства, гармонізація національних законодавчих норм із міжнародними стандартами та розробка нових законодавчих ініціатив у сфері інновацій. Це дозволить не лише підвищити безпеку міст, але й сприятиме технологічному розвитку країни в цілому.

3.2. Рекомендації щодо застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні на регіональному рівні

В умовах воєнного стану в Україні особливу увагу потрібно приділити застосуванню Smart-технологій для посилення безпеки міст-мегаполісів на регіональному рівні. Впровадження інноваційних технологій може суттєво підвищити рівень безпеки, оптимізувати управління ресурсами та забезпечити ефективне реагування на загрози. У цьому контексті розробка рекомендацій щодо застосування Smart-технологій є важливим завданням для органів місцевого самоврядування, державних установ, підприємств та громади.

У сучасних умовах воєнного стану, які значною мірою впливають на функціонування українських міст-мегаполісів, зростає необхідність застосування Smart-технологій для посилення безпеки на регіональному рівні. Інноваційні рішення можуть суттєво підвищити рівень безпеки міст, полегшити управління інфраструктурою та сприяти швидшому реагуванню на надзвичайні ситуації. Нижче подано основні рекомендації щодо впровадження Smart-технологій на регіональному рівні для зміцнення безпеки в умовах воєнного стану.

1. Інтеграція систем відеоспостереження та аналітики. Однією з ключових Smart-технологій для посилення безпеки в умовах воєнного стану є система відеоспостереження з використанням сучасних аналітичних інструментів. Важливо впровадити технології, які не лише фіксують події, але й

дозволяють в режимі реального часу аналізувати інформацію та виявляти потенційні загрози. Це може включати:

- Використання штучного інтелекту (ШІ) для аналізу відеопотоків і автоматичного виявлення підозрілої активності;
- Системи розпізнавання облич для ідентифікації осіб, що можуть становити загрозу безпеці;
- Аналіз поведінкових моделей для запобігання можливим терористичним актам або іншим загрозам;
- Використання камер з високою роздільною здатністю для моніторингу критичних об’єктів інфраструктури.

Інтеграція таких систем на рівні регіональних центрів безпеки дозволить покращити контроль над ситуацією в містах і прискорити процес прийняття рішень у разі виникнення загроз.

2. Створення єдиної платформи для управління міськими Smart-системами. Для ефективного управління безпекою міст-мегаполісів необхідно впровадити єдину платформу, яка об’єднуватиме всі Smart-системи міста. Це дозволить центральним та регіональним органам влади оперативно отримувати інформацію з різних джерел, аналізувати її та взаємодіяти з іншими структурами безпеки.

Єдина платформа повинна включати такі функції:

- Інтеграція даних з відеокамер, датчиків руху, систем пожежної безпеки та інших пристроїв;
- Можливість обміну інформацією з поліцією, медичними службами та рятувальниками;
- Використання великих даних (Big Data) для аналізу криміногенної ситуації та передбачення можливих загроз;
- Забезпечення кібербезпеки платформи для запобігання кібератакам, які можуть паралізувати роботу критичної інфраструктури міста.

Така інтеграція допоможе зменшити кількість помилок та знизити час реагування на надзвичайні ситуації.

3. Використання інтелектуальних транспортних систем (ITS). В умовах воєнного стану та підвищеного навантаження на міську інфраструктуру інтелектуальні транспортні системи (ITS) можуть відігравати важливу роль у забезпеченні безпеки. ITS дозволяють управляти транспортними потоками, знижувати ризики аварій та підвищувати мобільність у містах. Зокрема, можна виділити такі рекомендації:

- Впровадження системи моніторингу трафіку для виявлення заторів та аварій, що можуть бути використані ворожими силами для створення хаосу;
- Використання інтелектуальних світлофорів, які адаптуються до поточного навантаження на дороги та дозволяють швидко евакуювати населення в разі загрози;
- Впровадження електронних систем управління громадським транспортом, які забезпечують безперебійне функціонування під час надзвичайних ситуацій;
- Інтеграція транспортних систем з іншими міськими Smart-системами для забезпечення комплексного підходу до управління містом.

Це допоможе не тільки знизити кількість інцидентів на дорогах, але й покращить координацію дій в умовах військових загроз.

4. Розвиток системи електронного оповіщення. Система електронного оповіщення є важливим елементом захисту міських мешканців під час надзвичайних ситуацій, зокрема в умовах воєнного стану. На регіональному рівні необхідно запровадити інноваційні системи оповіщення, які б дозволили оперативно інформувати населення про можливі загрози та заходи безпеки.

Основні характеристики таких систем мають включати:

- Можливість надсилання сповіщень на мобільні пристрої мешканців з інформацією про небезпеку та необхідні дії;
- Використання різних каналів зв’язку, зокрема SMS, мобільні додатки та системи оповіщення через соціальні мережі;
- Інтеграція з системами відеоспостереження та аналітики для автоматичного виявлення надзвичайних ситуацій;

- Підтримка роботи в умовах, коли частина інфраструктури може бути пошкоджена внаслідок військових дій.

Розвиток таких систем дозволить значно підвищити рівень захищеності населення та скоротити час реакції на виникнення небезпечних ситуацій.

5. Запровадження публічно-приватного партнерства для впровадження Smart-рішень. Для успішного впровадження Smart-технологій на регіональному рівні важливо залучати приватні інвестиції та створювати сприятливі умови для розвитку публічно-приватного партнерства (PPP). Це дозволить знизити навантаження на державний бюджет і водночас прискорити впровадження інноваційних рішень.

Для ефективної реалізації PPP на регіональному рівні варто впровадити такі заходи:

- Розробка нормативно-правової бази, яка регулюватиме взаємодію державних та приватних структур у сфері Smart-технологій;
- Запровадження податкових пільг для компаній, що інвестують у проекти, спрямовані на покращення безпеки міст;
- Створення спеціальних грантових програм для стартапів, які займаються розробкою рішень у сфері громадської безпеки;
- Впровадження механізмів державно-приватного співфінансування для реалізації масштабних проектів.

Це дозволить значно підвищити ефективність впровадження Smart-технологій та зменшити витрати з боку державного сектору.

6. Посилення нормативно-правової бази на регіональному рівні. Одним із головних викликів для впровадження Smart-технологій є відсутність достатньої нормативно-правової бази на регіональному рівні. Верховна Рада України вже працює над рядом законопроектів, але на рівні місцевих органів необхідно також розробити та ухвалити регіональні стратегії та нормативні документи, які б регулювали впровадження Smart-технологій для безпеки.

Рекомендації для посилення нормативно-правової бази включають:

- Розробка регіональних програм розвитку Smart-технологій із чітко визначеними цілями та етапами реалізації;
- Впровадження регіональних стандартів для впровадження технологій відеоспостереження, кібербезпеки та інтелектуальних транспортних систем;
- Створення місцевих робочих груп для моніторингу впровадження Smart-рішень і підготовки рекомендацій для центральних органів влади;
- Узгодження регіональних нормативних документів з національними стратегіями та міжнародними стандартами у сфері громадської безпеки.

Це дозволить підвищити рівень координації між місцевими та центральними органами влади та забезпечити комплексний підхід до вирішення проблем безпеки.

7. Залучення міжнародних організацій та грантових програм. У сучасних умовах Україна має можливість залучати підтримку міжнародних організацій для власного розвитку та повоєнного відновлення. По-перше, міжнародні організації надають фінансові ресурси, що дозволяють реалізовувати масштабні проекти. Грантові програми також сприяють технологічному обміну, завдяки чому українські міста отримують доступ до передових рішень та досвіду інших країн. Крім того, міжнародні партнери допомагають забезпечити стандартизацію та безпеку даних, що є критичним у умовах війни. Важливим аспектом є також політична підтримка та легалізація технологічних змін на міжнародному рівні.

8. Створення регіональних платформ для моніторингу та аналізу. Важливим є створення регіональних платформ для моніторингу та аналізу безпекових ситуацій. Такі платформи повинні об'єднувати дані з різних джерел, таких як системи відеоспостереження, датчики, сенсори та інформаційні системи. Це дозволить швидко реагувати на зміни в безпековій ситуації, проводити аналіз загроз та розробляти ефективні стратегії реагування.

9. Інтеграція систем безпеки. Важливою рекомендацією є інтеграція різних систем безпеки в єдину інформаційну мережу. Це дозволить органам

місцевого самоврядування та правоохоронним органам ефективно обмінюватися інформацією та координувати свої дії в умовах надзвичайних ситуацій. Наприклад, інтеграція системи оповіщення населення, відеоспостереження, контролю доступу та інших технологій може значно підвищити рівень безпеки в регіоні.

10. Використання аналітики даних. Аналіз даних є ключовим інструментом для підвищення безпеки. Використання алгоритмів машинного навчання та штучного інтелекту дозволить прогнозувати потенційні загрози на основі історичних даних та тенденцій. Регіональні адміністрації повинні впроваджувати аналітичні інструменти для оцінки ризиків та прийняття обґрунтованих рішень у сфері безпеки.

11. Розробка мобільних додатків. Розробка мобільних додатків для громадян може стати важливим елементом у системі безпеки. Ці додатки можуть використовуватися для оперативного оповіщення населення про небезпечні ситуації, надання інформації про безпечні маршрути, а також для збору даних про підозрілі дії. Окрім того, додатки можуть забезпечувати зв'язок між населенням та органами влади, що підвищить рівень взаємодії у сфері безпеки.

12. Освіта та підвищення обізнаності. Регіональні органи влади повинні реалізовувати програми з освіти та підвищення обізнаності населення щодо використання Smart-технологій у сфері безпеки. Це може включати тренінги, семінари та інформаційні кампанії, що сприятимуть розумінню важливості новітніх технологій та їхньої ролі у забезпеченні безпеки. Громадяни мають бути проінформовані про можливості, які надають Smart-технології, та способи їх використання у повсякденному житті.

13. Співпраця з приватним сектором. Співпраця з приватним сектором є важливим аспектом впровадження Smart-технологій. Регіональні органи влади повинні активно залучати приватні компанії до реалізації проектів у сфері безпеки, використовуючи моделі публічно-приватного партнерства. Це

дозволить забезпечити фінансування, доступ до новітніх технологій та експертизу в реалізації інноваційних рішень.

14. Забезпечення кібербезпеки. В умовах застосування Smart-технологій необхідно також приділяти увагу забезпеченню кібербезпеки. Регіональні органи влади повинні розробити та впровадити програми захисту інформаційних систем, які використовуються для управління безпекою міст. Це включає захист від кібератак, захист персональних даних та забезпечення безпеки комунікаційних мереж.

15. Створення міжвідомчих робочих груп. Для координації дій у сфері безпеки регіональні адміністрації повинні створити міжвідомчі робочі групи, до складу яких входитимуть представники різних органів влади, правоохоронних структур та інших зацікавлених сторін. Ці групи повинні займатися обміном інформацією, аналізом ситуації та розробкою спільних стратегій для підвищення безпеки в регіонах.

16. Розробка стратегій реагування на надзвичайні ситуації. Регіональні органи влади повинні розробити стратегії реагування на надзвичайні ситуації з урахуванням специфіки регіону та можливостей використання Smart-технологій. Ці стратегії повинні включати алгоритми дій у випадку загрози, механізми оповіщення населення та координації дій між різними службами.

17. Моніторинг і оцінка ефективності. Останньою, але не менш важливою рекомендацією є впровадження системи моніторингу та оцінки ефективності впровадження Smart-технологій у сфері безпеки. Регулярний аналіз результатів та зворотній зв'язок від населення дозволять коригувати стратегії та програми, підвищуючи їхню ефективність у забезпеченні безпеки міст.

Загалом, застосування Smart-технологій для підвищення безпеки міст-мегаполісів в умовах воєнного стану в Україні має стати пріоритетом для регіональних органів влади. Інтеграція новітніх технологій у систему безпеки, активне залучення населення та співпраця з приватним сектором можуть

суттєво поліпшити ситуацію з безпекою в містах, знизити ризики та покращити якість життя громадян.

Висновки до розділу 3

Перспективи удосконалення застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні є важливою темою, оскільки сучасні міста стикаються зі значними викликами в умовах збройного конфлікту. Розвиток та адаптація Smart-рішень може відіграти ключову роль у забезпеченні громадської безпеки, ефективному управлінні критичною інфраструктурою, моніторингу та попередженні загроз, пов'язаних як із фізичними, так і кібернетичними ризиками.

Попри численні виклики, розвиток Smart-технологій в Україні вже набрав обертів. Використання таких технологій не обмежується тільки великими містами, але й може бути застосоване в менш урбанізованих регіонах для забезпечення безпеки. Особливо це актуально в контексті підвищеної загрози диверсій, які можуть бути спрямовані на інфраструктуру поза межами великих міст.

У підрозділі 3.1 основні висновки стосуються необхідності вдосконалення законодавчої бази. По-перше, законодавство має бути адаптоване до реалій війни, де пріоритетом стає безпека громадян. Для цього слід ввести норми, що регулюватимуть впровадження та використання Smart-технологій для моніторингу і управління безпековими процесами в умовах підвищених загроз. Зокрема, рекомендується активне використання технологій штучного інтелекту для аналізу даних про потенційні загрози та автоматичне реагування на них. Слід також підвищити відповідальність місцевих органів за впровадження таких технологій і забезпечення їх ефективної інтеграції з державними структурами. На законодавчому рівні важливо впровадити стандарти для обробки, зберігання та обміну даними, що дозволить забезпечити безпеку конфіденційної інформації в умовах війни.

На законодавчому рівні впровадження Smart-технологій для посилення безпеки вимагає створення нових нормативно-правових актів та удосконалення чинної бази. Необхідно врахувати особливості воєнного стану, коли збільшується потреба в більш точних і швидких рішеннях для захисту інфраструктури та громадян. Рекомендації стосуються впровадження правових стандартів для забезпечення належної інтеграції технологій штучного інтелекту, великих даних та інших інструментів для безпеки в містах. Важливою є також координація державних і регіональних структур для ефективного застосування таких рішень.

У підрозділі 3.2 розглядаються рекомендації на регіональному рівні. Основна увага приділяється тому, що місцеві органи влади повинні мати достатню автономію у прийнятті рішень щодо впровадження технологій, але з урахуванням загальнонаціональних стандартів та рекомендацій. На регіональному рівні важливо розвивати партнерства з міжнародними організаціями та грантовими програмами для отримання фінансових і технічних ресурсів. Це дозволить містам швидше впроваджувати передові технології та адаптувати їх до своїх потреб. Важливим є також активне залучення громадян до процесу впровадження технологій через створення прозорих платформ для зворотного зв'язку та участі в управлінні міською безпекою.

На регіональному рівні важливо активніше залучати місцеві органи влади та приватні структури до впровадження Smart-технологій. Це дозволить підвищити ефективність захисту в конкретних умовах регіональних міст-мегаполісів. Рекомендації включають розробку локальних стратегій для інтеграції систем відеоспостереження, аналітичних платформ для моніторингу ризиків, та адаптації Smart-технологій до умов війни. Також необхідно залучати міжнародні організації та фонди для фінансової підтримки впровадження цих інновацій.

В підсумку, обидва підходи – як на законодавчому, так і регіональному рівнях – мають взаємодіяти для ефективного використання Smart-рішень.

Тема перспектив удосконалення Smart-технологій для посилення безпеки в умовах воєнного стану в Україні є важливою для забезпечення безпеки громадян та сталого функціонування критичних систем. Використання таких технологій надає можливості для підвищення ефективності управління безпекою в містах, мінімізації ризиків та своєчасної реакції на загрози. Успішна інтеграція Smart-рішень залежить від координації на державному та регіональному рівнях, а також підтримки міжнародної спільноти та донорів.

ВИСНОВКИ

У кваліфікаційній роботі висвітлено низку теоретичних, методичних і практичних аспектів щодо застосування Smart-технологій для посилення безпеки міст-мегаполісів в умовах воєнного стану в Україні. Основні результати дослідження знайшли відображення у наступних висновках:

1. Розкрито сутність Smart-технологій, їх основні риси та характерні властивості. Визначено, що ці технології спрямовані на інтеграцію цифрових систем для забезпечення ефективного управління безпекою в мегаполісах.

Smart-технології є важливою складовою концепції сучасних мегаполісів, які прагнуть забезпечити безпеку своїх громадян. Концепція безпеки міст повинна враховувати всі основні компоненти – фізичну, соціальну й кібербезпеку.

Розглянуто теоретичні засади дослідження Smart-технологій. Було з'ясовано, що Smart-технології мають широкий спектр застосування, спрямований на оптимізацію міської інфраструктури, підвищення ефективності управління містами та безпеки громадян. Їх ключові риси включають інтеграцію різних інформаційних систем та можливість використання великих даних і штучного інтелекту. Сучасний світ, що все більше глобалізується, відкриває нові можливості для впровадження таких технологій, проте викликає й нові виклики, особливо в умовах війни. Теоретичні засади безпеки мегаполісів базуються на створенні систем управління кризовими ситуаціями, превентивних технологіях моніторингу та прогнозування загроз.

2. Досліджено актуальні стратегії використання Smart-технологій у містах-мегаполісах світу та особливості їх впровадження в глобалізованому світі. З’ясовано, що в сучасних умовах такі рішення активно використовуються в різних сферах, включаючи безпеку міст, для моніторингу ситуацій у реальному часі, аналітики великих даних та швидкої реакції на загрози.

Сформульовано теоретичні засади посилення безпеки в містах-мегаполісах, зокрема через інтеграцію цифрових інструментів в управління громадською безпекою. Це включає автоматизовані системи моніторингу та управління транспортом, безпекові камери та IoT-рішення для контролю за міськими об'єктами.

Оцінено сучасний стан використання Smart-технологій для безпеки українських міст. Визначено, що найбільш активно ці технології впроваджуються в містах Київ, Львів та Харків, де функціонують системи відеоспостереження та автоматизовані платформи для моніторингу безпеки.

3. Проаналізовано правове регулювання застосування Smart-технологій у сфері безпеки. Досліджено стан та динаміку використання Smart-технологій для посилення безпеки в українських мегаполісах. Визначено, що незважаючи на значні успіхи у цій галузі, впровадження технологій відбувається нерівномірно. Нормативно-правове регулювання залишається складним аспектом через постійно змінювані умови воєнного стану.

Регулювання на національному рівні не завжди встигає за технологічним розвитком, що призводить до певних правових прогалин. Організаційно-економічні механізми застосування Smart-технологій вимагають удосконалення для забезпечення стійкості та ефективності використання у кризових умовах.

Досліджено нормативно-правові аспекти регулювання Smart-технологій під час воєнного стану. Виявлено, що поточна законодавча база не повною мірою відповідає потребам сучасних викликів, зокрема не врегульовано питання кібербезпеки та захисту персональних даних.

4. Проведено порівняльний аналіз досвіду країн, що використовують Smart-рішення. Наголошено на важливості міжнародного досвіду та співпраці в удосконаленні Smart-технологій. Акцент зроблено на адаптації кращих практик із західних країн до українських реалій для забезпечення високої якості безпекових послуг.

Успішне впровадження Smart-технологій в умовах воєнного стану можливе лише за умов синергії зусиль держави, регіональних органів та

міжнародних партнерів, а також за наявності чіткої стратегії розвитку та належного фінансування.

5. Розроблено рекомендації щодо інтеграції Smart-технологій у системи міського управління безпекою, серед яких:

- Інтеграція Smart-технологій у національні системи безпеки Подальше впровадження Smart-технологій для моніторингу, прогнозування та реагування на загрози національній безпеці. Наприклад, створення єдиної інтегрованої платформи на базі штучного інтелекту для аналізу великих обсягів даних про можливі загрози (наприклад, терористичні атаки, кібератаки, природні катастрофи).

- Розробка національних стандартів для впровадження Smart-технологій

Ухвалення стандартів, що регламентують використання Smart-технологій у критично важливих секторах, таких як енергетика, транспорт, медицина. Це сприятиме підвищенню ефективності використання таких технологій і зниженню ризиків їх неправильного застосування.

- Розвиток Smart-технологій для посилення кібербезпеки держави Активне впровадження інноваційних технологій, таких як блокчейн, криптографія та автоматизовані системи виявлення та нейтралізації кіберзагроз, для захисту національних баз даних, урядових систем та об’єктів критичної інфраструктури.

6. Визначено перспективи подальшого розвитку Smart-технологій у контексті зміцнення національної безпеки.

Рекомендації на законодавчому рівні включають необхідність розробки чітких регуляторних актів, що визначали б правові основи застосування Smart-рішень для забезпечення громадської безпеки та захисту стратегічних об'єктів. Зокрема, під час воєнного стану особливу увагу слід приділяти захисту даних і посиленню кібербезпеки. На регіональному рівні рекомендовано підвищувати координацію між місцевими органами влади та силовими структурами для ефективнішого реагування на потенційні загрози. Smart-технології можуть

допомогти покращити цей процес завдяки інтеграції систем моніторингу та аналізу даних у реальному часі.

Запропоновано рекомендації щодо вдосконалення законодавчого регулювання використання Smart-технологій в умовах воєнного стану. Визначено необхідність розробки чітких нормативних актів, які б забезпечували надійну кібербезпеку та захист критичної інфраструктури.

Рекомендовано створення регіональних центрів управління безпекою, які б об’єднували різні Smart-системи для моніторингу і реагування на загрози.

Наголошено на важливості міжнародного досвіду та співпраці в удосконаленні Smart-технологій. Акцент зроблено на адаптації кращих практик із західних країн до українських реалій для забезпечення високої якості безпекових послуг. Висновки підкреслюють, що успішне впровадження Smart-технологій в умовах воєнного стану можливе лише за умов синергії зусиль держави, регіональних органів та міжнародних партнерів, а також за наявності чіткої стратегії розвитку та належного фінансування.

Запропоновано рекомендації органам публічної влади України щодо роботи над впровадженням Smart-технологій для посилення безпеки міст-мегаполісів, зокрема:

- Розробка та впровадження загальнонаціональної стратегії використання Smart-технологій для безпеки міст.

Забезпечити розробку нормативно-правового документа, який визначить ключові принципи, напрямки та механізми впровадження Smart-технологій для посилення безпеки. Ця стратегія має враховувати сучасні виклики, зокрема загрози воєнного стану та кібератаки.

- Інтеграція Smart-технологій у системи міської інфраструктури. Прискорити модернізацію міських систем управління через впровадження технологій "розумного міста" (Smart City), таких як системи відеоспостереження з розпізнаванням облич, інтегровані платформи для управління даними та аналітики, а також автоматизовані системи реагування на надзвичайні ситуації.

- Посилення кібербезпеки у використанні Smart-технологій.

Розробити ефективні механізми захисту інформаційних систем, пов’язаних із Smart-технологіями. Залучити спеціалістів з кібербезпеки для створення захищених мереж обміну даними, особливо в умовах воєнного стану, де збільшується ризик кібератак на критичну інфраструктуру.

- Підвищення рівня цифрової грамотності серед управлінців та громадян.

Запровадити освітні програми для службовців органів місцевого самоврядування та широкої громадськості, щоб пояснити принципи використання Smart-технологій. Це сприятиме більшій ефективності їх впровадження та зменшенню опору змінам на місцевому рівні.

- Розширення публічно-приватного партнерства для впровадження Smart-технологій.

Створити механізми залучення інвестицій приватного сектора до проєктів із впровадження Smart-технологій. Це дозволить ефективніше реалізовувати інноваційні рішення для посилення безпеки, а також забезпечить сталий розвиток міської інфраструктури в умовах обмежених державних ресурсів.

Таким чином, у роботі визначено ключові напрями розвитку Smart-технологій для забезпечення безпеки міст в умовах воєнного стану. Незважаючи на значні виклики, такі технології є перспективним інструментом для підвищення ефективності управління безпекою, попередження загроз і захисту критичної інфраструктури, що має важливе значення для України в сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 7 принципів безпечного міста. Платформа розвитку міст. URL: http://urbanua.org/ideyi-i-proekty/koncepciyi-i-strategiyi/253 (дата звернення: 21.09.2024)

2. Smart city: технології «розумного міста» та їх цільове призначення. Everest.ua. 26.01.2021 URL: https://eukraine.org.ua/ua/news/smart-city-tehnologiyi-rozumnogo-mista-ta-yih-cilove-priznachennya (дата звернення: 21.09.2024)

3. SMART-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. Київ : Заповіт, 2021. 398 с. URL : https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf (дата звернення: 21.09.2024)

4. Аналіз загроз національній безпеці у сфері внутрішньої політики (експертне опитування). Національний інститут стратегічних досліджень. 2023. 30 с. URL: https://niss.gov.ua/sites/default/files/2023-07/ad_analiz-zagroz_14072023.pdf (дата звернення: 21.09.2024)

5. Андрієнко А. Оцінювання зрілості органів місцевого самоврядування великих міст України у сфері впровадження концепції «smart city» у повоєнний період. Вісник НТУ ДП. 2022. № 1. С. 59–70.

6. Андрієнко А.О. Упровадження концепції «Smart City» в управління великими містами України: монографія. Вінниця, Україна: ГО «Європейська наукова платформа». 2023. 196с. URL: https://publishing.logos-science.com/index.php/books/article/view/311/310 (дата звернення: 21.09.2024)

7. Антонюк І. В., Кошова С. П. Запровадження програм smart~city у великих містах: вітчизняний та зарубіжний досвід. 2021. Інвестиції: практика та досвід № 18. С. 99–107. URL:http://www.investplan.com.ua/pdf/18_2021/18.pdf (дата звернення: 21.09.2024)

8. Атаманова Н. В., Смирнов М. Д. Діджиталізація державноправової сфери в Україні. Актуальні проблеми вітчизняної юриспруденції. 2022. № 1. DOI: https://doi.org/10.32782/392233 (дата звернення: 21.09.2024)

9. Балашова Д. Urban fear. Страх і безпека у великому місті. 22.11.2023. URL: https://pragmatika.media/urban-fear-strakh-i-bezpeka-u-velykomu-misti/ (дата звернення: 21.09.2024)

10. Бобровський О. Смарт-технологізація публічного управління як рушійна сила його розвитку. Аспекти публічного управління. 2020. Том 8, спецвипуск № 1. С. 15–17. URL: https://aspects.org.ua/index.php/journal/article/download/747/723/ (дата звернення: 21.09.2024)

11. Бородін Є., Піскоха Н., Демошенко, Г. Проблеми і переваги цифровізації місцевого самоврядування. Аспекти публічного управління. 2021. № 9(4). С. 95–103. DOI: https://doi.org/10.15421/152141 (дата звернення: 21.09.2024)

12. Буряк Г., Йовдія Г. Цифрова держава: проблеми, інструменти їх вирішення та майбутнє Є-громадянина у Smart-місті. URL: https://zovu.org/digital-state-problems-tool/ (дата звернення: 21.09.2024)

13. Вербицький І., Пирогова Д., Грищенко М. Механізми участі громадян у процесі прийняття рішень органами міської влади у Києві. Cedos. 2018. URL: https://inlnk.ru/1PN9XY (дата звернення: 21.09.2024)

14. Воронкова В.Г., Романенко Т.П., Андрюкайтене Реґіна. Генеза від інформаційного суспільства до «smart-суспільства» в контексті історичної еволюції сучасного світу: теоретико-концептуальний контекст // Гілея: науковий вісник. Збірник наукових праць. К. : Вид-во «Гілея», 2017. Вип. 116 (1). С. 128–133.

15. Гаращук А. Безпека майбутього – у Ладижині поліція презентувала новітній «smart» простір. 27.03.2023. URL: https://vinnitsa.info/article/u-ladyzhyni-politsiya-prezentuvala-bezpeku-maybutn-oho (дата звернення: 21.09.2024)

16. Гончаренко І. Г., Слинько М. Ю. Оцінювання ступеня орієнтації регіонів України на смарт-спеціалізацію та інноваційний розвиток. Збірник

наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. 2020. № 59. С. 135–142.

17. Дащук Ю.Є, Лепкий М.І. Досвід використання smart-технологій в управлінні туристичним продуктом міста. Приазовський економічний вісник. Випуск 3(14) 2019. С. 294–299. URL: http://pev.kpu.zp.ua/journals/2019/3_14_uk/51.pdf (дата звернення: 21.09.2024)

18. Єршова О. Л., Бажан Л. І. Розумне місто – концепція, моделі, технології, стандартизація. Статистика України. 2020, № 2-3. DOI: https://doi.org/10.31767/su.2-3(89-90)2020.02-03.08 (дата звернення: 21.09.2024)

19. Жирак Р. М. Феномен життєстійкості як складова розвитку урбоекосистем. Сучасні проблеми архітектури та містобудування. 2022. Вип. 64. С. 179–193. URL : http://archinform.knuba.edu.ua/article/view/267479/263335 (дата звернення: 21.09.2024)

20. Жукович І. А. Smart-міста як новий об’єкт статистичних досліджень: визначення терміна. Статистика України. 2015. № 1. С. 18–22.

21. Захарова О. В., Федоренко Н. А., Деньга Л. М. Потенціал Черкаського регіону у запровадженні технологій смарт-спеціалізації. Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. Черкаси, 2021. Вип. 60. С. 30–40.

22. Карповець М. Місто як світ людського буття : монографія / М. Карповець. – Острог : Видавництво Національного університету «Острозька академія». 2014. – 258 с. URL: https://eprints.oa.edu.ua/id/eprint/4727/1/%D0%9A%D0%B0%D1%80%D0%BF%D0%BE%D0%B2%D0%B5%D1%86%D1%8C_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf (дата звернення: 21.09.2024)

23. Касич А. О., Федоряк Р. М., Собяніна А. П. Інноваційна технологія «SMART CITY» як механізм покращення рівня життя в сучасному місті.

Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент. 2017. Вип. 27. Ч. 1. С. 50–54. URL : http://www.vestnik-econom.mgu.od.ua/journal/2017/27-1-2017/13.pdf (дата звернення: 21.09.2024)

24. Корепанов О.С. Методологічні засади статистичного забезпечення управління розвитком «розумних» сталих міст в Україні. Дисертація на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.10 / Національна академія статистики, обліку та аудиту. Київ, 2018. 638

25. Корнійченко А. О. Співвідношення правових категорій «інформаційне суспільство» та «smart-суспільство». Наукові записки. Серія: Право. 2022. № 12. С. 90–94. URL: https://pravo.cusu.edu.ua/index.php/pravo/article/view/117/101 (дата звернення: 21.09.2024)

26. Кривоніс О. Розумні міста України. Що таке смарт-сіті і як це працює. 09.02.2022. URL: https://www.bezpeka-shop.com/ua/blog/obzor/umnye-goroda-ukrainy-chto-takoe-smart-siti-i-kak-eto-rabotaet/ (дата звернення: 21.09.2024)

27. Кунанець Н. Е., Небесний Р. М., Мацюк О. В. Особливості формування цілей соціальних та соціо-комунікаційних складових у проектах «smart city». Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2016. № 854. С. 257–274.

28. Максіменцева Н. О., Максімцев М.Г. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору Державне управління: удосконалення та розвиток. 2024. № 2. 33 с. URL: https://nayka.com.ua/index.php/dy/article/view/2992/3028 (дата звернення: 21.09.2024)

29. Малюков О. Теоретичні аспекти впровадження «розумних» технологій у діяльність органів місцевого самоврядування. Теорія та практика державного управління. 2019. Том 1, № 64 С. 178–186. DOI: https://doi.org/10.34213/tp.19.01.21

URL: https://periodicals.karazin.ua/tpdu/article/view/20667 (дата звернення: 21.09.2024)

30. Маматова Т. В., Андрієнко А. О. Концепція «розумної територіальної громади» в контексті забезпечення інтелектуалізованого місцевого розвитку. Децентралізація влади в Україні: оцінювання результатів формування та розвитку самодостатніх громад : монографія / за заг. та наук. ред. С. М. Серьогіна, І. А. Чикаренко. Дніпро : ДРІДУ НАДУ, 2019. С. 73–84.

31. Маматова Т., Кравцов О. Забезпечення якості публічних послуг в умовах цифрової трансформації. Publishing House «Baltija Publishing». 2021. № 7. DOI: https://doi.org/10.30525/978-9934-26-082-7-10 (дата звернення: 21.09.2024)

32. Маркевич К. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. / Видання, здійснене за підтримки Представництва Фонду Ф. Науманна за Свободу в Україні. Київ. Центр Разумкова. 2021. 399 с. URL: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf (дата звернення: 21.09.2024)

33. Матеріали Міжнародної науково-практичної конференції 19-20 грудня 2018 року Ред.-упорядник: д.філософ.н., проф. В. Г. Воронкова. Запоріжжя. Вид-во ЗДІА. 2019. 258 с. URL: https://old-zdia.znu.edu.ua/gazeta/MHPKzmist18ckc2.pdf (дата звернення: 21.09.2024)

34. Махначова Н.М. Інноваційний розвиток території на основі смарт-критеріїв. публічне управління і адміністрування в Україні. 2019. Випуск 11. С. 148–152. URL: https://ir.vtei.edu.ua/g.php?fname=26646.pdf (дата звернення: 21.09.2024)

35. Мойсенко В. Тенденції щодо доступності комерційних приміщень для маломобільних груп населення. 12.07.2024. https://propertytimes.com.ua/blogs/vira_moysenko/tendentsiyi_schodo_dostupnosti_komertsiynih_primischen_dlya_malomobilnih_grup_naselennya (дата звернення: 21.09.2024)

36. Мужанова Т.М. «Розумне місто» як інноваційна модель управління. Економіка. Менеджмент. Бізнес. 2017. № 2(20). С. 116–122. URL : http://journals.dut.edu.ua/index.php/emb/article/view/1515/1447 (дата звернення: 21.09.2024)

37. Мунько А.Ю. Поступ українських міст щодо реалізіції концепції smart-city в управлінських процесах. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. 2022. Том 33 (72) № 6. С. 161–166. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2022/6_2022/25.pdf (дата звернення: 21.09.2024)

38. Мураєв Є.В. Український досвід впровадження концепції смарт-міст: основні досягнення та проблеми. Вісник Хмельницького національного університету. 2020. №2, (280). С. 91–96. URL: http://journals.khnu.km.ua/vestnik/?p=843 (дата звернення: 21.09.2024)

39. Перелі Д. Місце смарт-технологій в системі публічного управління в Україні. Актуальні питання у сучасній науці. 2023. № 4(10). С. 141-150. URL: http://perspectives.pp.ua/index.php/sn/article/view/4323/4346 (дата звернення: 21.09.2024)

40. Перелі Д.Д. Концепція смарт-міста в умовах розвитку інформаційного суспільства. Публічне управління у сфері державної безпеки та охорони громадського порядку. 2023. Вип. 33. С. 136–140. URL: https://pag-journal.iei.od.ua/archives/2023/33-2023/25.pdf (дата звернення: 21.09.2024)

41. Перелі Д.Д. Формування концепції смарт-міст в системі публічного управління. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. Том 34 (73) № 4 2023. С. 46–51. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/4_2023/9.pdf (дата звернення: 21.09.2024)

42. Попов М., Комаровський І., Яценко В. Інформаційні системи та технології в публічному управлінні. Теоретичні та прикладні питання

державотворення. 2023. № 30. С. 35–46. URL: http://taais.oridu.odessa.ua/article/view/294963 (дата звернення: 21.09.2024)

43. Ревіталізація міст – досвід Європейського Союзу для України : навч. посібник / [О. А. Сич, Н. С. Ситник, А. В. Стасишин, В. В. Круглякова]; за заг. ред. канд. екон. наук., доц. О. А. Сич. Львів. ЛНУ імені Івана Франка. 2023. 312 с. https://financial.lnu.edu.ua/wp-content/uploads/2024/01/Revitalizatsiia-mist.pdf (дата звернення: 21.09.2024)

44. Розумна трансформація міст: безпечніше та комфортніше. Transparency International Ukraine. 23.02.2024. URL: https://ti-ukraine.org/news/rozumna-transformatsiya-mist-bezpechnishe-ta-komfortnishe/ (дата звернення: 21.09.2024)

45. Романовська Ю. Соціально-економічна безпека міста. Економічний часопис Волинського національного університету імені Лесі Українки. 2019. № 4, 20 (грудень). С. 82–92. DOI: https://doi.org/10.29038/2411-4014-2019-04-82-92 URL: https://echas.vnu.edu.ua/index.php/echas/article/view/508 (дата звернення: 21.09.2024)

46. Севастьянов Р. В. Актуальні проблеми розвитку «Розумних міст» (Smart city). Вісник Хмельницького національного університету. 2021. № 2. С. 170–175. URL : http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/08/2021-2-en-30.pdf (дата звернення: 21.09.2024)

47. Семенишин М. Диджиталізація українських громад: лідери цифрової трансформації обговорили можливості та перспективи. 17.03.2023. https://u-lead.org.ua/news/161?fbclid=IwAR1f53hBvrOjtboJsGaD0aMcPCnccPqzh9CDTpnh8cO_M9ndMHIAt-znd-k (дата звернення: 21.09.2024)

48. Слинько М. Ю. Нормативне підґрунтя реалізації смарт-спеціалазації в регіонах України. Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. 2021. Вип. 61. С. 75– 85.

49. Соколовська О.О. Smart City: використання інформаційно-комунікативних технологій у місцевому самоврядуванні. Аспекти публічного управління. Регіональне та муніципальне управління № 11-12 (13-14) листопад-грудень 2014. С. 77–84

50. Ткач С.М. Управління розвитком міст на засадах концепції Smart City у Західному регіоні України. Регіональна економіка. 2021. №2. С. 91-99. URL: https://re.gov.ua/re202102/re202102_091_TkachSM.pdf (дата звернення: 21.09.2024)

51. Тютюник В.В., Тютюник О.О. Усачов Д. В. Особливості створення системи акустичного моніторингу джерел надзвичайних ситуацій у контексті розвитку концепції «smart city». Науковий вісник: Цивільний захист та пожежна безпека. 2023. № 2 (16). С.58–76. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/19263/1/209-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-1188-1-10-20231214.pdf (дата звернення: 21.09.2024)

52. Участь представників Національного транспортного університету у Форумі «Розумне місто та технологічне оновлення України» (Smart Building Forum). 21.03.2024. URL: http://www.ntu.edu.ua/uchast-predstavnikiv-natsionalnogo-transportnogo-universitetu-u-forumi-rozumne-misto-ta-tehnologichne-onovlennya-ukrayini-smart-building-forum/ (дата звернення: 21.09.2024)

53. Чорток Ю. В., Євдокимова А. В., Нечипоренко Р. М., Майборода О. В. Зелені Smart-city в Україні: як поєднати реалії вітчизняного підприємництва та стандарти ЄС. Вісник СумДУ. Серія «Економіка». 2020. № 2. С. 126–132. DOI: https://doi.org/10.21272/1817-9215.2020.2-15 (дата звернення: 21.09.2024)

54. Чукут С. А., Дмитренко В. І. Смарт-сіті чи електронне місто : сучасні підходи до розуміння впровадження Е-урядування на місцевому рівні. Інвестиції : практика та досвід. 2016. № 13. С. 89–93. URL : http://www.investplan.com.ua/pdf/13_2016/17.pdf (дата звернення: 21.09.2024)

55. Чуль О. М. Концепція розбудови міст в рамках розвитку креативної економіки : методологічний та практичний аспект. Електронний журнал «Ефективна економіка». URL : http://www.economy.nayka.com.ua/?op=1&z=3348 (дата звернення: 21.09.2024)

56. Швець Г. Цифрова трансформація як фактор покращення національної безпеки України. 03.01.2024. https://censs.org/digital-transformation-as-a-factor-in-improving-the-national-security-of-ukraine/ (дата звернення: 21.09.2024)

57. Шестаковська, Т. Л. Аналіз тенденцій та викликів впливу цифрових технологій на публічне управління. Economic Synergy. 2023. № 2. С. 8–22. DOI: https://doi.org/10.53920/ES-2023-2-1 URL: https://es.istu.edu.ua/EconomicSynergy/article/view/116 (дата звернення: 21.09.2024)

58. Шлапак А., Іващенко О., Никонюк К. Соціальна безпека міста: зміст, фактори впливу та індикатори оцінювання. Економіка та суспільство. 2024. № 59. 6 с. DOI: https://doi.org/10.32782/2524-0072/2024-59-159 URL: https://economyandsociety.in.ua/index.php/journal/article/view/3511 (дата звернення: 21.09.2024)

59. Ягорі Я. Повітряні магістралі та небесні сади: як виглядатимуть міста майбутнього у 2030 році. 07.10.2023. https://www.epravda.com.ua/publications/2023/10/7/705036/ (дата звернення: 21.09.2024)

Документ підписано у сервісі Вчасно (продовження)
ННІНО_2024_281_Кумиков І.В..pdf

Документ відправлено: 00:42 20.12.2024
Документ отримано: 00:42 20.12.2024

Відправник документу

Отримувач документу

Електронний підпис
00:42 20.12.2024
Ідентифікаційний код: 2686200868
Кожина Алла Василівна
Власник ключа: Кожина Алла Василівна
Час перевірки КЕП/ЕЦП: 00:42 20.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 382367105294AF97040000001AA60D002ED32C03
Тип підпису: кваліфікований
Тип сертифікату: кваліфікований

Електронний підпис
13:01 20.12.2024
Ідентифікаційний код: 2869021966
ГЕЛИЧ АЛЛА ОЛЕКСАНДРІВНА
Власник ключа: ГЕЛИЧ АЛЛА ОЛЕКСАНДРІВНА
Час перевірки КЕП/ЕЦП: 13:01 20.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 5E984D526F82F38F04000000442597013B65A505
Тип підпису: удосконалений
Тип сертифікату: кваліфікований

Електронний підпис
13:34 23.12.2024
Ідентифікаційний код: 3423415916
Кумиков Ігор Вадимович
Власник ключа: Кумиков Ігор Вадимович
Час перевірки КЕП/ЕЦП: 13:34 23.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 382367105294AF9704000000777A150046E1AD02
Тип підпису: кваліфікований
Тип сертифікату: кваліфікований