ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

ФАКУЛЬТЕТ ПРАВА, ПУБЛІЧНОГО УПРАВЛІННЯ І МЕНЕДЖМЕНТУ

КАФЕДРА ПУБЛІЧНОГО УПРАВЛІННЯ ТА МЕНЕДЖМЕНТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Кібербезпека в системі публічного управління»

Здобувачка 4 курсу АПУАЗ групи
Освітньої програми:
Публічне управління та адміністрування
Спеціальності:
281 Публічне управління та адміністрування
Галузі знань:
28 Публічне управління та адміністрування
Ступеня вищої освіти: бакалавр
Полянська Анна Миколаївна

Використання чужих ідей,
Результатів і текстів мають посилання на відповідне джерело
_____Полянська А.М.

Науковий керівник:
доктор філософії з публ. управління та адміністрування, старший викладач
Кушко Ігор Сергійович

Розширена шкала _____
Кількість балів: _____ Оцінка: ECTS _____
Голова комісії _____ _____
(підпис) (ініціали, прізвище)
Члени комісії _____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)

м. Вінниця
2026 р.

АНОТАЦІЯ

Полянська А.М. Кібербезпека в системі публічного управління. 281 Публічне управління та адміністрування. Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, 2026 р.

Робота присвячена комплексному дослідженню теоретичних засад та практичних механізмів зміцнення кіберстійкості територіальних громад у сучасній системі публічного управління України. У дослідженні розкрито еволюцію поняття «кіберстійкість» як стратегічної характеристики держави, що визначає здатність публічних інституцій забезпечувати безперервність функціонування в умовах гібридної агресії та цілеспрямованих кібератак.

Проаналізовано нормативно-правову базу України та міжнародний досвід, що дозволило обґрунтувати необхідність гармонізації вітчизняного законодавства з вимогами Директиви NIS 2 та впровадження моделі «розподіленої відповідальності» на муніципальному рівні. Здійснено діагностику вразливостей інформаційних систем органів місцевого самоврядування в умовах воєнного стану, де ключовим ризиком визначено «людський фактор».

Наукова новизна роботи полягає у розробці авторського алгоритму реагування на кіберінциденти для територіальних громад, який поєднує технічні заходи з організаційними регламентами взаємодії між суб'єктами національної системи кібербезпеки. Запропоновано прикладні шляхи вдосконалення муніципального менеджменту через впровадження моделей публічно-приватного партнерства та формування системної культури кібергігієни серед службовців і мешканців громад.

Практичне значення отриманих результатів полягає у можливості їх використання органами місцевого самоврядування при розробці локальних стратегій цифровізації, положень про кіберзахист та планів безперервності діяльності.

Ключові слова: публічне управління, кібербезпека, кіберстійкість, територіальна громада, критична інформаційна інфраструктура, алгоритм реагування, кіберінцидент, цифрова трансформація, публічно-приватне партнерство, кібергігієна.

ABSTRACT

Polianska A. Cybersecurity in the System of Public Administration. 281 «Public Management and Administration». – Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, 2026.

The work is devoted to a comprehensive study of the theoretical foundations and practical mechanisms for strengthening the cyber resilience of territorial communities within the modern system of public administration in Ukraine. The research reveals the evolution of the concept of «cyber resilience» as a strategic characteristic of the state, which determines the ability of public institutions to ensure continuity of functioning in conditions of hybrid aggression and targeted cyberattacks.

The regulatory framework of Ukraine and international experience were analyzed, which allowed justifying the need to harmonize domestic legislation with the requirements of the NIS 2 Directive and the implementation of a «shared responsibility» model at the municipal level. A diagnosis of vulnerabilities in the information systems of local self-government bodies under martial law was carried out, where the «human factor» was identified as a key risk.

The scientific novelty of the work lies in the development of an original cyber incident response algorithm for territorial communities, which combines technical measures with organizational regulations for interaction between subjects of the national cybersecurity system. Applied ways of improving municipal management through the introduction of public-private partnership models and the formation of a systemic culture of cyber hygiene among officials and community residents are proposed.

The practical significance of the obtained results lies in the possibility of their use by local self-government bodies when developing local digitalization strategies, regulations on cyber protection, and business continuity plans.

Keywords: public administration, cybersecurity, cyber resilience, territorial community, critical information infrastructure, response algorithm, cyber incident, digital transformation, public-private partnership, cyber hygiene.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API (Application Programming Interface) – прикладний програмний інтерфейс.

Держспецзв'язку – Державна служба спеціального зв'язку та захисту інформації України.

ДЦКЗ – Державний центр кіберзахисту.

ЄС – Європейський Союз.

КІІ – критична інформаційна інфраструктура.

КСЗІ – комплексна система захисту інформації.

МСП – малі та середні підприємства.

НКЦК – Національний координаційний центр кібербезпеки при РНБО України.

НСК – Національна система кібербезпеки.

ОМС – органи місцевого самоврядування.

ПЗ – програмне забезпечення.

ППП – публічно-приватне партнерство.

РНБО – Рада національної безпеки і оборони України.

СБУ – Служба безпеки України.

ТГ – територіальна громада.

ЦНАП – центр надання адміністративних послуг.

BCP (Business Continuity Plan) – план забезпечення безперервності діяльності.

BYOD (Bring Your Own Device) – використання власних пристроїв для роботи.

CDTO (Chief Digital Transformation Officer) – заступник керівника з питань цифрової трансформації.

CERT-UA (Computer Emergency Response Team of Ukraine) – урядова команда реагування на комп'ютерні надзвичайні події України.

CISO (Chief Information Security Officer) – керівник (уповноважений) з питань інформаційної безпеки.

DDoS (Distributed Denial of Service) – розподілена атака типу «відмова в обслуговуванні».

DRP (Disaster Recovery Plan) – план аварійного відновлення.

IRP (Incident Response Plan) – план реагування на інциденти.

ISO (International Organization for Standardization) – Міжнародна організація зі стандартизації.

MFA (Multi-Factor Authentication) – багатофакторна автентифікація.

NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технологій США.

RDP (Remote Desktop Protocol) – протокол віддаленого робочого стола.

SLA (Service Level Agreement) – угода про рівень надання послуг.

SOC (Security Operations Center) – центр операцій із безпеки.

VPN (Virtual Private Network) – віртуальна приватна мережа.

ВСТУП

Актуальність теми. Трансформація парадигми державного управління в умовах глобальної цифровізації зумовила перехід від традиційних моделей надання адміністративних послуг до концепції «цифрової держави», де ефективність функціонування владних інституцій безпосередньо залежить від стабільності та захищеності інформаційно-комунікаційних систем. Для України, яка перебуває в стані повномасштабної збройної агресії з боку Російської Федерації, питання кібербезпеки перестало бути виключно технічним завданням IT-підрозділів і набуло статусу фундаментального пріоритету національної безпеки.

Особливої гостроти ця проблема набуває на рівні територіальних громад, які внаслідок реформи децентралізації отримали широкі повноваження щодо управління критичною інфраструктурою, ведення місцевих реєстрів та розпорядження значними масивами персональних даних мешканців. Проте, як свідчить практика, саме муніципальний сектор залишається найбільш вразливою ланкою в системі державного управління через обмеженість ресурсного забезпечення, дефіцит кваліфікованих кадрів та відсутність уніфікованих алгоритмів реагування на кіберзагрози.

Сучасні виклики, такі як цілеспрямовані атаки на системи життєзабезпечення, використання методів соціальної інженерії проти службовців та поширення дезінформації, вимагають від органів місцевого самоврядування переходу до стратегії кіберстійкості. На відміну від статичного захисту, кіберстійкість передбачає формування такої системи публічного управління, яка здатна адаптуватися до інцидентів, забезпечувати живучість критичних процесів та швидке відновлення після деструктивних впливів. Необхідність теоретичного переосмислення ролі органів місцевого самоврядування у загальнодержавній системі кібербезпеки та розробка прикладних інструментів зміцнення цифрового суверенітету громад зумовлюють вибір теми та актуальність даного дослідження.

Об’єкт дослідження – суспільні відносини у сфері публічного управління кібербезпекою та національною безпекою України на рівні територіальних громад в умовах цифрової трансформації та воєнних викликів.

Предмет дослідження – теоретико-методологічні засади, нормативно-правове регулювання, управлінські механізми та практичні інструменти забезпечення кіберстійкості територіальних громад як невід’ємного складника національної стійкості держави.

Мета дослідження полягає у комплексному теоретичному обґрунтуванні та розробці науково-практичних рекомендацій щодо вдосконалення механізмів публічного управління, спрямованих на зміцнення кіберстійкості територіальних громад, захист їхньої критичної інформаційної інфраструктури та підвищення загального рівня цифрової безпеки регіонів.

Завдання дослідження:

1. Розкрити теоретичний зміст поняття «кіберстійкість» у контексті публічного управління та визначити її ієрархічне місце в структурі національної безпеки держави.
2. проаналізувати стан нормативно-правового регулювання та міжнародний досвід (зокрема стандартів ЄС та НАТО) щодо забезпечення кібербезпеки на муніципальному рівні.
3. здійснити діагностику вразливостей інформаційних систем органів місцевого самоврядування в умовах воєнного стану та оцінити ефективність існуючих каналів взаємодії ОМС із державними інституціями.
4. запропонувати алгоритм реагування органів публічної влади на кіберінциденти, орієнтований на забезпечення безперервності функціонування критичних сервісів громади.
5. обґрунтувати шляхи оптимізації ресурсного забезпечення через впровадження публічно-приватного партнерства та розробку стратегії формування культури кібергігієни серед службовців і мешканців громад.

Методологічна основа дослідження. Основу даного дослідження становить комплексне використання діалектичного методу пізнання

суспільно-політичних явищ, що дозволило розглянути процеси формування кіберстійкості в системі публічного управління як динамічне явище, яке перебуває у постійному розвитку під впливом зовнішніх безпекових викликів та внутрішніх трансформацій державного апарату. Для досягнення об’єктивності та наукової достовірності результатів у роботі було застосовано систему спеціальних методів наукового пошуку:

— системно-структурний метод став базовим інструментом для ґрунтовного аналізу архітектури національної системи кібербезпеки як цілісного організму, що дало змогу чітко детермінувати ієрархічне місце та функціональну роль органів місцевого самоврядування у загальнодержавному контурі захисту критичної інформаційної інфраструктури.

— компаративістський (порівняльно-правовий) метод було задіяно для здійснення критичного зіставлення сучасного стану українського законодавства із передовими міжнародними стандартами, зокрема положеннями Директиви ЄС NIS2 та стратегічними концепціями країн-членів НАТО, що дозволило виявити прогалини у вітчизняному регулюванні муніципальної кібербезпеки та окреслити вектори його подальшої гармонізації.

— ризико-орієнтований підхід слугував методологічним підґрунтям для діагностики та класифікації вразливостей інформаційних систем органів місцевого самоврядування, що дозволило змістити фокус дослідження з опису технічних недоліків на оцінку реальних управлінських та соціальних загроз, які виникають в умовах воєнного стану.

— метод наукового моделювання був використаний як конструктивний інструмент для проектування авторських управлінських алгоритмів реагування на кіберінциденти, що забезпечило перехід від теоретичних роздумів до створення практично-орієнтованих регламентів діяльності органів публічної влади під час цифрових криз.

— методи синтезу та узагальнення застосовувалися на заключному етапі дослідження для агрегації отриманих результатів та формування

концептуальних висновків щодо стратегічних напрямів удосконалення публічного адміністрування у сфері зміцнення кіберстійкості громад, забезпечуючи цілісність та логічну завершеність роботи.

Наукова новизна отриманих результатів полягає у поглибленні теоретичних підходів до розуміння кіберстійності як динамічної характеристики публічного управління, а також у розробці авторського алгоритму інцидент-менеджменту для територіальних громад, який поєднує технічні заходи із організаційно-правовими регламентами взаємодії.

Практичне значення. Сформульовані в роботі пропозиції можуть бути використані органами місцевого самоврядування при розробці локальних стратегій цифровізації, положень про кіберзахист та планів безперервності діяльності. Результати дослідження сприятимуть налагодженню ефективної комунікації між громадами та суб'єктами національної системи кібербезпеки.

Апробація та впровадження результатів дослідження. Результати дослідження були апробовані на двох науково-практичних заходах у 2026 році: конференції «Глобальні виклики і сталий розвиток територіальних громад: досвід України» (31 березня) та Міжнародній конференції «Менеджмент у добу трансформацій: стратегічний, інноваційний та людський виміри» (24 квітня). Під час доповідей було обґрунтовано концептуальний підхід до кіберстійкості як стратегічного елемента публічного управління та фактора національної безпеки в умовах воєнного стану. Практичне впровадження напрацювань підтверджується розробкою та апробацією алгоритмів реагування на кіберінциденти та стратегічних розділів для муніципальних програм цифрової трансформації.

Структура роботи. Дипломна робота складається зі вступу, трьох розділів, дев'яти підрозділів, висновків до кожного розділу, загальних висновків та списку використаних джерел. Загальний обсяг роботи відповідає встановленим академічним вимогам.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1. Поняття «кіберстійкість» та її місце в структурі національної безпеки держави.

У сучасній теорії публічного управління трансформація безпекового середовища під впливом глобальної цифровізації зумовила перехід від статичних моделей захисту інформації до динамічної концепції забезпечення живучості державних інституцій. Центральним елементом цієї нової парадигми постає категорія «кіберстійкість», яка в контексті державного будівництва розглядається як критична спроможність системи публічного управління зберігати свою цілісність та функціональність в умовах перманентних деструктивних впливів у цифровому просторі. Для наукового аналізу даної проблематики необхідно першочергово здійснити дефініцію базових термінів, що складають методологічний фундамент дослідження [24, с. 50-55].

Фундаментальною категорією у цьому контексті є публічне управління у сфері кібербезпеки, під яким слід розуміти цілеспрямовану діяльність суб’єктів владних повноважень, спрямовану на формування та реалізацію державної політики, що забезпечує захищеність національних інтересів у кіберпросторі через нормативне регулювання, координацію зусиль державного та приватного секторів, а також ресурсне забезпечення систем захисту. Специфіка такого управління полягає у переході від суто технічного контролю до стратегічного менеджменту ризиків, де головним об’єктом стає не лише інформація, а й безперервність надання публічних сервісів громадянам.

Тісно пов’язаним, проте специфічним за своєю природою, є поняття кібербезпеки – це стан захищеності життєво важливих інтересів людини, суспільства та держави, при якому забезпечується сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища

шляхом своєчасного виявлення та нейтралізації загроз. В системі публічного управління кібербезпека виступає як необхідний базис, орієнтований на захист конфіденційності, цілісності та доступності даних (CIA-тріада).

Аналізуючи генезу поняття «кіберстійкість» у публічному управлінні, слід підкреслити, що воно є значно ширшим за класичне поняття захисту. Якщо традиційні підходи орієнтовані на створення бар'єрів для недопущення інциденту, то кіберстійкість виходить з аксіоми неминучості виникнення кризових ситуацій. [57].

У цьому контексті кіберстійкість слід розглядати не просто як сукупність технічних характеристик системи, а насамперед як стратегічну спроможність системи публічного врядування безперервно виконувати свої сервісні функції перед громадянами та бізнесом навіть у глибоко кризовий період. В умовах гібридної агресії спроможність органів влади швидко регенерувати втрачені цифрові функції стає важливішим показником ефективності управління, ніж спроба побудови абсолютно непроникної системи. Кіберстійкість виступає як адаптивний механізм державного управління, що дозволяє мінімізувати час простою державних сервісів та запобігти соціальному хаосу у разі масштабного збою.

Місце кіберстійкості в структурі національної безпеки держави визначається її роллю як фундаментального гаранта стабільності політико-адміністративної системи. В ієрархії національних інтересів забезпечення стійкості цифрових активів посідає пріоритетне місце, оскільки сучасна держава де-факто є цифровою платформою, на якій базуються всі інші процеси: від розподілу бюджетних коштів до управління оборонним потенціалом. Таким чином, кіберстійкість є невід'ємним складником державної безпеки, що забезпечує імунітет національного суверенітету від зовнішніх інформаційних та технологічних інтервенцій, гарантуючи при цьому стабільність надання публічних послуг як базову умову суспільної довіри. [18].

Аналізуючи генезу поняття «кіберстійкість» у публічному управлінні, слід підкреслити, що воно є значно ширшим за класичне поняття захисту. Для чіткого розмежування цих концептів доцільно навести порівняльну характеристику **(див. табл. 1.1)**.

Таблиця 1.1. Концептуальні відмінності між кібербезпекою та кіберстійкістю в публічному управлінні

Характеристика	Кібербезпека (традиційна)	Кіберстійкість (сучасні вимоги)
Основна мета	Запобігання проникненню та недопущення інциденту.	Забезпечення безперервності функцій за умови успішної атаки.
Ставлення до загроз	Акцент на створенні «непроникного» периметра.	Визнання неминучості інцидентів та готовність до них.
Механізм дії	Превентивний захист (бар'єри, фаєрволи).	Адаптивність, швидке відновлення та регенерація.
Об'єкт фокусу	Технічна цілісність інформаційних систем.	Живучість державних інституцій та критичних процесів.
Результативність	Відсутність зафіксованих зломів.	Мінімальний час простою та швидке повернення до роботи.

Джерело: складено автором на основі [24]

В умовах гібридної агресії спроможність органів влади швидко регенерувати втрачені цифрові функції стає важливішим показником ефективності управління, ніж спроба побудови абсолютно непроникної системи. У цьому аспекті кіберстійкість виступає як адаптивний механізм державного управління, що дозволяє мінімізувати час простою державних сервісів та запобігти соціальному хаосу у разі масштабного збою.

Місце кіберстійкості в структурі національної безпеки держави визначається її роллю як фундаментального гаранта стабільності політико-адміністративної системи. В ієрархії національних інтересів забезпечення

стійкості цифрових активів посідає пріоритетне місце, оскільки сучасна держава де-факто є цифровою платформою, на якій базуються всі інші процеси, від розподілу бюджетних коштів до управління оборонним потенціалом. Таким чином, кіберстійкість є невід'ємним складником державної безпеки, що забезпечує імунітет національного суверенітету від зовнішніх інформаційних та технологічних інтервенцій [16, с. 29-34].

Науковий підхід до класифікації кіберстійкості в системі національної безпеки дозволяє виділити три стратегічні рівні її реалізації в публічному управлінні. Перший рівень – інституційний, що передбачає стійкість самих органів державної влади, їх систем документообігу та прийняття рішень. Другий рівень – інфраструктурний, який охоплює захищеність енергетичних, транспортних та фінансових мереж, що перебувають у сфері регулювання публічної влади. Третій рівень – суспільний, що базується на довірі громадян до цифрових інституцій та здатності соціуму зберігати згуртованість в умовах інформаційних атак [26, с. 20-30].

Особливе значення в теорії публічного управління має взаємозв'язок кіберстійкості з категорією «національна стійкість». В межах концепції забезпечення національної стійкості України, кібернетичний компонент розглядається як «нервова система», пошкодження якої призводить до паралічу всього державного організму. Впровадження принципів кіберстійкості у діяльність суб'єктів публічної влади вимагає відмови від фрагментарного підходу на користь системного ризико-орієнтованого менеджменту. Це передбачає, що кожен керівник органу місцевого самоврядування чи державного відомства повинен розглядати кіберризики як невід'ємну частину загальних управлінських ризиків, що можуть вплинути на національну безпеку. Практична реалізація такого підходу потребує інтеграції безпекових параметрів безпосередньо у стратегічні документи планування розвитку громад **(приклад структури відповідного розділу стратегії наведено у Додатку А)**

Ефективність функціонування системи національної безпеки безпосередньо залежить від того, наскільки глибоко принципи кіберстійкості інтегровані в регламенти публічного адміністрування. Це включає створення резервних копій державних реєстрів, впровадження систем дзеркального відображення критичних даних та підготовку персоналу до роботи в умовах відсутності зв'язку. Управлінська модель кіберстійкості базується на принципі «неперервного вдосконалення», де кожен інцидент аналізується не лише як технічна помилка, а як прогалина в системі управління, що потребує негайної корекції нормативної бази чи організаційної структури [24, с. 50-56].

Підсумовуючи теоретичний аналіз, варто зазначити, що у структурі національної безпеки кіберстійкість виконує функцію стабілізуючого фактора, який запобігає трансформації локального кіберінциденту у масштабну національну кризу. Вона забезпечує «запас міцності» державного апарату, дозволяючи йому виконувати свої зобов'язання перед громадянами навіть у найбільш несприятливих умовах. Розвиток кіберстійкості, як об'єкта публічного управління є вимогою часу, оскільки в епоху мережевих воєн саме здатність до відновлення, а не лише до захисту, стає головною ознакою сильної та суверенної держави.

Отже, встановлено, що в сучасній науці публічного управління категорія «кіберстійкість» пройшла еволюційний шлях від вузькотехнічного параметра надійності інформаційних систем до рівня фундаментальної стратегічної характеристики національної безпеки держави. Встановлено, що ключовою відмінністю кіберстійкості від традиційної кібербезпеки є її орієнтованість на забезпечення життєздатності системи в умовах гарантованого виникнення загроз, що вимагає впровадження нових підходів до державного адміністрування, заснованих на принципах адаптивності та швидкого відновлення критичних функцій.

Обґрунтовано, що місце кіберстійкості в структурі національної безпеки є центральним, оскільки вона виступає базисним інструментом збереження керованості державою в умовах глобальної цифровізації та гібридних загроз.

Доведено, що публічне управління у цій сфері має базуватися на інтегрованому підході, який поєднує нормативно-правове регулювання, розвиток технологічної інфраструктури та формування культури цифрової відповідальності на всіх рівнях владної ієрархії.

Отже, без належного рівня кіберстійкості будь-яка стратегія цифрової трансформації публічного сектору створює критичні вразливості для суверенітету держави, що актуалізує необхідність розробки дієвих механізмів державного контролю та стимулювання суб'єктів критичної інфраструктури до підвищення їхньої резистентності. Таким чином, кіберстійкість слід розглядати як динамічний процес і ключовий показник спроможності системи публічного управління гарантувати сталий розвиток суспільства в умовах перманентних викликів інформаційної епохи.

1.2. Нормативно-правове регулювання кібербезпеки на муніципальному рівні: український та міжнародний досвід.

У сучасній архітектурі публічного управління нормативно-правове регулювання кібербезпеки на муніципальному рівні постає як багаторівнева система юридичних приписів, спрямованих на встановлення чітких правил гри, розподіл відповідальності та визначення стандартів захисту цифрових активів територіальних громад. Правове поле у цій сфері не є ізольованим, воно формується на перетині конституційного права, законодавства про місцеве самоврядування, інформаційного права та спеціалізованих актів у галузі національної безпеки.

Аналізуючи український досвід правового регулювання, слід зазначити, що тривалий час роль місцевого самоврядування у забезпеченні кіберстійкості залишалася на периферії уваги законодавця. Основним актом, що заклав фундамент національної системи, є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає органи місцевого

самоврядування, як повноправних суб'єктів забезпечення безпеки в кіберпросторі. Проте, публічне управління на місцях стикається з проблемою певної декларативності норм: закон покладає на громади обов'язок захищати свої ресурси, але часто не містить механізмів фінансового та методологічного забезпечення виконання цих обов'язків [54].

Важливим етапом стала Стратегія кібербезпеки України (2021–2025), яка вперше на рівні державної політики акцентувала увагу на децентралізації зусиль із кіберзахисту та необхідності створення регіональних центрів реагування на інциденти [56].

Для наочного порівняння вітчизняного підходу з провідними світовими практиками доцільно розглянути **таблицю 1.2.**

Таблиця 1.2. Порівняльна характеристика моделей нормативно-правового регулювання муніципальної кібербезпеки

Країна / Регіон	**Ключовий правовий інструмент**	**Основний управлінський підхід**	**Рівень муніципальної відповідальності**
Україна	ЗУ «Про основні засади забезпечення кібербезпеки»	Централізовано-декларативний	Суб'єкт системи, але з обмеженим фінансовим ресурсом.
Європейський Союз	Директива NIS2	Ризико-орієнтований імператив	Високий: обов'язковий аудит та звітність протягом 24 годин.
Естонія	Закон про кібербезпеку (стандарти ISKE)	Технологічна стандартизація	Чіткі технічні вимоги для кожного типу муніципальних даних.
США	Стандарти NIST та програми CISA	Грантове стимулювання	Пряма залежність фінансування від рівня відповідності стандартам.

Джерело: складено автором на основі [7, 8, 10, 49, 54, 53, 54, 56]

Особливе місце в системі джерел права займають підзаконні акти Кабінету Міністрів України, зокрема Постанова № 518, що затверджує Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Для публічного управління на рівні територіальних громад ці норми є імперативними, оскільки вони встановлюють мінімальні стандарти безпеки, яких повинні дотримуватися комунальні підприємства та виконавчі органи рад. Проте, реалізація цих вимог ускладнюється відсутністю спеціальних законів, які б адаптували загальнодержавні стандарти до специфічних потреб невеликих громад, що потребує розробки типових муніципальних регламентів кібергігієни та управління інцидентами [22].

Міжнародний досвід пропонує більш інтегровані та жорсткі моделі нормативного регулювання, де кібербезпека на муніципальному рівні розглядається як обов'язкова умова надання публічних послуг. Найбільш релевантною для України є Директива Європейського Союзу про заходи для високого спільного рівня кібербезпеки в межах Союзу (NIS2). Даний документ радикально змінює підходи до публічного управління, оскільки він прямо включає органи місцевого самоврядування та регіональні адміністрації до переліку «суттєвих» або «важливих» суб'єктів, що підлягають нагляду з боку державних регуляторів. Відповідно до NIS2, муніципалітети зобов'язані не лише впроваджувати технічні засоби захисту, а й проводити регулярні аудити ризиків, звітувати про інциденти протягом 24 годин та забезпечувати безпеку ланцюгів постачання цифрових продуктів [5].

Порівняльний аналіз показує, що в країнах з розвиненою демократією, таких як Естонія чи Німеччина, нормативне регулювання базується на принципі «спільної відповідальності» (Shared Responsibility). В Естонії, наприклад, Закон про кібербезпеку доповнюється детальними стандартами ISKE (трирівнева система захисту), де для кожного типу муніципальної інформаційної системи прописано конкретні правові та технічні вимоги. Це дозволяє публічним управлінцям на місцях уникати двозначності при плануванні бюджетів на IT-безпеку та забезпечує однорідність захисного

контуру всієї держави. У США регулювання на місцевому рівні здійснюється через грантові програми CISA, де фінансування громади напряму корелює з її відповідністю стандартам NIST (National Institute of Standards and Technology) [8].

Варто акцентувати увагу на тому, що в контексті євроінтеграції Україна має здійснити масштабну гармонізацію національного законодавства з нормами NIS2. Це вимагатиме внесення змін до Закону України «Про місцеве самоврядування», де необхідно чітко прописати повноваження громад у сфері кіберстійкості, визначити порядок створення муніципальних підрозділів з кібербезпеки та встановити правові підстави для фінансування заходів захисту з місцевих бюджетів. Публічне управління у цій сфері має еволюціонувати від формального дотримання інструкцій до створення живої екосистеми безпеки, де норма права стимулює розвиток технологій та компетенцій службовців [52].

Підсумовуючи, слід зазначити, що сучасна нормативно-правова база в Україні перебуває на стадії активного реформування. Головним викликом для публічного врядування є подолання розриву між високими стандартами, прописаними у стратегічних документах, та реальними можливостями їх імплементації на рівні територіальних громад. Створення дієвого правового механізму, який би поєднував державний контроль із муніципальною автономією, є ключовим фактором зміцнення кіберстійкості всієї системи національної безпеки [58, с. 490-491].

Отже, нормативно-правове регулювання встановлено, що формування ефективної системи кіберстійкості на муніципальному рівні неможливе без створення цілісної та несуперечливої юридичної архітектури, яка б гармонійно поєднувала національні інтереси з повноваженнями місцевого самоврядування. Визначено, що на сучасному етапі в Україні спостерігається перехід від декларативного визнання суб’єктності територіальних громад у кіберпросторі до встановлення конкретних імперативних вимог щодо захисту критичної інфраструктури, проте правові механізми реалізації цих вимог

потребують суттєвого доопрацювання в частині ресурсного забезпечення та методичного супроводу.

Доведено, що міжнародний досвід, зокрема імплементація директиви NIS2, є ключовим орієнтиром для реформування вітчизняного законодавства, оскільки він пропонує модель «розподіленої відповідальності» та встановлює жорсткі стандарти кібергігієни для органів публічної влади всіх рівнів. Обґрунтовано, що пріоритетним завданням публічного управління є розробка та впровадження локальних нормативних актів, які б деталізували загальнодержавні вимоги до специфіки муніципального врядування, перетворюючи кібербезпеку з факультативного завдання на обов'язковий стандарт якості надання адміністративних послуг. Таким чином, гармонізація українського правового поля із міжнародними стандартами є необхідною передумовою для побудови резистентної системи національної безпеки, здатної протидіяти викликам цифрової епохи.

1.3. Роль органів місцевої влади у забезпеченні стійкості критичної інформаційної інфраструктури громад

У системі сучасного публічного управління забезпечення живучості та безперебійного функціонування територіальних громад безпосередньо залежить від здатності органів місцевої влади гарантувати захищеність своїх цифрових активів. Роль органів місцевого самоврядування у сфері кіберстійкості трансформувалася з допоміжної технічної функції у стратегічний напрям муніципального менеджменту, оскільки саме на місцевому рівні зосереджені об'єкти, від яких залежить повсякденна життєдіяльність населення: системи водопостачання, енергомережі, медичні реєстри та сервіси надання адміністративних послуг.

Ефективна реалізація політики цифрової трансформації на місцевому рівні вимагає від органів влади не лише впровадження новітніх сервісів, а й створення надійної системи захисту базових процесів надання

адміністративних послуг. Для цілісного розуміння даного процесу та формування дієвої стратегії захисту необхідно оперувати базовими категоріями, що визначають суб'єктно-об'єктний склад управління критичною інфраструктурою, оскільки саме чітка ідентифікація елементів системи дозволяє уникнути управлінського хаосу під час кризових ситуацій [36, с. 27-28].

Центральним об'єктом прикладання управлінських зусиль у цій сфері є критична інформаційна інфраструктура (КІІ) громади, яка розглядається як складна сукупність об'єктів, зокрема інформаційних систем, електронних комунікаційних мереж та автоматизованих систем управління технологічними процесами, що забезпечують стабільне надання життєво важливих послуг у громаді, і порушення роботи яких може призвести до негативних наслідків для національної безпеки, економічної стабільності або здоров'я громадян на локальному рівні. Управління такими об'єктами вимагає особливого підходу, оскільки будь-яка деградація сервісів – від водопостачання до виплати соціальних допомог – миттєво трансформується із технічної проблеми в гостру соціально-політичну кризу [16, с. 29-34].

У цьому контексті пріоритетною якісною характеристикою системи стає стійкість об'єктів КІІ, що визначається як спроможність інфраструктурних систем зберігати свою цілісність, доступність та функціональну придатність навіть під час інтенсивних кібератак, а також здатність до максимально швидкого відновлення базових параметрів роботи після інциденту без втрати критично важливих даних. Стійкість не є статичним станом, а виступає динамічним показником ефективності публічного адміністрування, що базується на ризико-орієнтованому підході та впровадженні механізмів адаптації до нових типів загроз, які постійно еволюціонують в умовах гібридної агресії.

Ключову роль у забезпеченні життєдіяльності вказаних об'єктів відіграють суб'єкти публічного управління кіберстійкістю на місцях, до яких належать виборні органи місцевого самоврядування, виконавчі комітети,

профільні структурні підрозділи з питань цифровізації та керівники комунальних підприємств, які наділені законодавчими повноваженнями щодо формування та реалізації локальних політик захисту територіального кіберпростору. Взаємодія між цими суб'єктами становить організаційну основу кіберзахисту, де політична воля керівництва громади має поєднуватися з фаховою експертизою технічних спеціалістів та відповідальністю розпорядників критичних активів [30].

Розширення ролі вказаних суб'єктів передбачає не лише технічне обслуговування мереж, а й стратегічне планування ресурсів, розробку планів безперервності діяльності та налагодження горизонтальних зв'язків із державними інституціями кібербезпеки. Таким чином, гармонійне поєднання об'єктного захисту КІІ із професійною діяльністю суб'єктів управління дозволяє сформувати цілісну екосистему цифрової стійкості, яка здатна гарантувати безпеку мешканців громади та недоторканність їхніх цифрових прав у сучасному турбулентному середовищі [30].

Аналізуючи функціональне навантаження органів місцевої влади, слід підкреслити, що їх роль реалізується через комплексну модель управління ризиками, де пріоритетом є не лише технічний захист, а й організаційна готовність до криз. Публічне управління в цій сфері розпочинається з ідентифікації та категоризації об'єктів КІІ. Громада повинна чітко усвідомлювати, які саме цифрові вузли є критичними, наприклад, збій у системі електронного документообігу міської ради є серйозним інцидентом, проте вихід з ладу автоматизованої системи управління тиском у водопровідній мережі через кібервтручання є критичною загрозою життю мешканців. Таким чином, роль влади полягає у проведенні системного аудиту та веденні реєстру локальних об'єктів критичної інфраструктури відповідно до вимог національного законодавства.

Важливим аспектом діяльності органів місцевого самоврядування є координація взаємодії між державними інституціями та приватним сектором. Оскільки значна частина критичної інфраструктури часто належить

приватним компаніям, органи місцевої влади виступають інтегратором зусиль. Управлінська функція тут полягає у створенні майданчиків для обміну інформацією про загрози, спільному проведенні кібернавчань та розробці планів взаємодопомоги у разі надзвичайних ситуацій. Публічне управління у такому контексті перетворюється на сервісну функцію, що забезпечує «горизонтальну» стійкість громади через партнерство.

Окрему увагу в межах підрозділу варто приділити ресурсному забезпеченню та кадровому потенціалу. У сучасних умовах роль органів місцевої влади полягає у трансформації бюджетної політики громади: кібербезпека має розглядатися не як витратна стаття, а як інвестиція в безпеку. Це передбачає створення в штатах рад посад профільних фахівців з інформаційної безпеки, регулярне фінансування оновлення програмного забезпечення та впровадження систем моніторингу подій безпеки. Управлінський виклик тут полягає у подоланні «цифрового розриву» між великими містами та невеликими територіальними громадами, де брак ресурсів часто компенсується використанням хмарних технологій, що, у свою чергу, потребує нових правових регламентів взаємодії з хмарними провайдерами.

У контексті воєнного стану роль місцевої влади у забезпеченні стійкості КІІ набула екзистенційного значення. Організація диверсифікації каналів зв’язку, впровадження систем резервного живлення для серверного обладнання та забезпечення фізичного захисту об’єктів зв’язку – це пряма відповідальність муніципальних управлінців. Крім того, органи місцевого самоврядування відіграють ключову роль у забезпеченні «людського фактору» стійкості, через навчання службовців основам кібергігієни влада мінімізує ризики успішного застосування методів соціальної інженерії з боку агресора, що часто є початковою точкою атак на критичні системи.

Підсумовуючи, можна стверджувати, що роль органів місцевої влади є визначальною у формуванні низової ланки національної кіберстійкості. Без належної уваги до захисту інфраструктури громад на локальному рівні

загальнодержавна система безпеки залишатиметься вразливою. Публічне управління має забезпечити перехід від пасивної моделі очікування вказівок з центру до активної суб'єктності, де кожна громада розглядає свій цифровий простір як частину загальнонаціонального оборонного периметра, що потребує щоденного моніторингу, захисту та вдосконалення.

У ході теоретичного аналізу ролі органів місцевої влади було доведено, що місцеве самоврядування є фундаментальною ланкою в ієрархії забезпечення стійкості критичної інформаційної інфраструктури держави. Встановлено, що управлінська суб'єктність місцевої влади у цій сфері реалізується через триєдину функцію, ідентифікацію критичних активів, координацію міжсекторальної взаємодії та забезпечення безперервності надання публічних послуг в умовах деструктивних кібервпливів. Визначено, що ефективність реалізації цієї ролі прямо корелює з рівнем інтеграції кібербезпекових стандартів у щоденні процедури муніципального адміністрування.

Обґрунтовано, що в умовах воєнного стану та гібридних загроз роль місцевої влади трансформується у бік оперативного управління кризами, що вимагає не лише технічної оснащеності, а й високої управлінської гнучкості та здатності до швидкої адаптації регламентів діяльності. Виявлено, що ключовим бар'єром для повної реалізації потенціалу громад у сфері кіберстійкості залишається ресурсна асиметрія та дефіцит кваліфікованих кадрів, що актуалізує потребу в розробці нових механізмів державної підтримки та міжмуніципального співробітництва. Таким чином, зміцнення ролі місцевого самоврядування у сфері захисту КІІ є необхідною умовою для формування життєздатної моделі національної безпеки, здатної гарантувати стабільність держави «від громади до центру».

Висновки до розділу 1

У результаті проведеного теоретико-методологічного дослідження концептуальних засад забезпечення кіберстійкості в системі національної безпеки та публічного управління було сформульовано низку науково обґрунтованих висновків, що становлять базис для подальшого аналізу сучасного стану територіальних громад.

По-перше, встановлено, що в сучасній парадигмі публічного врядування категорія «кіберстійкість» еволюціонувала з суто технологічного параметра захищеності інформаційних систем до рівня фундаментальної стратегічної характеристики держави, що визначає спроможність її політико-адміністративної системи до самозбереження. На відміну від класичної кібербезпеки, яка фокусується на превентивних заходах та створенні бар'єрів для недопущення інцидентів, кіберстійкість у публічному управлінні базується на визнанні неминучості виникнення кризових ситуацій у цифровому просторі. Вона визначається як комплексна здатність суб'єктів владних повноважень передбачати загрози, витримувати деструктивні впливи, оперативно відновлювати критичні функції та адаптувати управлінські алгоритми до нових викликів, що забезпечує безперервність надання публічних послуг та збереження довіри громадян до інституцій влади.

По-друге, доведено, що місце кіберстійкості в структурі національної безпеки держави є центральним і системоутворюючим, оскільки в умовах тотальної цифровізації управлінських процесів будь-яка деградація цифрової інфраструктури автоматично призводить до підриву воєнної, економічної, соціальної та інформаційної безпеки. В управлінському аспекті кіберстійкість виступає як «горизонтальний» компонент, що пронизує всі рівні державної ієрархії та вимагає відходу від фрагментарного захисту окремих вузлів на користь побудови цілісної екосистеми живучості. Обґрунтовано, що національна безпека в цифрову епоху прямо залежить від здатності органів публічної влади мінімізувати час відновлення критичних реєстрів та систем

управління після успішних кібератак, що є критично важливим для збереження державного суверенітету в умовах гібридної агресії.

По-третє, аналіз нормативно-правового регулювання засвідчив, що в Україні сформовано базову юридичну архітектуру кібербезпеки, проте рівень її імплементації на муніципальному рівні залишається недостатнім через певну декларативність окремих норм та відсутність деталізованих регламентів взаємодії. Встановлено, що міжнародний досвід, зокрема впровадження Директиви ЄС NIS2, пропонує перспективну модель «розподіленої відповідальності», де органи місцевого самоврядування розглядаються як повноцінні та відповідальні суб'єкти забезпечення стійкості національної інфраструктури. Доведено, що гармонізація вітчизняного законодавства із європейськими стандартами вимагає чіткого законодавчого закріплення повноважень громад у сфері кіберзахисту, визначення джерел фінансування відповідних заходів та встановлення жорстких вимог до аудиту безпеки в муніципальному секторі.

По-четверте, визначено, що роль органів місцевої влади у забезпеченні стійкості критичної інформаційної інфраструктури (КІІ) громад є ключовою, оскільки саме на місцевому рівні здійснюється безпосереднє управління життєво важливими ресурсами та персональними даними мешканців. Публічне управління у цій сфері має зміщуватися від формального виконання інструкцій до активного ризико-орієнтованого менеджменту, що включає інвентаризацію критичних цифрових активів, розвиток кадрового потенціалу та створення локальних протоколів реагування на інциденти. Виявлено, що стійкість громади є не лише технічним завданням, а результатом ефективної координації між владою, приватним сектором та громадянським суспільством, де місцеве самоврядування виступає головним модератором безпекових процесів.

Зрештою, резюмовано, що подальший розвиток системи публічного управління у сфері кіберстійкості потребує інтегрованого підходу, який

поєднує нормативне вдосконалення, технологічну модернізацію та формування високого рівня кіберкультури серед службовців.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ВИКЛИКІВ КІБЕРСТІЙКОСТІ ТЕРИТОРІАЛЬНИХ ГРОМАД В УКРАЇНІ

2.1. Оцінка вразливості інформаційних систем органів місцевого самоврядування в умовах воєнного стану.

У сучасній системі публічного управління аналіз поточного стану кіберстійкості територіальних громад вимагає проведення критичної та системної оцінки вразливостей інформаційних систем, які в умовах повномасштабного воєнного стану перетворилися на об’єкти цілеспрямованої та перманентної агресії. Слід розуміти, що вразливість інформаційної системи органу місцевого самоврядування не вичерпується лише технічними недоліками у програмному коді чи застарілими апаратними рішеннями, вона являє собою складний організаційно-управлінський дефіцит, що за певних умов створює передумови для реалізації суб’єктом загрози несанкціонованого впливу на ресурси системи, що призводить до порушення конфіденційності, цілісності або доступності критично важливих муніципальних даних.

Для публічного адміністрування безпеки на місцевому рівні першочерговим етапом є ідентифікація того, що саме становить вразливість у конкретному контексті громади. Це внутрішня властивість інформаційної системи або середовища її функціонування, яка за відсутності належного контролю з боку публічних управлінців може бути використана зловмисником для здійснення деструктивного впливу. Оцінка таких прогалин дозволяє суб’єктам управління виявити слабкі ланки в архітектурі цифрового врядування та розробити адекватну стратегію їх нейтралізації, що є критично важливим для збереження керованості територією [34].

Особливе значення в умовах гібридної війни має аналіз потенційних шляхів проникнення, що визначаються як вектор атаки. Це конкретний шлях або засіб, за допомогою якого суб’єкт загрози отримує несанкціонований доступ до активів ОМС. Розуміння векторів атак дозволяє органам влади зміщувати акценти з пасивного захисту на активне управління периметром безпеки [30].

На основі проведеного аналізу, ключові недоліки, що загрожують стійкості громад, доцільно систематизувати у наступній таблиці:

Таблиця 2.1. Класифікація вразливостей інформаційних систем ОМС в умовах воєнного стану

Група вразливостей	Основні характеристики та прояви	Приклади ризиків для громади
Технологічні	Використання застарілого або неліцензійного ПЗ; відсутність оновлень (patch management); низька захищеність периметра.	Експлуатація вразливостей VPN/RDP для впровадження програм-вимагачів (ransomware).
Організаційно-процедурні	Відсутність регламентів доступу; незакріплена відповідальність у посадових інструкціях; відсутність планів безперервності.	Витік даних при роботі в режимі релокації або через використання особистих пристроїв (BYOD).
Людські	Низький рівень кібергігієни; вразливість до методів соціальної інженерії; психологічне виснаження персоналу.	Успішні фішингові атаки на посадовців, що стають «точкою входу» в муніципальну мережу.
Інфраструктурні	Фізична концентрація серверів; відсутність територіально рознесених резервних центрів.	Безповоротна втрата даних через фізичне знищення серверної кімнати під час обстрілів.

Джерело: складено автором самостійно.

Об’єктом захисту у цьому процесі виступає безпосередньо інформаційна система місцевого самоврядування, яка у науці публічного управління розглядається як складна організаційно-технічна система. Вона інтегрує в собі не лише технічні засоби та програмне забезпечення, а й бази даних та, що найважливіше, персонал, який забезпечує автоматизацію управлінських функцій на місцевому рівні. Саме людський чинник у цій системі часто

виявляється найменш стійким до маніпуляцій, що потребує впровадження жорстких протоколів кібергігієни [34].

Нинішня безпекова ситуація визначається як воєнний стан у кіберпросторі – особливий режим функціонування національної системи кібербезпеки. Він характеризується експоненціальним зростанням інтенсивності атак з боку державних та недержавних угруповань країни-агресора, чиї дії спрямовані на системне руйнування цифрової інфраструктури державного управління, викрадення персональних даних мешканців та масовану деморалізацію населення через блокування сервісів життєзабезпечення.

Оцінка вразливостей інформаційних систем органів місцевого самоврядування в умовах воєнного стану дозволяє виділити три основні групи критичних недоліків, що потребують негайного управлінського реагування. Перша група – технологічні вразливості, зумовлені використанням застарілого програмного забезпечення, відсутністю регулярних оновлень та низьким рівнем захищеності мережевого периметра. Багато громад досі використовують піратське або неліцензійне ПЗ, що містить відомі вразливості, які легко експлуатуються агресором для впровадження програм-вимагачів або шпигунського обладнання. Особливо критичною є вразливість систем віддаленого доступу (VPN, RDP), які впроваджувалися поспіхом для забезпечення дистанційної роботи працівників рад, часто без належної багатофакторної автентифікації [24, с. 60-70].

Друга група – організаційно-процедурні вразливості, що є наслідком недосконалості муніципального менеджменту. До них належать відсутність чітких регламентів доступу до персональних даних, незакріпленість відповідальності за кібербезпеку в посадових інструкціях та відсутність планів безперервності діяльності. В умовах війни, коли частина працівників змушена працювати в умовах релокації або з використанням власних пристроїв, ризик витоку інформації через незахищені домашні мережі зростає експоненціально. Публічне управління у таких випадках часто демонструє реактивний характер,

намагаючись усувати наслідки інциденту, замість того, щоб системно усувати процедурні прогалини [26].

Третя, і чи не найважливіша група – людські вразливості, пов’язані з низьким рівнем кібергігієни серед службовців. Аналіз свідчить, що більшість успішних атак на громади розпочиналися з фішингових розсилок, спрямованих на конкретних посадовців. В умовах психологічного тиску воєнного стану уважність персоналу знижується, що робить методи соціальної інженерії надзвичайно ефективними. Брак системного навчання працівників ОМС основам цифрової безпеки перетворює кожного користувача системи на потенційну «точку входу» для ворога [26].

Воєнний стан вніс суттєві корективи в архітектуру вразливостей громад. По-перше, з’явився фактор фізичного знищення інфраструктури, що призводить до втрати доступу до серверів та локальних копій даних. Якщо громада не забезпечила вчасний вивіз критичних даних у хмарні сховища або не створила територіально рознесених резервних центрів, вразливість «втрати доступності даних» стає фатальною. По-друге, спостерігається інтенсифікація атак на ланцюги постачання, де вразливість розробника муніципального софту стає вразливістю сотень громад одночасно.

Публічне управління кіберстійкістю вимагає впровадження методології безперервного моніторингу вразливостей. Це означає, що оцінка стану систем має бути не разовою акцією перед аудитом, а постійним процесом ідентифікації ризиків. Використання автоматизованих сканерів вразливостей у поєднанні з аналітикою від Держспецзв’язку та CERT-UA дозволяє ОМС діяти на випередження. Проте, на заваді стає хронічне недофінансування та дефіцит ІТ-спеціалістів у штатах сільських та селищних рад, що створює ситуацію «цифрової беззахисності» значної частини територій [31].

Аналізуючи сучасний стан вразливостей інформаційних систем органів місцевого самоврядування встановлено, що умови воєнного стану радикально змінили ландшафт кіберзагроз, висвітливши глибокі системні прогалини в цифровій стійкості громад. Доведено, що технічні вразливості, хоч і є

небезпечними, часто є лише похідними від організаційних недоліків публічного управління, зокрема відсутності системного підходу до менеджменту ризиків та ігнорування стандартів кібергігієни. Визначено, що найбільш критичною вразливістю залишається «людський фактор», який у поєднанні з методами соціальної інженерії та психологічним тиском війни стає основним вектором проникнення в муніципальні мережі.

Доведено, що для забезпечення належного рівня кіберстійкості органи місцевої влади повинні здійснити перехід від пасивної експлуатації систем до активної моделі управління вразливостями, яка базується на хмарних технологіях, регулярному аудиті та безперервному навчанні персоналу. Виявлено, що подолання існуючих вразливостей потребує не лише фінансових інвестицій, а й фундаментальної зміни управлінської культури, де кібербезпека визнається пріоритетним компонентом цивільного захисту населення. Таким чином, оцінка вразливостей є необхідним діагностичним інструментом, що дозволяє громадам сформувати адекватний план захисту критичної інформаційної інфраструктури в умовах перманентної загрози національній безпеці.

2.2. Механізми взаємодії органів місцевого самоврядування з державними інституціями

У сучасній архітектурі публічного управління забезпечення кіберстійкості територіальних громад неможливе без розбудови складної системи ієрархічних та горизонтальних зв’язків, оскільки механізми взаємодії органів місцевого самоврядування з державними інституціями становлять цілісну сукупність правових, організаційних та технологічних процедур, спрямованих на синхронізацію зусиль суб’єктів владних повноважень задля захисту національного кіберпростору [24].

В умовах воєнного стану ця взаємодія набуває ознак стратегічного партнерства, де органи місцевого самоврядування виступають первинною

ланкою збору даних про інциденти, а профільні державні установи забезпечують експертну підтримку, методологічне керівництво та координацію контрзаходів [12].

Центральним елементом цієї архітектури є функціонування національної системи кібербезпеки, під якою в публічному управлінні розуміють сукупність суб'єктів кібербезпеки та взаємопов'язаних заходів, що здійснюються ними із застосуванням відповідних методів і засобів у кіберпросторі з метою гарантування безпеки національних інтересів. Для системного розуміння того, як розподіляються ролі між учасниками цього процесу, нижче наведено класифікацію основних суб'єктів та векторів їхньої співпраці з муніципалітетами **(див. табл. 2.2)**.

Таблиця 2.2. Функціональна модель взаємодії ОМС із суб'єктами національної системи кібербезпеки

Суб'єкт взаємодії	**Основна роль у системі управління**	**Ключові інструменти та напрями взаємодії**
Держспецзв'язку	Головний регулятор та методолог системи.	Категоризація об'єктів критичної інфраструктури, впровадження єдиних стандартів захисту.
CERT-UA	Центральний сервісний хаб з реагування на події.	Інформаційний обмін (Threat Intelligence Sharing), оперативне сповіщення про кібератаки, технічна допомога.
Кіберполіція	Правоохоронний сегмент системи.	Розслідування кіберзлочинів, протидія соціальній інженерії, підвищення цифрової грамотності службовців.
Служба безпеки України (СБУ)	Контррозвідувальний захист.	Запобігання кібердиверсіям та терористичним актам, захист суспільно-

		політичної стабільності регіону.
НКЦК при РНБО	Координаційний та аналітичний центр.	Міжвідомчий діалог, формування національних стратегій, доступ до аналітики Big Data про загрози.

Джерело: складено автором на основі [7, 8, 10, 49, 54, 53, 54, 56]

У межах цієї системи взаємодія з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку) базується на впровадженні єдиних державних стандартів, де цей орган виконує роль головного регулятора та методолога. Для громад це означає необхідність дотримання регламентів, що визначають порядок категоризації об'єктів критичної інфраструктури, тобто таких систем та мереж, порушення роботи яких може спричинити серйозні наслідки для національної безпеки або соціально-економічного стану громади [26].

Операційним ядром такої співпраці виступає урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA), яка в системі публічного адміністрування виконує функцію центрального сервісного хаба. Взаємодія з CERT-UA реалізується через інформаційний обмін (Threat Intelligence Sharing), що являє собою процес систематичної передачі даних про індикатори компрометації, тактики та процедури хакерських угруповань [26].

Для місцевого самоврядування цей механізм є критичним, оскільки він дозволяє отримувати оперативні сповіщення про нові типи вірусів-шифрувальників або фішингові кампанії, що дає змогу впроваджувати превентивні заходи до моменту реальної атаки на муніципальні сервери.

Важливим компонентом публічного управління у цій сфері є залучення правоохоронного сегмента, де співпраця ОМС із Департаментом кіберполіції Національної поліції України дозволяє трансформувати технічний інцидент у юридично значущий процес розслідування. У цьому контексті кіберзлочин трактується як суспільно небезпечне діяння у кіберпросторі та з його

використанням, відповідальність за яке передбачена законом про кримінальну відповідальність. Взаємодія тут виходить за межі простої фіксації зламів, вона включає спільну діяльність щодо підвищення рівня цифрової грамотності службовців, що є ключовим інструментом превенції, оскільки більшість атак використовують «людський фактор» як точку входу в захищені мережі органів влади [26].

Водночас, безпекова вертикаль підсилюється через взаємодію з територіальними підрозділами Служби безпеки України, чия роль у системі публічного управління кіберстійкістю полягає у здійсненні контррозвідувальних заходів. Це передбачає захист від кібердиверсій, спрямованих на дестабілізацію суспільно-політичної обстановки в регіоні або підрив життєзабезпечення громад. ОМС у цій моделі виступають як суб'єкти, що забезпечують первинний моніторинг стану критичних систем та негайно інформують спецслужби про ознаки цілеспрямованих деструктивних впливів, що можуть свідчити про підготовку масштабних ворожих операцій у цифровому просторі [57].

Управлінська модель взаємодії на сучасному етапі еволюціонує в бік створення регіональних вузлів кібербезпеки під егідою Національного координаційного центру кібербезпеки (НКЦК) при РНБО України. НКЦК виступає робочим органом Ради національної безпеки і оборони України, який забезпечує координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку [31].

Для представників територіальних громад НКЦК є платформою для міжвідомчого діалогу, де муніципальні управлінці можуть брати участь у формуванні національних стратегій та отримувати доступ до передових аналітичних продуктів, що базуються на великих даних (Big Data) про стан кіберзагроз у всій державі.

Проте, незважаючи на наявність розвиненої інституційної структури, публічне управління стикається з викликом подолання «інформаційних бар'єрів», які часто виникають через надмірну бюрократизацію процесів

звітності. Механізми взаємодії потребують переходу від паперового документообігу до використання автоматизованих систем обміну даними про кіберінциденти, що дозволяє скоротити час реакції з годин до секунд. Це особливо важливо для громад, що знаходяться в зоні бойових дій або на прифронтових територіях, де кібератаки часто супроводжують фізичні обстріли об'єктів енергетики чи водопостачання, вимагаючи миттєвої координації між цивільними управлінцями, технічними спеціалістами та військовими [24].

Зміцнення кіберстійкості громад вимагає також імплементації механізмів публічно-приватного партнерства (ППП) у цифровій сфері. В публічному управлінні ППП розглядається як форма співробітництва між державними партнерами та приватними партнерами, що базується на об'єднанні їхніх ресурсів для досягнення суспільно значущих результатів. Для ОМС це відкриває можливість залучення експертизи провідних ІТ-компаній для проведення аудиту безпеки муніципальних систем, що дозволяє компенсувати кадровий голод у штатах місцевих рад. Державні інституції у цій схемі виконують роль гаранта безпеки та валідатора рішень, забезпечуючи, щоб залучення приватного сектору не створювало нових вразливостей для національних інтересів [46].

Таким чином, взаємодія органів місцевого самоврядування з державними структурами стає динамічною системою колективної оборони, де кожна громада стає повноцінним учасником загальнонаціональної мережі кіберстійкості. Ця мережа базується на принципі ешелонованого захисту, де невдача на рівні локальної безпеки одного ОМС має бути негайно компенсована ресурсами та досвідом центральних органів, не допускаючи каскадного поширення загрози на інші елементи державної інфраструктури. Тільки через поглиблення такої інтеграції та перехід до сервісно-орієнтованої моделі підтримки з боку держави можливо забезпечити реальну живучість територіальних громад перед обличчям гібридних загроз сучасності.

Отже, існуючі механізми взаємодії, можна стверджувати, що ефективність національної системи кібербезпеки прямо пропорційна якості інтеграції територіальних громад у єдиний інформаційно-аналітичний простір держави. Встановлено, що сучасна модель публічного управління у цій сфері базується на складному поєднанні жорсткої вертикалі підпорядкування у питаннях стандартів захисту з гнучкими горизонтальними зв'язками для оперативного обміну даними про загрози. Доведено, що ключовим фактором успіху такої взаємодії є діяльність спеціалізованих інституцій, як-от CERT-UA та НКЦК, які виконують роль «комунікаційних мостів», нівелюючи розрив між централізованою політикою безпеки та обмеженими ресурсними можливостями окремих органів місцевого самоврядування.

Обґрунтовано, що в умовах воєнного стану подальший розвиток взаємодії має відбуватися шляхом тотальної автоматизації процесів передачі індикаторів компрометації та створення регіональних центрів підтримки кіберстійності (Security Operations Centers), що дозволить перетворити ОМС із пасивних отримувачів інструкцій на активних суб'єктів спільного моніторингу. Виявлено, що подолання існуючих бюрократичних перепон та підвищення рівня взаємної довіри між різними рівнями публічної влади є невід'ємною передумовою для формування життєздатного кіберщита держави. Таким чином, налагоджені механізми взаємодії виступають не просто адміністративним інструментом, а стратегічним гарантом стабільності та неперервності функціонування публічної влади, забезпечуючи синергію зусиль усіх ланок державного апарату у захисті цифрового суверенітету України.

2.3. Ресурсне забезпечення кіберзахисту на рівні громад

У системі публічного управління реалізація стратегічних цілей щодо зміцнення національної безпеки безпосередньо залежить від якості та повноти ресурсного наповнення відповідних програм, оскільки ресурсне забезпечення

кіберзахисту на рівні громад становить сукупність фінансових, людських, технологічних та інформаційних активів, що залучаються органами місцевого самоврядування для створення та підтримки ефективного оборонного периметра в цифровому просторі. В умовах децентралізації та воєнного стану питання адекватності ресурсів набуває особливої гостроти, оскільки територіальні громади (ТГ) змушені самостійно балансувати між потребами гуманітарного сектору та необхідністю інвестування в дорогі технології захисту критичної інформаційної інфраструктури [24].

Першим і найбільш вагомим складником є фінансове забезпечення кібербезпеки, під яким у публічному адмініструванні розуміють процес акумулювання та цільового використання грошових коштів місцевих бюджетів, державних субвенцій та донорської допомоги для фінансування заходів із захисту інформації. Публічне управління у цій сфері стикається з проблемою «залишкового принципу» фінансування цифрових потреб, де витрати на кіберзахист часто розглядаються як необов'язкові. Проте, сучасна модель управління вимагає впровадження ризико-орієнтованого бюджетування, де обсяг виділених коштів прямо корелює з потенційними збитками від зупинки муніципальних сервісів або витоку персональних даних мешканців громади [26].

Технологічний компонент ресурсного забезпечення охоплює програмно-апаратні засоби кіберзахисту – сукупність технічних пристроїв (серверів, маршрутизаторів, фаєрволів) та спеціалізованого програмного забезпечення, що забезпечують технічну реалізацію політик безпеки. Для багатьох громад викликом є застарілість парку комп'ютерної техніки та використання програмних продуктів, що не мають підтримки розробника, що створює «технологічні діри» в безпеці. Публічне управління має орієнтуватися на впровадження моделі хмарних обчислень, що дозволяє громадам орендувати захищені потужності у сертифікованих провайдерів, мінімізуючи капітальні витрати на закупівлю власного дорогого обладнання [26].

Найскладнішим аспектом ресурсного забезпечення є кадрове забезпечення, що в контексті кіберстійкості визначається як наявність у штаті ОМС кваліфікованих спеціалістів, здатних здійснювати адміністрування систем захисту, моніторинг інцидентів та навчання персоналу. Враховуючи, що людський фактор залишається критичною вразливістю, для об'єктивної оцінки рівня знань та практичних навичок службовців доцільно використовувати спеціалізований інструментарій тестування **(див. Додаток Б)**

З огляду на викладене, критично важливим вектором модернізації кадрової політики в системі публічного управління є нормативне закріплення та практичне впровадження спеціалізованого індикатора кіберграмотності як предиктора професійної придатності посадових осіб. Даний індикатор має виступати не лише формальним критерієм оцінки, а бути інтегрованим як обов'язкова детермінанта у процедури щорічного оцінювання та атестації службовців місцевого самоврядування.

Така стратегічна трансформація дозволить перевести питання кібербезпеки з площини факультативних знань чи вузькоспеціалізованих навичок у категорію невід'ємної професійної компетенції сучасного управлінця, де рівень засвоєння стандартів цифрової гігієни та операційної стійкості безпосередньо корелюватиме з результатами службового просування. Впровадження цієї моделі забезпечує формування дієвого мотиваційного стимулу для безперервного інтелектуального самовдосконалення персоналу, стимулюючи перехід від пасивного дотримання інструкцій до проактивної участі у забезпеченні цифрового суверенітету громади.

Більше того, системна імплементація індикатора кіберграмотності дозволяє мінімізувати деструктивний вплив людського фактору, зокрема через суттєве зниження вразливості посадових осіб до методів соціальної інженерії, що є ключовим етапом у побудові архітектури цілісної системи кіберстійкості публічних інституцій. Таким чином, перевірка знань щодо алгоритмів

реагування на кіберзагрози та принципів безпечної обробки інформації має стати фундаментом для прийняття управлінських рішень щодо кадрового резерву та професійної легітимації керівного складу ОМС.

В Україні спостерігається значний «кадровий голод» на муніципальному рівні, оскільки конкуренція за фахівців із приватним сектором та центральними органами влади часто є нерівною. Публічне управління намагається розв'язати цю проблему через запровадження посад CDTO (Chief Digital Transformation Officer) на рівні громад, чиїм завданням є не лише цифровізація, а й стратегічне управління кіберризиками. Проте для малих територіальних громад, які мають критичний дефіцит фінансування, найбільш перспективним управлінським рішенням є перехід до моделі міжмуніципального співробітництва (Shared Services). Створення єдиних центрів кібербезпеки або спільних центрів моніторингу для кількох сусідніх територіальних громад дозволить ефективно використовувати обмежений кадровий ресурс, залучаючи одного висококваліфікованого спеціаліста для обслуговування цифрового контуру декількох ОМС одночасно [60].

Інтелектуальний ресурс також включає інформаційно-методичне забезпечення, тобто наявність актуальних баз знань, стандартів ISO/IEC 27001, регламентів та інструкцій, які адаптовані до потреб конкретної громади. Без належної документальної бази навіть найсучасніше обладнання не гарантує безпеки, оскільки відсутність чітких процедур доступу та реагування призводить до хаосу під час реальної кібератаки. Органи місцевого самоврядування мають виступати замовниками розробки локальних Положень про кіберзахист, які б чітко розподіляли відповідальність між технічними спеціалістами, керівниками підрозділів та рядовими користувачами систем [60].

Важливим, проте часто ігнорованим ресурсом є організаційний капітал, що проявляється у здатності ОМС до горизонтальної взаємодії. В умовах обмежених фінансів громади можуть застосовувати механізми міжмуніципального співробітництва, створюючи спільні центри обробки

даних або залучаючи одного профільного спеціаліста для обслуговування кількох сусідніх громад. Це дозволяє оптимізувати витрати та забезпечити рівномірний рівень захищеності територій. Крім того, значним ресурсом є міжнародна технічна допомога, де через грантові програми та проекти громади отримують доступ до ліцензійного ПЗ та професійних тренінгів [60].

Зміцнення ресурсного забезпечення потребує переходу до моделі інвестиційного управління, де кібербезпека сприймається як фундамент для залучення зовнішніх інвестицій у громаду. Інвестор не прийде в регіон, де цифрові реєстри власності чи системи управління енергетикою є вразливими до зламу. Таким чином, публічне управління має вибудовувати систему ресурсного наповнення кіберзахисту як безперервний процес модернізації, де фінансові вкладення, технологічні оновлення та розвиток людського капіталу перебувають у стані постійної синергії, забезпечуючи життєздатність громади в умовах глобальних цифрових викликів та воєнної агресії [24].

Отже, аналізуючи ресурсне забезпечення кіберзахисту на рівні громад можна зробити висновок, що критичний дефіцит фінансових та кадрових ресурсів залишається головним бар'єром на шляху до досягнення реальної кіберстійкості територіальних громад України. Встановлено, що існуюча модель фінансування «за залишковим принципом» не відповідає рівню актуальних загроз, що вимагає впровадження нових підходів до муніципального бюджетування, заснованих на оцінці ризиків та пріоритетності захисту критичної інформаційної інфраструктури.

Технологічне переоснащення громад має відбуватися не шляхом хаотичних закупівель обладнання, а через системний перехід на захищені хмарні сервіси та централізовані платформи моніторингу, що дозволить нівелювати нерівність у ресурсному забезпеченні великих міст та малих сільських громад. Виявлено, що інтелектуальний ресурс, виражений у методичній підготовці персоналу та наявності чітких регламентів, є найбільш доступним, проте найменш задіяним інструментом підвищення безпеки. Таким чином, ресурсна політика публічного управління у сфері кіберзахисту

має еволюціонувати від пасивного споживання бюджетних коштів до активного залучення донорської допомоги, розвитку партнерств та інвестування в людський капітал як головний гарант стійкості цифрового суверенітету громади.

Висновки до розділу 2

У результаті проведення системного аналізу сучасного стану та ідентифікації ключових викликів кіберстійкості територіальних громад України в умовах воєнного стану було сформульовано низку висновків, що відображають реальний стан захищеності цифрового простору на місцевому рівні та ефективність існуючих управлінських механізмів.

По-перше, здійснена оцінка вразливостей інформаційних систем органів місцевого самоврядування дозволила констатувати, що повномасштабна воєнна агресія радикально змінила ландшафт загроз, трансформувавши кіберпростір громад у повноцінну арену бойових дій, де цифрова інфраструктура муніципалітетів стала пріоритетною ціллю для деструктивних впливів. Встановлено, що критичний рівень вразливості зумовлений не лише технічними недоліками застарілого програмного забезпечення чи відсутністю ліцензійних засобів захисту, а насамперед глибокими організаційними прогалинами в системі публічного адміністрування. Доведено, що «людський фактор», підсилений методами соціальної інженерії та психологічним тиском війни, залишається найбільш критичною слабкою ланкою, через яку реалізується більшість успішних кіберінцидентів, що підкреслює необхідність переходу від суто техніцентричного захисту до соціотехнічної моделі управління безпекою, де кожен працівник ОМС розглядається як активний елемент оборонного контуру.

По-друге, аналіз існуючих механізмів взаємодії органів місцевого самоврядування з державними інституціями засвідчив наявність розвиненої, але подекуди надмірно бюрократизованої вертикалі координації, де ключову роль відіграють Держспецзв’язку, CERT-UA та НКЦК при РНБО. На стратегічному рівні взаємодія задекларована як пріоритетна, на операційному рівні громади часто стикаються з дефіцитом оперативної методичної підтримки та складністю процедур обміну інформацією про інциденти в реальному часі. Обґрунтовано, що ефективність національної системи

кібербезпеки прямо залежить від здатності державних органів перейти до сервісно-орієнтованої моделі підтримки громад, яка передбачає автоматизацію передачі індикаторів компрометації та створення регіональних центрів моніторингу, що дозволить нівелювати часовий розрив між виявленням загрози та її нейтралізацією.

По-третє, дослідження ресурсного забезпечення кіберзахисту на рівні громад висвітлило системну асиметрію між обсягом покладених на місцеве самоврядування завдань та реальною фінансово-кадровою спроможністю їх виконання. Встановлено, що хронічне недофінансування потреб цифровізації за «залишковим принципом» та критичний кадровий голод, зумовлений неконкурентністю публічного сектору на ринку праці ІТ-фахівців, створюють ситуацію «цифрового розриву», коли малі територіальні громади залишаються практично беззахисними перед професійними кіберугрупованнями. Доведено, що вихід із цієї ресурсної кризи полягає у впровадженні інноваційних управлінських рішень, таких як міжмуніципальне співробітництво, спільне використання хмарних технологій та активне залучення міжнародної технічної допомоги, що дозволяє оптимізувати видатки та забезпечити базовий стандарт безпеки для всіх територій, незалежно від їхнього бюджетного потенціалу.

По-четверте, резюмовано, що сучасний стан кіберстійкості громад України характеризується високим рівнем адаптивності в умовах криз, проте він все ще потребує переходу від реактивної моделі «гасіння пожеж» до проактивної стратегії ризико-орієнтованого управління. Виявлено, що головним викликом для публічної влади є необхідність одночасного забезпечення доступності електронних сервісів для громадян та гарантування найвищого рівня захисту персональних даних і реєстрів в умовах постійного фізичного та цифрового терору. Обґрунтовано, що кіберстійкість громади слід розглядати не як статичний стан захищеності, а як динамічну здатність політико-адміністративної системи до безперервного функціонування та

швидкої регенерації втрачених функцій, що є невід’ємною умовою загальної життєздатності держави.

Таким чином, зміцнення кіберстійкості територіальних громад потребує комплексного переформатування підходів до публічного управління, де технологічна модернізація має бути нерозривно пов’язана з нормативним удосконаленням, кадровим розвитком та розбудовою довірчих відносин між усіма рівнями влади та приватним сектором. Отримані висновки слугують аналітичним підґрунтям для розробки конкретних шляхів удосконалення публічного управління у сфері кіберстійності, що становить зміст заключного розділу дипломної роботи.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗМІЦНЕННЯ КІБЕРСТІЙКОСТІ ГРОМАД

3.1. Розробка алгоритму реагування органів влади на кіберінциденти у громаді

У межах удосконалення публічного управління у сфері цифрової безпеки особливого значення набуває формалізація процесів кризового менеджменту, оскільки алгоритм реагування органів влади на кіберінциденти у громаді становить собою послідовну сукупність адміністративних та технічних дій, спрямованих на своєчасне виявлення, локалізацію, усунення наслідків та розслідування деструктивних впливів у кіберпросторі громади.

Розробка такого алгоритму є необхідною умовою переходу від хаотичного реагування до системного інцидент-менеджменту[*], що дозволяє органам місцевого самоврядування мінімізувати операційні збитки та забезпечити безперервність надання публічних послуг навіть за умов успішної реалізації загрози.

Для забезпечення методологічної цілісності розроблюваного алгоритму та уніфікації управлінської діяльності в умовах кризових ситуацій необхідно впровадити в практику муніципального менеджменту чіткі дефініції, що визначають межі та зміст процесу реагування. Розуміння категоріального апарату дозволяє суб'єктам публічної влади діяти в єдиному інформаційному полі, уникаючи двозначності при прийнятті оперативних рішень [16, с. 29-35].

Центральною категорією, що ініціює запуск управлінських механізмів, постає кіберінцидент у громаді, який у системі публічного управління розглядається як подія або серія небажаних та непередбачуваних подій у кіберпросторі, що мають ознаки цілеспрямованої атаки, несанкціонованого втручання або масштабного технічного збою. Такі події безпосередньо призводять або створюють реальну загрозу порушення цілісності,

[*] Інцидент-менеджмент (управління інцидентами) – це процес виявлення, реєстрації, аналізу та оперативного усунення збоїв у роботі IT-сервісів або безпеки, спрямований на відновлення їх нормальної роботи та мінімізацію впливу на бізнес.

конфіденційності та доступності інформації в системах органів місцевого самоврядування чи комунальних підприємств, що забезпечують життєдіяльність території [18, с.17-23].

Для ефективної протидії таким викликам ключовим інструментом стає алгоритмізація реагування – це складний процес проектування та впровадження чітких посадових інструкцій, технологічних карт та формалізованих протоколів міжвідомчої взаємодії. Даний процес спрямований на детермінацію порядку дій кожного суб'єкта публічної влади з моменту первинної фіксації аномалії в системі, що дозволяє усунути суб'єктивізм та хаотичність у діях персоналу, перетворюючи реагування на злагоджений механізм інцидент-менеджменту.

Даний процес спрямований на детермінацію порядку дій кожного суб'єкта публічної влади з моменту первинної фіксації аномалії в системі, що дозволяє усунути суб'єктивізм та хаотичність у діях персоналу, перетворюючи реагування на злагоджений механізм інцидент-менеджменту **(деталізована операційна карта алгоритму представлена у *Додатку В*)**

Невід'ємним етапом стримування загрози є локалізація інциденту, під якою в контексті муніципального управління розуміють комплекс екстрених заходів, спрямованих на негайне обмеження зони деструктивного впливу кібератаки. Це передбачає застосування технічних та адміністративних важелів наприклад, фізичне або логічне відключення інфікованого сегмента мережі від інтернету, ізоляція скомпрометованих серверів, що здійснюється з метою запобігання каскадному поширенню загрози на інші критичні активи громади та збереження працездатності суміжних систем [26, с. 70-75].

Завершальним, проте стратегічно найважливішим елементом управлінського циклу є пост-інцидентний аналіз. Ця категорія визначається як обов'язкова управлінська процедура ретроспективного розбору причин виникнення інциденту, оцінки своєчасності та ефективності дій персоналу, а також ідентифікації прогалин у системі захисту. Результати такого аналізу слугують базою для внесення системних коректив у стратегію кіберстійкості

громади, забезпечуючи трансформацію негативного досвіду в інструмент зміцнення цифрового суверенітету муніципалітету.

Пропонований авторський алгоритм базується на міжнародному стандарті NIST SP 800-61 та адаптований до специфіки функціонування органів місцевого самоврядування в Україні. Він включає п’ять основних етапів, кожен з яких супроводжується конкретними управлінськими рішеннями [8].

Перший етап – виявлення та ідентифікація. Публічне управління на цьому етапі передбачає створення системи моніторингу та зворотного зв’язку, де рядовий працівник ради або автоматизована система повідомляють про аномальну роботу реєстрів. Роль ОМС полягає у призначенні відповідальної особи офіцера з кібербезпеки, яка проводить первинну верифікацію події та класифікує її за рівнем критичності для громади.

Другий етап – стримування та ізоляція. Метою цього етапу є «замороження» ситуації. Алгоритм передбачає негайне виконання технічних протоколів, зміну паролів адміністраторів, ізоляцію скомпрометованих серверів та створення «миттєвих знімків» системи для подальшого аналізу. Управлінське рішення на цьому етапі – переведення критичних служб громади на резервні канали або тимчасовий паперовий регламент роботи.

Третій етап – повідомлення та взаємодія. Відповідно до законодавства України, ОМС зобов’язані протягом визначеного часу повідомити про інцидент до CERT-UA та територіального підрозділу СБУ. Алгоритм регламентує форму та зміст такого повідомлення, забезпечуючи повноту даних для отримання зовнішньої допомоги. Публічне управління також передбачає розробку стратегії комунікації з мешканцями громади, щоб запобігти паніці у разі недоступності публічних сервісів [23].

Четвертий етап – елімінація та відновлення. Це етап очищення систем від залишків шкідливого програмного забезпечення та повернення до штатного режиму функціонування. Роль місцевої влади полягає у забезпеченні

контролю за цілісністю відновлених даних із резервних копій та тестуванні систем перед їх повним запуском у публічний доступ.

П’ятий етап – оцінка та вдосконалення. Це фінальна управлінська стадія, де за результатами інциденту готується звіт для голови громади та депутатського корпусу. На основі цього звіту приймаються рішення про виділення додаткового ресурсного забезпечення, зміну локальних нормативних актів або проведення позапланового навчання персоналу з питань кібергігієни [8].

Розроблений алгоритм може стати частиною плану безперервності діяльності громади, що затверджується рішенням сесії місцевої ради. Публічне управління кіберстійкістю через алгоритмізацію процесів дозволяє усунути фактор суб’єктивності та паніки під час реальної кризи. Крім того, наявність такого алгоритму є основою для проведення регулярних «кібернавчань», під час яких керівництво громади та технічні спеціалісти відпрацьовують сценарії реагування у формі штабних ігор [5].

Важливо, щоб алгоритм не був статичним документом, а постійно оновлювався з урахуванням нових векторів атак, таких як атаки на ланцюги постачання або використання штучного інтелекту зловмисниками. Тільки за умови детальної регламентації кожної дії – від моменту виявлення фішингового листа до повного відновлення бази даних ЦНАПу – органи місцевого самоврядування зможуть забезпечити реальну стійкість громади як невід’ємної частини цифрового суверенітету держави.

Отже, розробка алгоритму реагування на кіберінциденти встановлено, що формалізація управлінських процедур є критично важливим фактором мінімізації негативних наслідків кібератак для територіальних громад. Доведено, що впровадження чіткої послідовності дій – від ідентифікації загрози до пост-інцидентного аналізу – дозволяє органам місцевого самоврядування трансформувати реактивний підхід до безпеки у проактивну стратегію кіберстійкості. Запропонований алгоритм виконує роль не лише технічної інструкції, а й інструменту публічного управління, що забезпечує

скоординованість зусиль усіх суб’єктів місцевої влади та гарантує стабільність надання соціально значущих послуг у кризових ситуаціях.

Таким чином, ефективність функціонування алгоритму прямо залежить від його інтеграції в нормативно-правове поле громади та регулярного практичного відпрацювання персоналом, що дозволяє виявити та усунути прогалини в системі захисту до моменту реальної агресії. Отже, розробка та впровадження регламентованих протоколів реагування є дієвим шляхом удосконалення муніципального менеджменту, який перетворює кібербезпеку з абстрактного поняття на керований та прогнозований процес захисту інтересів мешканців громади в умовах сучасних гібридних викликів.

3.2. Впровадження моделей публічно-приватного партнерства для підвищення цифрової безпеки регіону

У сучасній теорії публічного управління концепція публічно-приватного партнерства у сфері кібербезпеки розглядається не просто як інструмент закупівлі послуг, а як стратегічна співпраця між органами державної влади чи місцевого самоврядування та суб’єктами приватного сектору, зокрема провідними ІТ-компаніями, операторами зв’язку та спеціалізованими аудиторськими фірмами. Таке співробітництво спрямоване на системне об’єднання обмежених бюджетних ресурсів, високих технологічних компетенцій та операційних ризиків задля проектування та підтримки стійкої цифрової екосистеми регіону.

Впровадження подібних моделей є об’єктивною необхідністю для територіальних громад України, оскільки нинішня динаміка розвитку кіберзагроз та швидкість оновлення інструментарію зловмисників значно випереджають спроможність класичного бюрократичного апарату до адаптації. Це зумовлює критичну потребу в залученні гнучких, інноваційних та масштабованих рішень, які традиційно притаманні приватному високотехнологічному бізнесу [41, с. 197-206].

Для ефективної імплементації інструментів партнерства в систему публічного управління на місцевому рівні необхідно, перш за все, чітко дефініціювати базові категорії, що регламентують ці відносини та створюють основу для прийняття управлінських рішень.

Фундаментальним поняттям у цьому контексті виступає безпосередньо публічно-приватне партнерство у сфері кібербезпеки, яке слід трактувати як юридично оформлене та інституційно стійке довгострокове співробітництво. У межах такої співпраці приватний партнер бере на себе чіткі зобов'язання щодо професійного проектування, впровадження або безпосереднього операційного управління складними системами захисту критичної інфраструктури громади. Взамін приватний суб'єкт отримує гарантовані фінансові виплати з місцевого бюджету або набуває право на надання додаткових комерційних послуг на базі створеної інфраструктури, що забезпечує баланс інтересів обох сторін [48].

Однією з найбільш затребуваних управлінських моделей у межах такого партнерства є аутсорсинг функцій безпеки, що в міжнародній практиці реалізується через залучення постачальників керованих послуг безпеки. Дана модель передбачає, що орган місцевого самоврядування передає найбільш трудомісткі та високотехнологічні функції, такі як безперервний моніторинг мереж, автоматизоване виявлення інцидентів та технічний захист периметра, зовнішній спеціалізованій компанії. При цьому критично важливо, що публічна влада не самоусувається від процесу, а зберігає за собою виключну відповідальність за політичне, стратегічне та нормативне управління, визначаючи рівень допустимих ризиків та пріоритети захисту муніципальних активів.

Вищим ступенем інтеграції ресурсів у регіональному вимірі є створення спільного центру операцій з безпеки. Дана структура функціонує як спеціалізований регіональний проектний офіс, де на спільних засадах державні службовці профільних департаментів та залучені приватні експерти здійснюють цілодобовий моніторинг кіберпростору громади чи області. Такий

підхід дозволяє нівелювати кадровий дефіцит у штатах місцевих рад, забезпечуючи доступ муніципалітетів до експертизи світового рівня та дороговартісного програмного забезпечення для аналізу великих даних про кіберзагрози [16, 29-35].

Наріжним каменем стійкості такої співпраці є принцип розподілу ризиків, який виступає головним регулятором ефективності ППП. Він передбачає встановлення солідарної відповідальності сторін за кінцеву результативність впроваджених заходів кіберзахисту. У цій архітектурі відносин приватний партнер несе прямі фінансові та репутаційні ризики за неналежну якість наданого сервісу або несвоєчасне реагування на атаку, тоді як публічний партнер відповідає за політичні наслідки перед громадою та виборцями у разі порушення цілісності критичних сервісів. Тільки за умови такого збалансованого розподілу обов'язків публічне управління здатне трансформувати потенційні загрози в контрольовані ризики, забезпечуючи реальну живучість цифрового простору громади.

Публічне управління пропонує декілька варіативних моделей впровадження ППП, адаптованих до потреб цифрової безпеки регіону. Першою є консультативно-інформаційна модель, що базується на створенні регіональних кіберхабів або консультаційних рад, де місцевий ІТ-бізнес надає органам влади безкоштовну експертизу, бере участь у розробці стратегій розвитку громади та проводить безоплатні тренінги для держслужбовців. Така модель не потребує значних бюджетних витрат і є ідеальною точкою входу для невеликих громад, що прагнуть розпочати діалог з бізнесом [41, с. 197- 206].

Другою, більш складною, є сервісна модель. В межах цієї моделі громада не закуповує дороге обладнання та ліцензії, а купує «результат» – захищений периметр мережі. Приватний партнер інвестує власні кошти у розгортання інфраструктури захисту, а громада виплачує щомісячні платежі за фактично отримані послуги безпеки. Це дозволяє ОМС уникнути капітальних витрат та

перейти до операційних витрат, що є значно ефективнішим з погляду муніципального бюджетування в умовах дефіциту коштів [18].

Третя модель – інноваційно-інвестиційна, що передбачає спільне будівництво регіональних центрів обробки даних або систем «Безпечне місто». У цій моделі приватний партнер використовує інфраструктуру для надання послуг бізнесу, одночасно забезпечуючи захищене зберігання державних реєстрів та відеоданих на пільгових умовах для громади. Такий синергетичний підхід дозволяє перетворити кібербезпеку з «витратної статті» на драйвер технологічного розвитку регіону [18].

Основним бар'єром для впровадження ППП у сфері кібербезпеки залишається проблема довіри та конфіденційності. Публічне управління має розробити чіткі угоди про рівень послуг (SLA – Service Level Agreement) та угоди про нерозголошення (NDA), які б гарантували державі збереження контролю над суверенними даними. Важливим кроком є також вдосконалення процедур публічних закупівель, оскільки традиційні тендери часто орієнтовані на найнижчу ціну, що є неприпустимим у питаннях безпеки [24, с. 68].

Впровадження моделей ППП дозволяє вирішити ключову проблему публічного управління – «інтелектуальний розрив». Залучаючи кращі таланти з приватного сектору, громада отримує доступ до технологій штучного інтелекту для аналізу загроз, передових систем шифрування та досвіду відбиття складних атак. Таким чином, ППП стає не просто фінансовим інструментом, а механізмом трансформації управлінської культури, де держава та бізнес усвідомлюють спільну відповідальність за цифровий суверенітет України на рівні кожної окремої громади.

Підсумовуючи розгляд моделей публічно-приватного партнерства, слід констатувати, що залучення приватного сектору до зміцнення кіберстійкості громад є безальтернативним шляхом модернізації системи публічного управління в умовах обмежених ресурсів та постійної еволюції загроз. Встановлено, що перехід до сервісних моделей безпеки та створення спільних центрів моніторингу дозволяє органам місцевого самоврядування подолати

кадровий дефіцит та технологічну застарілість систем захисту. Доведено, що успіх ППП залежить від здатності влади сформувати чітке правове поле та прозорі механізми розподілу ризиків, де приватний партнер виступає не просто постачальником послуг, а стратегічним союзником у забезпеченні національної безпеки.

Отже, впровадження ППП сприяє формуванню в регіоні стійкої інноваційної екосистеми, де кібербезпека стає фундаментом для цифрового розвитку територій та підвищення інвестиційної привабливості громад. Виявлено, що подолання психологічних та бюрократичних бар'єрів у відносинах «влада – бізнес» є необхідною передумовою для побудови дієвого кіберщита, здатного функціонувати в умовах воєнного стану та гібридної агресії. Таким чином, публічно-приватне партнерство слід розглядати як ключовий управлінський інструмент зміцнення кіберстійкості, що забезпечує синергію державних інтересів та приватних технологічних можливостей задля захисту цифрового суверенітету регіону.

3.3. Формування культури кібергігієни серед службовців органів місцевого самоврядування та мешканців громади як інструмент превенції загроз

У сучасній архітектурі національної безпеки перехід до людиноцентристської моделі захисту інформаційного простору обумовлює необхідність системного формування культури кібергігієни. В межах публічного управління цей процес розглядається як цілеспрямований та безперервний виховання стійких навичок безпечної поведінки в цифровому середовищі як серед суб'єктів владних повноважень, так і серед безпосередніх отримувачів публічних сервісів. Культура кібергігієни не є статичним набором знань, а постає як динамічний інструмент превенції загроз, що дозволяє суттєво мінімізувати ризики, пов'язані із соціальною інженерією, фішингом та іншими методами психологічного впливу. Це набуває критичного значення, оскільки, за даними аналітичних звітів, людський фактор та маніпулятивні

техніки становлять понад 80% первинних векторів атак на інформаційні системи територіальних громад.

Для забезпечення наукової обґрунтованості освітньо-управлінської діяльності в громаді необхідно впровадити в практичний обіг категорію кібергігієни (Cyber Hygiene). Вона визначається як сукупність базових правил, щоденних практик та стійких звичок, спрямованих на підтримання безпеки комп'ютерних систем, мереж та персональних даних. Подібно до правил особистої гігієни в реальному житті, ці заходи мають виконуватися користувачами на регулярній, системній та майже несвідомій основі, створюючи первинний бар'єр для потенційних зловмисників [34].

Основним викликом для безпеки громади залишається соціальна інженерія, яка являє собою складну сукупність методів маніпуляції свідомістю та поведінкою людини через обман, залякування або штучне створення атмосфери довіри. Зловмисники використовують ці техніки для експлуатації «людської вразливості» з метою отримання несанкціонованого доступу до конфіденційної інформації органів місцевого самоврядування. В умовах воєнного стану психологічний тиск на службовців посилюється, що робить превентивну роботу в цьому напрямі життєво необхідною для збереження цілісності муніципальних реєстрів [30].

Відповідно, превенція загроз у публічному управлінні постає як стратегічний напрям діяльності, орієнтований на випередження виникнення інцидентів шляхом усунення їхніх глибинних першопричин. Головним інструментом такої превенції є системне підвищення рівня цифрової грамотності як населення, так і службовців, що дозволяє трансформувати громаду з пасивного об'єкта атаки на активний суб'єкт кіберзахисту. Ефективність цієї стратегії безпосередньо залежить від того, наскільки якісно сформована кіберкультура організації – сукупність спільних цінностей, переконань та патернів поведінки працівників ОМС. Саме ця культура визначає реальне ставлення персоналу до вимог безпеки та їхню внутрішню

готовність неухильно дотримуватися регламентів захисту інформації, навіть у стресових ситуаціях [33].

Розширення масштабів навчання та впровадження програм із кібергігієни дозволяє органам місцевої влади створити так званий «людський фаєрвол». Це передбачає не лише технічну підготовку, а й зміну управлінської парадигми, де кожен працівник усвідомлює власну відповідальність за цифрову стійкість всієї громади. Тільки через інтеграцію кібергігієни в щоденну діяльність публічного сектору можливо забезпечити реальну живучість демократичних інституцій в епоху тотальної цифровізації та постійних гібридних викликів [50].

Публічне управління кіберстійкістю на рівні громади має розпочинатися з трансформації внутрішньої корпоративної культури муніципалітету. Основним управлінським інструментом тут виступає система безперервного навчання (Lifelong Learning), яка відходить від формальних інструктажів на користь інтерактивних методів. Пропонована стратегія включає впровадження обов’язкових симуляцій фішингових атак, під час яких службовці отримують тестові повідомлення, а за результатами їхніх дій проводиться індивідуальна корекційна робота. Це дозволяє сформувати «цифровий імунітет» та критичне мислення при роботі з електронною поштою та соціальними мережами.

Важливим кроком є інтеграція вимог кібергігієни в посадові інструкції та кодекси етики державних службовців і працівників ОМС. Публічне адміністрування має забезпечити створення системи стимулів, де дотримання правил багатофакторної автентифікації, регулярної зміни паролів та заборони використання сторонніх носіїв інформації стає невід’ємною частиною професійної атестації. Тільки через перетворення технічних правил на етичні норми можна досягти реальної зміни поведінкових моделей у бюрократичному середовищі [18].

Другим вектором публічного управління є робота з мешканцями громади, які є активними користувачами муніципальних сервісів. Громада, в якій мешканці розуміють ризики передачі своїх даних третім особам, є значно

стійкішою до кіберзагроз. Роль місцевої влади полягає в організації муніципальних інформаційних кампаній, створенні цифрових хабів на базі бібліотек чи ЦНАПів, де люди похилого віку та молодь можуть отримати базові навички безпечного користування Інтернетом.

Управлінський ефект від такої діяльності є подвійним: по-перше, знижується навантаження на технічні служби ОМС через зменшення кількості інцидентів, спричинених помилками користувачів; по-друге, підвищується загальна легітимність і довіра до цифрових реформ у державі. Використання платформ на кшталт «Дія.Освіта», як базового ресурсу для мешканців дозволяє громаді інтегруватися в загальнонаціональний освітній простір, економлячи місцеві ресурси на розробку власного контенту.

Підсумовуючи аналіз процесу формування культури кібергігієни, слід констатувати, що людський капітал є найбільш гнучким та водночас найбільш значущим інструментом превенції кіберзагроз у системі публічного управління. Встановлено, що без належного рівня цифрової культури службовців та мешканців громади навіть найдорожчі технологічні рішення залишаються малоефективними перед обличчям методів соціальної інженерії. Доведено, що системна освітня діяльність ОМС дозволяє перетворити потенційну вразливість на активний захисний механізм, де кожен користувач стає свідомим учасником процесу забезпечення національної безпеки.

Отже, формування кіберкультури має стати постійною функцією муніципального менеджменту, що базується на принципах ігрофікації, практичної спрямованості та безперервності. Виявлено, що синергія між суворими адміністративними регламентами для службовців та широкою просвітницькою роботою серед мешканців створює надійний соціальний фундамент для кіберстійкості всієї громади. Таким чином, розвиток культури кібергігієни є ключовим шляхом удосконалення публічного управління, який дозволяє забезпечити довгостроковий «імунітет» територіальних громад до гібридних викликів сучасності та зміцнити цифровий суверенітет держави.

Висновки до розділу 3

У результаті розробки та обґрунтування стратегічних шляхів удосконалення публічного управління у сфері зміцнення кіберстійкості територіальних громад було сформульовано низку концептуальних висновків, що становлять прикладну основу для підвищення рівня національної безпеки на місцевому рівні.

По-перше, доведено, що фундаментальною умовою переходу від реактивної моделі захисту до проактивної стратегії життєздатності є впровадження чітко регламентованого алгоритму реагування на кіберінциденти, який формалізує послідовність дій органів місцевого самоврядування з моменту виявлення аномалії до повного відновлення функціональності систем. Встановлено, що такий алгоритм, адаптований до специфіки муніципального врядування, дозволяє нівелювати фактор суб'єктивності та паніки під час кризових ситуацій, забезпечуючи чітку координацію між технічними підрозділами, керівництвом громади та державними суб'єктами кібербезпеки. Обґрунтовано, що алгоритмізація процесів інцидент-менеджменту є не лише технічною потребою, а й важливим інструментом публічного адміністрування, який гарантує безперервність надання соціально значущих послуг мешканцям громади навіть за умов інтенсивного ворожого кібервпливу.

По-друге, визначено, що подолання хронічного ресурсного та технологічного дефіциту в громадах можливе лише через широке впровадження моделей публічно-приватного партнерства, які дозволяють інтегрувати інноваційний потенціал та інтелектуальні ресурси приватного IT-сектору в систему муніципального управління безпекою. Виявлено, що перехід до сервісних моделей (Security-as-a-Service) та створення спільних центрів моніторингу (Joint SOC) є найбільш ефективним шляхом модернізації інфраструктури громад, оскільки це дозволяє трансформувати значні капітальні витрати на операційні платежі та отримати доступ до передових

технологій захисту без необхідності утримання розгалуженого штату дефіцитних фахівців. Показано, що успіх такого партнерства прямо залежить від здатності публічної влади сформувати прозоре правове поле та гнучкі механізми розподілу ризиків, де бізнес виступає стратегічним союзником у захисті цифрового суверенітету регіону.

По-третє, встановлено, що формування культури кібергігієни серед службовців органів місцевого самоврядування та мешканців громади є найбільш дієвим і найменш затратним інструментом превенції загроз, що дозволяє нейтралізувати більшість атак, заснованих на методах соціальної інженерії. Отже, публічне управління у цій сфері має зміщуватися від формального інструктажу до створення «цифрового імунітету» через систему безперервного навчання, симуляції загроз та популяризацію навичок безпечної поведінки. Виявлено, що синергія між суворими адміністративними регламентами для персоналу ОМС та широкими просвітницькими кампаніями для населення створює стійкий соціальний фундамент кіберстійкості, де кожна людина стає свідомим суб'єктом захисту інформаційного простору громади, що критично важливо в умовах гібридної війни.

По-четверте, запропоновані шляхи вдосконалення становлять цілісну модель муніципального кіберменеджменту, яка базується на поєднанні жорстких алгоритмів дії, гнучких моделей співпраці з бізнесом та високого рівня обізнаності громадян. Доведено, що імплементація цих рекомендацій дозволить територіальним громадам вийти на новий рівень автономності та стійкості, перетворюючи їх із пасивних об'єктів захисту на активні вузли загальнонаціональної системи кібербезпеки. Встановлено, що ключовим фактором успіху запропонованих змін є політична воля місцевого керівництва та готовність до інституційної трансформації публічної влади в бік більшої відкритості, цифровізації та безпекової орієнтованості.

Таким чином, результати третього розділу підтверджують, що зміцнення кіберстійкості громад потребує комплексного управлінського підходу, де технічні рішення підсилюються організаційними регламентами та розвитком

людського капіталу. Запропоновані заходи дозволяють створити багаторівневу систему захисту, здатну ефективно функціонувати в умовах невизначеності та постійного зростання інтенсивності кіберзагроз, забезпечуючи надійне підґрунтя для сталого розвитку територіальних громад як невід'ємної частини суверенної цифрової держави.

ВИСНОВКИ

У результаті проведеного комплексного дослідження теоретико-методологічних засад, аналізу сучасного стану та розробки шляхів удосконалення публічного управління у сфері зміцнення кіберстійкості територіальних громад в Україні, було отримано низку науково обґрунтованих результатів, що дозволяють сформулювати наступні загальні висновки:

По-перше, на основі теоретико-методологічного аналізу встановлено, що в сучасній парадигмі національної безпеки категорія «кіберстійкість» пройшла складний шлях еволюційної трансформації, перетворившись із вузькоспеціалізованого технічного параметра надійності інформаційних систем на фундаментальну стратегічну характеристику публічного управління. Визначено, що ключовою дефініцією кіберстійкості є здатність політико-адміністративної системи громади та держави в цілому не лише чинити опір деструктивним впливам у кіберпросторі, а й витримувати їх, оперативно відновлювати критичні функції та адаптуватися до нових типів загроз, забезпечуючи безперервність надання публічних послуг. Доведено, що у структурі національної безпеки кіберстійкість посідає місце інтегруючого компонента, оскільки в умовах тотальної цифровізації управлінських процесів будь-яка втрата контролю над цифровими активами автоматично призводить до підриву воєнної, економічної та соціальної стабільності держави.

По-друге, дослідження нормативно-правового регулювання засвідчило, що Україна демонструє високі темпи уніфікації національного законодавства із міжнародними стандартами, зокрема через імплементацію положень Директиви ЄС NIS2, проте на муніципальному рівні все ще спостерігається певна фрагментарність правового поля. Встановлено, що роль органів місцевого самоврядування у забезпеченні стійкості критичної інформаційної інфраструктури є визначальною, оскільки саме на локальному рівні зосереджені об’єкти життєзабезпечення та масиви персональних даних громадян, що потребують захисту. Обґрунтовано, що публічне управління у

цій сфері має зміститися від формального виконання централізованих інструкцій до активної суб'єктності громад у формуванні локальних політик безпеки, що вимагає чіткого законодавчого закріплення повноважень та відповідальності місцевої влади за стан кіберзахисту підпорядкованих територій.

По-третє, аналіз сучасного стану та оцінка вразливостей інформаційних систем ОМС в умовах воєнного стану виявили системні прогалини в цифровій стійкості громад, зумовлені як зовнішніми факторами агресії, так і внутрішніми управлінськими недоліками. Доведено, що найбільш критичною вразливістю в системі публічного управління залишається «людський фактор», який у поєднанні з методами соціальної інженерії та психологічним тиском війни стає основним вектором проникнення в муніципальні мережі. В умовах воєнного стану актуалізували проблему фізичного захисту інфраструктури та необхідність термінової міграції критичних даних у хмарні сховища, що вимагає від муніципальних управлінців перегляду традиційних підходів до архітектури безпеки та впровадження систем безперервного моніторингу подій.

По-четверте, вивчення механізмів взаємодії ОМС із державними інституціями показало, що ефективність національної кіберстійкості прямо залежить від якості інформаційного обміну між місцевим самоврядуванням та такими структурами, як Держспецзв'язку, СБУ та Кіберполіція. Встановлено, що хоча інституційна база взаємодії створена, вона потребує подальшої цифровізації та дебюрократизації, зокрема через автоматизовані платформи передачі індикаторів компрометації (на кшталт MISP) та діяльність CERT-UA. Обґрунтовано, що публічне управління має еволюціонувати в бік створення сервісно-орієнтованої моделі підтримки громад, де держава виступає не лише контролером, а й активним партнером, що надає методологічну та технологічну допомогу малим територіальним громадам, які не мають власних потужних ресурсів для автономного кіберзахисту.

По-п’яте, аналіз ресурсного забезпечення висвітлив критичний розрив між актуальними загрозами та реальними можливостями громад щодо їх нейтралізації. Хронічний дефіцит фінансування «за залишковим принципом» та кадровий голод у сфері ІТ-безпеки є головними бар’єрами на шляху до реальної резистентності. Виходом із цієї ситуації визначено впровадження нових управлінських моделей, заснованих на міжмуніципальному співробітництві та спільному використанні експертного потенціалу. Встановлено, що ресурсна політика ОМС має переорієнтуватися на інвестиційне управління, де кібербезпека розглядається як фундамент соціально-економічного розвитку та обов’язкова умова інвестиційної привабливості регіону в цифрову епоху.

По-шосте, розроблений авторський алгоритм реагування на кіберінциденти пропонує громадам чіткий інструментарій кризового менеджменту, що дозволяє формалізувати процеси виявлення, локалізації та відновлення систем після атак. Алгоритмізація управлінських дій є ключовим шляхом удосконалення публічного управління, оскільки вона мінімізує вплив суб’єктивних чинників та забезпечує скоординованість зусиль усіх ланок влади. Встановлено, що такий алгоритм має бути інтегрований у плани безперервності діяльності громади та регулярно відпрацьовуватися під час практичних кібернавчань, що дозволяє підтримувати систему в стані постійної готовності до відбиття агресії.

По-сьоме, запропоновано впровадження моделей публічно-приватного партнерства, як найбільш перспективного шляху подолання технологічної застарілості муніципальних систем. Доведено, що залучення приватного сектору через сервісні моделі (Security-as-a-Service) та створення спільних центрів моніторингу дозволяє громадам отримати доступ до передових технологій захисту та інтелектуального капіталу ІТ-бізнесу без надмірних капітальних витрат. Виявлено, що роль публічного управління у цьому процесі полягає у формуванні прозорих правил гри, забезпеченні контролю за конфіденційністю даних та створенні стимулів для бізнесу брати участь у

зміцненні регіональної кіберстійкості як складника корпоративної соціальної відповідальності.

По-восьме, особливу увагу приділено формуванню культури кібергігієни, яка визначена як базовий інструмент превенції загроз. Системна освітня робота серед службовців ОМС та мешканців громади дозволяє перетворити потенційну «людську вразливість» на активний захисний механізм. Обґрунтовано, що публічне управління має трансформувати технічні регламенти безпеки в етичні норми поведінки, де кожен користувач муніципальних сервісів усвідомлює власну роль у забезпеченні цифрового суверенітету держави. Це потребує впровадження інноваційних методів навчання, симуляцій загроз та широких інформаційних кампаній, які б охоплювали всі верстви населення громади.

Резюмуючи результати дослідження, можна стверджувати, що зміцнення кіберстійкості територіальних громад в Україні потребує комплексної трансформації публічного управління, яка базується на синергії трьох факторів: жорсткої нормативної регламентації, гнучких моделей партнерства з приватним сектором та високого рівня цифрової культури суспільства. Реалізація запропонованих шляхів удосконалення дозволить сформувати в Україні децентралізовану, але цілісну систему кіберзахисту, здатну ефективно функціонувати в умовах перманентної гібридної війни та забезпечувати сталий розвиток громад як фундаменту національної безпеки держави. Тільки через інтеграцію кібербезпеки в усі рівні муніципального менеджменту можлива побудова сучасної, захищеної та сервісно-орієнтованої держави, здатної захистити інтереси своїх громадян у глобальному цифровому просторі.

Список використаних джерел

1. 30 найбільших кібератак на Україну. *Слово і Діло*. URL: https://www.slovoidilo.ua/2025/03/24/infografika/bezpeka/najmasshtabnishikiberataky-ukrayinu (дата звернення: 20.04.2026).

2. 535 кібератак і майже 9 тисяч критичних подій: результати роботи системи виявлення вразливостей у I півріччі 2025 року. *CyberSecNet*. URL: https://cybersec.net.ua/novyny/909-535-kiberintsydentiv-i-maizhe-9-tysiach-krytychnykh-podii-v-dtskz-vidzvituvaly-pro-rezultaty-roboty-systemy-vyiavlennia-vrazlyvostei-u-i-pivrichchi-2025-roku.html (дата звернення: 20.04.2026).

3. Cyber Resilience Review (CRR). Cybersecurity & Infrastructure Security Agency (CISA). URL: https://www.cisa.gov.

4. *Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM*. Stati Uniti : IGI Global, 2020. C. 135–137. URL: https://dokumen.pub/qdownload/cyber-security-auditing-assurance-and-awareness-through-csam-and-catram-9781799856092-1799856097.html (дата звернення: 20.04.2026).

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 20.04.2026).

6. Global Cybersecurity Index (GCI). International Telecommunication Union (ITU). URL: https://www.itu.int.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 20.04.2026).

8. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide / Cichonski P. et al. National Institute of Standards and

Technology. 2012. URL: https://www.researchgate.net/publication/329972954_NIST_Special_Publication_800-61_Revision_2_Computer_Security_Incident_Handling_Guide (дата звернення: 20.04.2026).

9. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. URL: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9 (дата звернення: 20.04.2026).

10. The EU's Cybersecurity Strategy for the Digital Decade. *European Commission*. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата звернення: 20.04.2026).

11. Аналітичні звіти Державної служби спеціального зв'язку та захисту інформації України щодо стану кібербезпеки. URL: https://cip.gov.ua.

12. Аналітичні матеріали Держспецзв'язку. *Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku (дата звернення: 20.04.2026).

13. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100–108.

14. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07 / Бухарєв Віталій Вікторович. Суми, 2018. 221 с.

15. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2019. № 2. С. 23–28.

16. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 8. С. 28–35.

17. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2019. № 1. С. 140–145.

18. Гончарук Ю. В. Забезпечення кібербезпеки в публічному управлінні: виклики та загрози воєнного часу. *Публічне адміністрування та національна безпека*. 2026. № 2 (67). С. 17–23. DOI: 10.25313/2617-572X-2026-2-11927 (дата звернення: 20.04.2026).

19. Горун О. Ю. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. *Інформація і право*. 2021. № 2 (37). С. 93–102.

20. Дешко Л. М., Бонарєва К. Д. Кібербезпека в Україні: Національна стратегія та міжнародне співробітництво. *Порівняльно-аналітичне право*. 2018. № 2. С. 136–158.

21. Деякі питання захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 20.04.2026).

22. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (дата звернення: 20.04.2026).

23. Дорогих С. О. Щодо питань інформаційної безпеки як напряму інформаційної політики України в умовах війни. *Інформація і право*. 2022. № 2 (41). С. 133–137.

24. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України : монографія. Київ : НІСД, 2021. 260 с.

25. Євсюкова О. В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. *Державне управління: удосконалення та розвиток*. 2021. № 2. URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf (дата звернення: 20.04.2026).

26. Жиляєв І. В. Публічне управління у сфері цифрової трансформації : підручник. Київ : АртЕк, 2022. 340 с.

27. Заскока Ю. Державна політика та правові механізми забезпечення кібербезпеки України: ретроспектива та сучасність. *Наукові інновації та передові технології*. 2022. № 10 (12). URL: http://perspectives.pp.ua/index.php/nauka/article/download/2591/2597 (дата звернення: 20.04.2026).

28. Зеленський підписав закон про кібербезпеку. *DOU*. URL: https://dou.ua/lenta/news/president-signs-law-on-cybersecurity/ (дата звернення: 20.04.2026).

29. Інтенсивність фішингових атак зросла, але люди стали більш обізнаними в питаннях кібергігієни: аналітичний звіт CERT-UA. *Держспецзв'язку*. URL: https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua (дата звернення: 20.04.2026).

30. Кібербезпека 2025: тренди, які визначать майбутнє. *IITD*. URL: https://iitd.ua/kiberbezpeka-2025-trendi-yaki-zminyat-pravila-gri-ta-viznachat-majbutnye/ (дата звернення: 20.04.2026).

31. Кібербезпека в умовах війни: виклики та рішення / за ред. О. В. Литвиненка. Київ : НТУУ «КПІ», 2024. 195 с.

32. Кібербезпека по-новому: Україна готує нові правила. *Galera News*. URL: https://galera.news/kiberbezpeka-2025-novi-pravyla-hry-v-ukraini-11887/ (дата звернення: 20.04.2026).

33. Кібербезпека у 2025 році: нові виклики та тренди. *Softline*. URL: https://softline.company/ua/news/kiberbezpeka-u-2025-rotsi-novi-vyklyky-ta-trendy.html (дата звернення: 20.04.2026).

34. Кіберстійкість громад: виклики та шляхи зміцнення. *Decentralization.ua*. URL: https://decentralization.ua/news/18734 (дата звернення: 20.04.2026).

35. Ковальова А., Яковлева А., Чорна А. Кримінальна відповідальність за кіберзлочини, вчинені в умовах воєнного стану. *Матеріали конференцій МЦНД : зб. тез доп.* (19.04.2024; Кропивницький, Україна). С. 63–64.

36. Колесніков А., Зяйлик М. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства*. 2017. Вип. 1(9). С. 26–29.

37. Конституція України : Закон від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 20.04.2026).

38. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Грані*. 2018. Т. 21, № 11. С. 40–46. DOI: 10.15421/151846.

39. Кулешов М. В. Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами Служби безпеки України. *Інформація і право*. 2019. № 2(29). С. 115–122.

40. Лахно В. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. *Безпека інформації*. 2022. Т. 22, № 1. С. 44–50.

41. Малахов Г. Б. Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України. *Інформація і право*. 2023. № 4 (47). С. 197–206.

42. Національний координаційний центр кібербезпеки (НКЦК). Офіційний портал РНБО. URL: https://rnbo.gov.ua.

43. Офіційний сайт Урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua.

44. Петров С. Г. Захист державних електронних інформаційних ресурсів України. *Інформація і право*. 2020. № 3 (34). С. 62–68. URL: https://ippi.org.ua/sites/default/files/9_17.pdf (дата звернення: 20.04.2026).

45. Петров С. Г. Стан наукової розробки проблеми захисту державних електронних інформаційних ресурсів в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2020. № 61, т. 2. С. 20–23.

46. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Актуальні проблеми міжнародних відносин*. 2022. Вип. 152. С. 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389 (дата звернення: 20.04.2026).

47. Про CERT-UA. *CERT-UA*. URL: https://cert.gov.ua/about-us (дата звернення: 20.04.2026).

48. Про державно-приватне партнерство : Закон України від 01.07.2010 № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text (дата звернення: 20.04.2026).

49. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 20.04.2026).

50. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) : Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14.12.2022. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 20.04.2026).

51. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 20.04.2026).

52. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 № 280/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр#Text (дата звернення: 20.04.2026).

53. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.04.2026).

54. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.04.2026).

55. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.04.2026).

56. Проєкт Стратегії кібербезпеки України. *Офіційний вебсайт РНБО України*. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 20.04.2026).

57. Публічне управління та адміністрування в умовах глобальних викликів : колект. монографія / за заг. ред. Н. М. Мельтюхової. Харків : Вид-во ХаРІ НАДУ «Магістр», 2023. 412 с.

58. Сливка М. М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний факультет Запорізького національного університету*. 2022. № 10. С. 489–491.

59. Станіславський Т. Розвиток міжнародного співробітництва України у сфері кібербезпеки. *Актуальні проблеми державного управління*. 2019. № 3. С. 58–67.

60. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

61. У 2024 році кількість кібератак на Україну зросла на 70% : [інформаційне повідомлення]. *Інститут масової інформації (IMI)*. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 (дата звернення: 20.04.2026).

62. Україна на 24 місці в рейтингу з кібербезпеки. *AIN.UA*. 2024. 16 черв. URL: https://ain.ua/2024/06/16/ukrayina-na-24-misczi-v-rejtyngu-z-kiberbezpeky/ (дата звернення: 20.04.2026).

63. Шинкаренко А. Ю., Ставицький О. В. Кібербезпека як один з механізмів забезпечення стабільного розвитку економіки в Україні. *Електронний архів НТУУ «КПІ» ім. І. Сікорського*. URL: https://ela.kpi.ua/bitstream/123456789/22611/1/2017-11_5-09.pdf (дата звернення: 20.04.2026).

64. Юрченко О. М. Міжнародний досвід правового регулювання кібербезпеки: уроки для України. *Журнал публічного управління*. 2025. № 2. С. 45–58.

65. Яковлєв П. О. Об’єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки України. *Право і суспільство*. 2020. № 3. С. 178–183.

ДОДАТКИ

ДОДАТОК А

Зразок структури розділу «Цифрова стійкість та безпека» для Стратегії розвитку територіальної громади

1. Загальні положення: Визначення цілей захисту інформаційного простору громади та відповідність національним стандартам.

2. Аналіз поточного стану: Оцінка наявної ІТ-інфраструктури, перелік критичних реєстрів та систем життєзабезпечення (КІІ).

3. SWOT-аналіз кібербезпеки громади:

— сильні сторони: наявність кваліфікованих кадрів, сучасне ПЗ.

— слабкі сторони: дефіцит фінансування, застаріле обладнання.

— можливості: залучення міжнародних грантів, партнерство з ІТ-бізнесом.

— загрози: гібридна агресія, фішингові атаки на персонал.

4. Пріоритетні завдання: Впровадження систем моніторингу, навчання персоналу та модернізація серверних потужностей.

5. Очікувані результати: Зниження кількості успішних атак, мінімізація часу відновлення систем після збоїв.

ДОДАТОК Б

Інструментарій діагностики стану цифрової культури та кібергігієни в органах місцевого самоврядування

Шановний колего! Дане опитування проводиться з метою оцінки рівня кіберстійкості нашої громади та виявлення напрямів для вдосконалення системи захисту інформації. Ваші відповіді допоможуть мінімізувати ризики соціальної інженерії та підвищити ефективність публічного управління в умовах воєнного стану. Анкетування є анонімним.

І. БЛОК: Парольна політика та ідентифікація користувачів

1. Вкажіть періодичність оновлення паролів до Ваших робочих облікових записів (пошта, реєстри, CRM):

а) щомісяця (відповідно до стандартів безпеки);

б) один раз на 6 місяців;

в) ніколи не змінюю, якщо система не вимагає;

г) здійснюю зміну лише за наявності підозри на компрометацію акаунта.

2. Чи застосовуєте Ви багатофакторну автентифікацію (2FA) для доступу до критичних сервісів ОМС?

а) так, активована на всіх можливих ресурсах (СМС-код, автентифікатор);

б) активована лише на електронній пошті;

в) ні, вважаю це зайвою бюрократичною перепоною;

г) не володію інформацією щодо наявності такого функціоналу в моїх робочих системах.

ІІ. БЛОК: Комунікаційна безпека та поводження з документами

3. Як Ви здійснюєте передачу службових документів з обмеженим доступом у позаробочий час або в умовах релокації?

а) виключно через захищені канали зв’язку та корпоративну пошту;

б) іноді використовую персональні месенджери (Viber, Telegram) для оперативності;

в) використовую персональну пошту (Gmail, Ukr.net тощо) через зручність доступу;

г) це суворо заборонено моєю посадовою інструкцією, тому чекаю доступу до робочого місця.

4. Чи підключаєте Ви особисті пристрої (смартфон, ноутбук) до внутрішньої мережі ОМС без попередньої перевірки технічним спеціалістом?

а) так, це нормальна практика (BYOD-модель);

б) тільки у критичних ситуаціях;

в) ні, використовую лише сертифіковані корпоративні пристрої.

III. БЛОК: Протидія соціальній інженерії (Стрес-тест)

5. Уявіть, що Ви отримали лист від імені «ІТ-департаменту громади» з повідомленням про термінову необхідність оновити облікові дані через технічний збій. Ваші дії?

а) негайно перейду за посиланням у листі та введу новий пароль;

б) завантажу вкладений файл з «інструкцією», щоб ознайомитися з деталями;

в) проігнорую лист та видалю його як спам;

г) повідомлю уповноважену особу з питань кібербезпеки (CISO) або системного адміністратора для верифікації запиту.

6. Наскільки безпечним Ви вважаєте використання публічних Wi-Fi мереж для входу в адміністративні панелі муніципальних реєстрів?

а) цілком безпечно за умови використання складного пароля;

б) допустимо при використанні корпоративного VPN-з’єднання;

в) вважаю це критичною вразливістю і ніколи не практикую.

IV. БЛОК: Оцінка управлінського супроводу

7. Чи проходили Ви протягом останнього року навчання (тренінги, вебінари) з основ кібергігієни та безпеки в цифровому просторі?

а) так, систематично беру участь у заходах від Мінцифри/Держспецзв’язку;

б) проходив ознайомчий інструктаж при призначенні на посаду;

в) ні, отримую інформацію лише самостійно з відкритих джерел;

г) вважаю, що моїх поточних знань достатньо для виконання обов’язків.

Дякуємо за Вашу участь та внесок у цифрову стійкість нашої громади!

ДОДАТОК В

Деталізована операційна карта алгоритму реагування на кіберінциденти в органах місцевого самоврядування

Етап реагування	**Відповідальна особа/підрозділ**	**Необхідні дії та регламент виконання**
I. Виявлення та реєстрація	Спеціаліст IT-відділу / черговий	1. Первинна фіксація аномальної поведінки систем (зміна швидкості, помилки доступу). 2. Реєстрація події в журналі інцидентів протягом 10 хв.
II. Первинний аналіз та класифікація	Офіцер з кібербезпеки (CISO)	1. Верифікація типу загрози (DDoS, вірус-шифрувальник, витік даних). 2. Визначення рівня критичності (Низький/Середній/Критичний).
III. Стримування та локалізація	Група технічного захисту	1. Ізоляція уражених серверів або сегментів мережі (VLAN) від інтернету. 2. Блокування облікових записів, з яких зафіксовано підозрілу активність. 3. Створення контрольних знімків (snapshots) пам’яті для експертизи.
IV. Оповіщення та координація	Міський голова / Керівник апарату	1. Негайне сповіщення CERT-UA та територіального підрозділу СБУ (протягом 60 хв). 2. Підготовка офіційного пресрелізу для мешканців громади у разі зупинки сервісів.
V. Ліквідація та відновлення	IT-відділ + приватний партнер (за наявності)	1. Повне очищення систем від шкідливого ПЗ. 2. Поетапне відновлення даних із незалежних («холодних») резервних копій. 3. Перевірка цілісності відновлених баз даних перед запуском у публічний доступ.
VI. Пост-інцидентний аналіз	Робоча група (ОМС + експерти)	1. Проведення ретроспективної наради (Lessons Learned). 2. Внесення змін до локальних регламентів безпеки. 3. Оцінка потреби у додатковому навчанні персоналу.

Джерело: складено автором самостійно.