Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Навчально–науковий інститут фінансів, економіки, управління та права
Кафедра публічного управління, адміністрування та права

Кваліфікаційна робота

на тему: **«ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ»**

Виконала:
студентка академічної групи 401 ПУ
освітньо–професійної програми
«Публічне управління та адміністрування»
першого (бакалаврського) рівня
вищої освіти спеціальності
281 «Публічне управління та адміністрування»
_____ Т. С. Шостака
Науковий керівник: Кандидат наук з
державного управління, доцент
_____ В. В. Смаглюк

Полтава 2026 рік

Бібліографічний опис та анотація кваліфікаційної роботи

Бібліографічний опис: Шостака Тетяна Сергіївна. Інформаційна безпека органів місцевого самоврядування в Україні. Спеціальність: 281 «Публічне управління та адміністрування». Національний університет «Полтавська політехніка імені Юрія Кондратюка». Навчально–науковий інститут фінансів, економіки, управління та права. Кафедра публічного управління, адміністрування та права. Науковий керівник: Смаглюк Вікторія Валеріївна, кандидат наук з державного управління, доцент. Полтава. 2026 рік.

Зміст роботи: робота складається зі вступу, трьох розділів, висновків та пропозицій, списку використаних джерел, додатків.

Анотація. У роботі досліджено стан та проблеми інформаційної безпеки органів місцевого самоврядування в Україні під час дії воєнного стану. На прикладі Полтавської обласної ради проаналізовано основні вразливості цифрової інфраструктури, зокрема ризики використання незахищених каналів зв'язку та «гібридного» діловодства. Спираючись на європейський досвід, запропоновано прикладні кроки для посилення кіберстійкості територіальних громад. Доведено критичну необхідність перенесення муніципальних баз даних у хмарні сховища, ізоляції систем управління комунальними підприємствами та суворого дотримання посадовцями цифрової гігієни. Результати дослідження можуть бути використані місцевими радами для вдосконалення регіональних програм безпеки, зокрема ініціативи «Цифрова Полтавщина».

Ключові слова: інформаційна безпека, органи місцевого самоврядування, публічне управління, кіберзахист, кібербезпека, воєнний стан, захист персональних даних, цифровізація, хмарні технології, критична інфраструктура, інформаційні ресурси, цифрова грамотність, Полтавська обласна рада.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОМС – органи місцевого самоврядування.

ЦНАП – центр надання адміністративних послуг.

ОВА – обласна військова адміністрація.

ІКС – інформаційно–комунікаційні системи.

КСЗІ – комплексна система захисту інформації.

ДРРП – Державний реєстр речових прав (на нерухоме майно).

ІТ – інформаційні технології.

СБУ – Служба безпеки України.

ТЕЦ – теплоелектроцентраль.

ЗМІСТ

ВСТУП…….…..…… 5

РОЗДІЛ 1. ТЕОРЕТИКО–ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ…..... 9

1.1. Поняття, сутність та складові інформаційної безпеки в системі публічного управління…….…….. 9

1.2. Нормативно–правове забезпечення інформаційної безпеки місцевого самоврядування України…….. 16

РОЗДІЛ 2. АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ……....……. 23

2.1. Аналіз діяльності органів місцевого самоврядування із забезпечення захисту інформаційних ресурсів в умовах воєнного стану……... 23

2.2. Дослідження ключових проблем та вразливостей у системі інформаційної безпеки Полтавської обласної ради…… 28

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ..... 36

3.1. Адаптація міжнародного досвіду в сфері інформаційної безпеки в органах місцевого самоврядування……. 36

3.2. Пріоритети удосконалення напрямів інформаційної безпеки України та Полтавської області……... 42

ВИСНОВКИ ТА ПРОПОЗИЦІЇ……...……. 50

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……...……...…… 53

ДОДАТКИ ...……...……...…… 60

ВСТУП

Актуальність теми дослідження. Глобальна трансформація суспільства в інформаційне середовище зробила цифрові масиви даних головним рушієм прогресу. У системі державного менеджменту ці процеси відобразилися через масштабну цифровізацію, яка повністю змінила логіку взаємодії владних структур із населенням. Запуск широкої мережі електронних адміністративних послуг та відмова від паперового діловодства стали свідченням ефективності реформ. Однак інтенсивне проникнення технологій у публічне адміністрування несе і серйозні ризики. Питання інформаційної безпеки давно вийшли за рамки компетенції звичайних технічних спеціалістів. Сьогодні надійний кіберзахист – це фундамент для втримання державного суверенітету, гарантування стабільності апарату управління та збереження високого рівня довіри громадян до влади.

Для інституту місцевого самоврядування питання безпеки цифрових активів сьогодні постало з винятковою гостротою. Успішна реалізація реформи децентралізації призвела до того, що територіальні громади та обласні ради перебрали на себе не лише розширений обсяг фінансово–управлінських повноважень, а й статус головних утримувачів стратегічних баз даних. Нині саме на базовому та регіональному рівнях сконцентровані демографічні реєстри, містобудівні кадастри, масиви інформації соціального і медичного профілю, а також цифрові платформи управління комунальною інфраструктурою. Настільки масштабне акумулювання чутливих відомостей на місцях закономірно перетворює муніципальні інституції на одну з фундаментальних ланок у загальній архітектурі національної безпеки.

З початком повномасштабного вторгнення рф віртуальні мережі місцевих рад перетворилися на головні мішені для ворожих кібернетичних ударів та масштабних дезінформаційних кампаній. Введення правового режиму воєнного стану повністю змінило ландшафт ризиків, змусивши державу екстрено переформатувати підходи до управління інформацією.

Тоді як до війни безумовним орієнтиром залишалася всебічна транспарентність влади та розвиток політики відкритих даних, реалії бойових дій вимагають ювелірного балансування між суспільною підзвітністю муніципалітетів та суворими вимогами національної оборони. Як свідчить практика, безперешкодний доступ до бюджетної звітності, генеральних планів територій чи контактів службовців на офіційних вебресурсах рад створює ідеальне підґрунтя для ворожих спецслужб. Агресор інтенсивно збирає такі відомості за допомогою розвідки на основі відкритих джерел, щоб у подальшому використовувати їх для вузькоспрямованого фішингу та підготовки реальних кінетичних атак по регіональних об'єктах.

Попри загальнонаціональний курс на міграцію даних у хмарні сховища (стратегія «Cloud First»), кіберстійкість територіальних громад критично послаблюється хронічним недофінансуванням та дефіцитом IT–фахівців. Проте головною вразливістю муніципалітетів продовжує виступати людський фактор – збереження «гібридного» діловодства, неконтрольоване використання особистих гаджетів (модель BYOD) та службове листування у відкритих месенджерах зводять нанівець будь–які технічні бар'єри.

Зазначені системні недоліки особливо гостро проявляються на рівні регіональних владних інституцій. Для Полтавщини, яка під час війни перетворилася на стратегічний тиловий і гуманітарний хаб, безперервність управління має життєво важливе значення. Щоб гарантувати стабільну роботу Полтавської обласної ради та надійно убезпечити дані від компрометації, необхідно терміново відмовитися від ситуативного реагування на загрози на користь розбудови комплексної, ешелонованої архітектури кіберзахисту.

Усе це свідчить про наявність глибоких теоретико–правових та управлінських суперечностей у сфері муніципальної кібербезпеки. Гостра потреба захистити цифрові ресурси місцевих рад в умовах гібридної війни беззаперечно підтверджує високу актуальність та своєчасність обраної теми кваліфікаційної роботи.

Мета і завдання дослідження. Метою кваліфікаційної роботи є комплексне науково–практичне дослідження стану, проблем та нормативно–правового забезпечення інформаційної безпеки органів місцевого самоврядування в Україні, а також розробка прикладних напрямів і рекомендацій щодо її вдосконалення на регіональному рівні (на прикладі Полтавської обласної ради).

Для досягнення поставленої мети було визначено та вирішено такий комплекс дослідницьких завдань:

– з'ясувати теоретико–методологічні засади, сутність і структуру інформаційної безпеки як невід'ємної складової публічного управління;

– проаналізувати стан нормативно–правового забезпечення муніципального кіберзахисту та ідентифікувати головні законодавчі колізії (зокрема, проблему балансування між прозорістю влади та конфіденційністю даних);

– дослідити специфіку збереження цифрових ресурсів та управління інформацією в органах місцевого самоврядування під час дії воєнного стану;

– провести практичний аудит інфраструктури Полтавської обласної ради для виявлення її ключових організаційних, комунікаційних та технологічних вразливостей;

– систематизувати успішний міжнародний досвід побудови муніципальної кіберстійкості (на прикладі країн ЄС, Естонії, Сінгапуру) задля його адаптації до вітчизняних реалій;

– розробити стратегічні пріоритети та прикладну матрицю мінімізації цифрових ризиків для вдосконалення безпекової політики в органах влади та територіальних громадах Полтавської області.

Об'єкт дослідження – суспільно–управлінські відносини, що виникають у процесі забезпечення інформаційної безпеки в системі публічного управління та місцевого самоврядування України.

Предмет дослідження – теоретичні, нормативно–правові та організаційно–управлінські засади функціонування і вдосконалення системи інформаційної

безпеки органів місцевого самоврядування (на матеріалах Полтавської обласної ради).

Методи дослідження. Методологічне підґрунтя дослідження базується на комплексному поєднанні різних наукових підходів. Для розуміння природи інформаційної безпеки як управлінської категорії (змін у класичній тріаді CIA) застосовано метод системного аналізу. Дослідження законодавчої бази, що регулює обіг даних в органах місцевого самоврядування, здійснювалося нормативно–правовим методом. Міжнародний досвід та процеси впровадження е–сервісів оцінювалися через призму порівняльного й статистичного аналізу. Щоб практично ідентифікувати прогалини в діловодстві Полтавської обласної ради, було залучено інструментарій спостереження, індукції та дедукції. На завершальному етапі використано моделювання і синтез – це дозволило звести отримані дані у єдину авторську матрицю ризиків та розробити ешелоновану стратегію захисту.

Практичне значення одержаних результатів зумовлене тим, що всі теоретичні висновки та рекомендації переведені у площину готових прикладних інструментів. Зокрема, розроблену «Матрицю цифрових ризиків та прикладних заходів безпеки» можна безпосередньо застосовувати в роботі влади на місцях. Це ж стосується й алгоритмів усунення вразливостей від «гібридного» діловодства та неконтрольованої моделі BYOD. Ці рішення створювалися з урахуванням специфіки виконавчого апарату Полтавської обласної ради, проте вони є універсальними. Їх цілком доцільно впроваджувати у структурних підрозділах ОВА та в територіальних громадах базового рівня. Зрештою, матеріали цього дослідження стануть надійною базою для формування місцевих політик кібербезпеки та оновлення регіональних програм цифровізації.

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів (які містять шість підрозділів), висновків та пропозицій, списку використаних джерел і додатків. Основний текст роботи викладено на 41 сторінці. Робота містить 2 рисунки та 9 таблиць. Список використаних джерел налічує 51 найменування.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ

1.1. Поняття, сутність та складові інформаційної безпеки в системі публічного управління

Сучасний етап прогресу людства характеризується надзвичайно швидкими темпами проникнення цифрових технологій у кожну ланку суспільної взаємодії. Планета проходить через глобальну зміну парадигм від індустріального до інформаційного типу життєдіяльності. Основними активами для соціального та політичного процвітання стають дані та інтелектуальний капітал. У межах України подібні перетворення проявилися в оновленні управлінських структур через запуск цифрових сервісів, розвиток онлайн-взаємодії з населенням та переведення офіційної документації в електронний формат. Підсумком такої трансформації стала пряма кореляція між якістю роботи владних інституцій та рівнем стійкості і захисту їхніх комунікаційних систем від зовнішніх впливів.

Беручи до уваги ці чинники, захист інформаційного середовища перейшов із розряду вузькоспеціалізованих технічних завдань у статус фундаментальної засади державного регулювання та обов’язкового складника загальнонаціональної стійкості. Під час воєнного конфлікту, коли цифрова сфера виступає реальним плацдармом для протистояння, детальне розуміння архітектури та внутрішніх механізмів інформаційної безпеки є першочерговим для забезпечення державної цілісності та безперервності владних процесів на всіх рівнях.

Аби забезпечити змістовне та всебічне вивчення означеної теми, необхідно першочергово виконати теоретичне уточнення складу та сутності базових термінологічних категорій. Ключовим підґрунтям для розкриття сутності досліджуваного явища є його трактування у законодавстві. Базовий об’єкт нашого дослідження спирається на національне законодавство. Зокрема, профільний нормативний акт щодо інформації [34] визначає її як будь-який

масив зафіксованих даних, незалежно від природи їх носія - чи то фізичного, чи електронного. Натомість безпековий аспект цього явища розкривається в іншому законі [36], який трактує кіберзахист не просто як технічну категорію, а як фундаментальну гарантію недоторканності інтересів держави та суспільства від інформаційно-психологічних маніпуляцій чи несанкціонованого витоку даних. Проте в сучасній науці публічного управління підходи до розуміння інформаційної безпеки значно розширюються та деталізуються. Сучасна управлінська наука поступово відходить від вузького розуміння кіберзахисту. Наприклад, у дослідженнях А. Мінчекова [23] акцент зміщується на інституційну спроможність: безпека трактується як здатність владного апарату зберігати свою функціональність і безперервно реалізовувати державний курс навіть під тиском зовнішніх деструктивних факторів. Тобто фокус переноситься з комп’ютерних мереж на загальну стійкість системи управління. Тобто, на перший план виходить саме управлінський аспект - здатність органу влади продовжувати виконувати свої функції, незважаючи на кібератаки чи інформаційні кампанії з дискредитації.

Згідно з підходами І. Петроє, убезпечення інформаційного простору владних структур становить комплексну міждисциплінарну задачу. Авторка доводить, що ефективний менеджмент у цій сфері неможливий без синтезу юридичних, інженерних, психологічних та організаційних важелів [27]. Відповідно, кіберзахист не є статичним явищем, а являє собою безперервний алгоритм дій: від аудиту слабких місць і розробки тактики до впровадження захисних бар'єрів та їхньої подальшої модернізації.

У контексті місцевого самоврядування проблематика захисту даних набуває особливої гостроти. Чинна нормативна база [35] наділяє муніципалітети значним обсягом повноважень, що на тлі децентралізації призвело до акумулювання на локальному рівні колосальних масивів критично важливих відомостей. На сьогодні екосистема муніципальних даних охоплює реєстри жителів, бази соціального та медичного забезпечення, просторові та земельні кадастри, а також цифрові платформи, що керують об'єктами життєзабезпечення

(водоканали, тепломережі) та внутрішнім документообігом. Задля ефективного управління цими ресурсами та визначення пріоритетів безпеки їх доцільно класифікувати за функціональними напрямами (див. рис. 1.1).

Рисунок 1.1. Структура інформаційних ОМС, що потребують захисту

(Складено автором на основі нормативно-правових актів та матеріалів досліджень [13; 23; 27; 32; 34; 35])

Ця діаграма ілюструє складну структуру даних місцевих рад, де сервери та комп’ютери служать лише фізичними місцями зберігання. Така категоризація допомагає співробітникам краще зрозуміти ризики. Відповідно, вони можуть вибирати різні, специфічні методи захисту для кожного типу даних: від публічно оприлюднених рішень ради до суворо конфіденційної інформації.

Забезпечення цифрової стійкості сьогодні вийшло далеко за межі суто IT-підтримки. А. В. Кузьменко звертає увагу на управлінський парадокс: керівники змушені постійно шукати компроміс між необхідністю надійно ізолювати приватні дані та обов'язком підтримувати максимальну прозорість своєї діяльності перед громадою [13]. Ця рівновага є критичною для демократії, адже, як доводить І. О. Кульчій, саме безперешкодний доступ громадськості до урядової інформації слугує найефективнішим антикорупційним механізмом [15; 17]. Водночас така транспарентність не має створювати прогалин для витоку

чутливих відомостей мешканців чи даних, що загрожують національній безпеці, що суворо регламентується профільним законом щодо захисту персональних даних [32].

Змінюючи теоретичний ракурс на системний розгляд структури, необхідно зауважити, що базисом новітніх стратегій ідентифікації складових захисту інформації у міжнародній та вітчизняній практиці залишається канонічна концепція «тріади CIA». У контексті державного адміністрування та роботи місцевих владних інституцій ці чинники характеризуються унікальною специфікою реалізації, що відображено у таблиці 1.1.

Таблиця 1.1

Розширена модель складових інформаційної безпеки в органах місцевого самоврядування

Тріада CIA (Класична)	Управлінські компоненти
1. Конфіденційність 2. Цілісність 3. Доступність	1. Автентичність 2. Підконтрольність 3. Витривалість (стійкість)

Розроблено автором за матеріалом [13, 23, 27]

Як показано в таблиці 1.1, класична архітектура кібербезпеки (тобто, механізм CIA) в муніципальному управлінні має бути доповнена специфічними адміністративними параметрами. Фундаментальним принципом цієї моделі є конфіденційність, тобто надійний захист інформації від несанкціонованого втручання шляхом обмеженого доступу. Для місцевих органів влади це означає суворий контроль баз даних персональних даних громадян (включаючи адреси, реєстраційні номери платників податків та медичну інформацію), тендерних документів та проектів офіційних рішень до їх офіційного оприлюднення. Витік або порушення такої інформації не лише підривають довіру громадськості, але й створюють прямі правові ризики для організації.

Наступний ключовий параметр моделі – це цілісність інформації. Її головна мета полягає у захисті електронних документів від прихованого редагування, спотворення чи випадкового знищення. Для органів місцевого самоврядування це питання є критичним. Наприклад, будь-яке несанкціоноване втручання в бази земельного кадастру або фінансові рахунки здатне спровокувати масштабний управлінський колапс. Унеможливлення таких маніпуляцій є прямою запорукою довіри до влади. На практиці цей рівень безпеки забезпечується конкретними інструментами: суворим логуванням усіх дій у системі, чітким розмежуванням прав доступу та обов'язковим використанням кваліфікованих електронних підписів.

Завершальним критерієм тріади виступає доступність. Вона гарантує, що громадяни та посадовці матимуть безперебійний доступ до цифрових послуг і робочих реєстрів у потрібний час. Якщо офіційний портал місцевої ради чи внутрішні мережі установи паралізує хакерська атака (або навіть звичайний технічний збій сервера), робота апарату повністю зупиняється. За таких обставин сама концепція сервісного електронного урядування втрачає свою ефективність.

В умовах постійної еволюції кіберзагроз базова тріада закономірно розширюється новими компонентами, які стають критично важливими для публічного адміністрування. Серед них виділяється верифікованість (автентичність), що слугує технічним механізмом підтвердження оригінальності електронних документів та їхніх реальних авторів, повністю блокуючи спроби фальсифікації розпоряджень чи службових наказів керівництва. Не менш вагомою є невідмовність, або підконтрольність, яка формує середовище тотальної фіксації цифрових слідів посадовців у мережі. Завдяки цьому жоден співробітник не зможе приховати або заперечити факт свого втручання в муніципальні реєстри, що є ключовим інструментом для проведення внутрішніх аудитів. Завершує цю розширену модель операційна витривалість (стійкість) - характеристика, яка визначає здатність місцевої ради не припиняти виконання своїх стратегічних функцій під час активних хакерських атак та забезпечує максимально швидке відновлення інфраструктури після кризових інцидентів.

Щоб ця багатокомпонентна архітектура ефективно працювала на практиці, органам місцевого самоврядування потрібно кардинально змінити підхід до безпеки. Головне завдання – перейти від ситуативного реагування на інциденти до превентивного управління загрозами. У таких умовах фундаментом надійного захисту стають не лише профільні технічні спеціалісти, а насамперед кваліфіковані управлінці. Саме до їхньої компетенції належить розробка локальних регламентів, контроль за цифровою гігієною працівників апарату та постійний аналіз організаційних вразливостей. Завдяки цьому захист інформації перестає бути виключно технічним питанням і стає невід'ємною частиною ефективного публічного адміністрування.

Дослідник Є. В. Гончарук справедливо зазначає, що нові віртуальні загрози докорінно змінили характер громадської безпеки [5, с. 49]. Просто надійного захисту серверів вже недостатньо. Психологічна стійкість посадовців та широкої громадськості стає дедалі важливішою. В умовах гібридної війни місцеві органи влади змушені активно боротися з онлайн-дезінформацією та зловмисними маніпуляціями, що стало одним з їхніх першочергових завдань.

Повномасштабне вторгнення кардинально змінило пріоритети місцевої влади. Інформаційні ресурси рад опинилися під постійним прицілом. Як аргументовано зазначають О. М. Руденко та М. В. Захаров, ворог цілеспрямовано атакує їх для дестабілізації тилу [42]. Механізм є доволі простим, але дієвим. Отримавши доступ до сайту громади, хакери масово вкидають фейки. Це можуть бути повідомлення про здачу територій або ж чутки про критичну нестачу ресурсів. Їхня єдина мета – посіяти паніку та знищити довіру до місцевого керівництва. Через це надійний кіберзахист перестав бути формальністю і став питанням виживання всієї управлінської системи.

В умовах сучасної війни віртуальний простір фактично перетворився на лінію фронту. Втім, головною вразливістю залишається людська психологія. Можна розгорнути найдорожчі апаратні системи захисту, але вони виявляться абсолютно марними через звичайну неуважність персоналу. Працівники виконавчого апарату досі відкривають сумнівні фішингові листи. Вони роками

використовують слабкі паролі та регулярно підключають власні флешки до службової мережі. Наявність таких прогалин доводить одну важливу істину. Захист даних давно вийшов за межі компетенції ІТ-відділів і нині потребує жорсткого організаційного контролю.

З огляду на ці реалії Ю. Д. Гундертайло робить цілком закономірний висновок. Сьогодні цифрова гігієна посадовців – це вже не просто корисна опція, а базова умова для безперебійної роботи установи [6]. Такий підхід повністю підтримує Я. Ю. Цимбаленко. Дослідник підкреслює, що без глибокої кіберграмотності та критичного мислення компетентнісний профіль сучасного службовця є просто неповним [50]. Підсумовуючи цю думку, І. А. Сердюк влучно зазначає: загальна безпека всієї ради сьогодні тримається виключно на індивідуальній цифровій стійкості кожного окремого працівника [44].На завершення варто наголосити, що інформаційна безпека для органів місцевого самоврядування є комплексним завданням. Її слід розглядати як безперервний процес захисту цифрового середовища установи, побудований на поєднанні багатьох факторів, включаючи правові норми, управлінські рішення, технологічні засоби та, найголовніше, високий рівень обізнаності співробітників з питань кібербезпеки. Цей підхід виходить за рамки традиційних моделей безпеки даних.

Сучасні реалії вимагають не лише технічної стабільності електронних систем, але й від посадовців – здатності перевіряти інформацію та реагувати на інформаційно-психологічні атаки. Тому кібербезпека вже не є просто інженерним завданням, а стає стратегічним напрямом публічного управління. Сьогодні належний захист інформації є фундаментальною умовою для підтримки довіри громади, забезпечення безперервності роботи владних структур та збереження легітимності місцевого самоврядування.

1.2. Нормативно-правове забезпечення інформаційної безпеки місцевого самоврядування України

На мою думку, аналіз будь-якої управлінської системи слід починати з її нормативно-правової основи. Для органів місцевого самоврядування закон є не просто орієнтиром, а жорстким обмеженням. Посадові особи мають право діяти виключно в межах та у спосіб, що прямо передбачені законодавством. Саме тому сьогодні захист інформаційних систем територіальних громад – це вже не просто вузька технічна інструкція для ІТ-відділу, а прямий юридичний обов'язок керівництва ради. Він регулюється розгалуженим масивом актів, який змушений постійно адаптуватися до швидкого розвитку цифрових технологій. У підсумку, належна інформаційна стійкість стає базовою умовою для того, щоб місцева влада могла законно працювати, надавати електронні послуги та реалізовувати державну політику цифровізації на місцях.

Формування українського законодавства у цій сфері відбувалося поетапно. Його незмінним фундаментом виступають конституційні норми, які покликані збалансувати право суспільства на доступ до публічної інформації із необхідністю захищати персональні дані. Далі ця ієрархія доповнюється спеціальними законами щодо кіберзахисту електронних комунікацій, а в сучасних реаліях – ще й жорсткими вимогами правового режиму воєнного стану.

Уся ця комплексна нормативна конструкція створює середовище, де дані надійно захищені, а права громадян не порушуються. Розуміння цієї багаторівневої юридичної бази є критично важливим, адже саме на основі загальнодержавних вимог розробляються ефективні регіональні програми цифровізації та локальні політики захисту. Детальний огляд ключових нормативно-правових актів, які безпосередньо регулюють інформаційну стійкість в органах місцевого самоврядування, та їхній практичний вплив систематизовано у таблиці 1.2.

Таблиця 1.2

Законодавче забезпечення у сфері інформаційної безпеки та захисту даних в органах місцевого самоврядування

Назва закону	Дата прийняття	Короткий зміст (вплив на місцеве самоврядування)
Закон України «Про інформацію»	02.10.1992	Визначає обов'язковість своєчасного оприлюднення управлінських документів (проєктів рішень, звітів, генпланів) як базову умову законної роботи органу самоврядування.
Закон України «Про доступ до публічної інформації»	13.01.2011	Визначає публічний доступ до управлінської інформації як головний інструмент запобігання корупційним ризикам у виконавчому апараті.
Закон України «Про захист персональних даних»	01.06.2010	Формує механізм захисту персональних даних громадян, зобов'язуючи органи самоврядування не допускати розголошення чутливої інформації під час оприлюднення проєктів рішень та звітів.
Закон України «Про захист інформації в інформаційно-комунікаційних системах»	05.07.1994	Закріплює жорстку техніко-юридичну вимогу: робота з державними даними або конфіденційною інформацією в мережах самоврядування дозволена лише за наявності сертифікованої Комплексної системи захисту інформації.
Закон України «Про основні засади забезпечення кібербезпеки України»	05.10.2017	Радикально змінив підхід держави до захисту даних: убезпечення цифрового середовища визнано складником національної стійкості, а інформаційні системи місцевих рад офіційно віднесено до об’єктів критичної інфраструктури.
Закон України «Про електронні комунікації»	16.12.2020	Осучаснив нормативне регулювання у сфері передачі даних та забезпечення захисту електронних мереж, органічно доповнивши концепцію хмарних технологій.
Закон України «Про хмарні послуги»	02.02.2022	Легалізував концепцію «Cloud First», надавши місцевим радам законне право переносити свої реєстри у захищені сертифіковані центри обробки даних (замість побудови дорогих локальних серверних).

Розроблено автором на основі нормативно-правових актів [29, 31, 32, 34, 37, 40]

Зазначені нормативні вимоги є визначальними для органів місцевого самоврядування, оскільки їхній апарат щодня обробляє значні масиви інформації в реєстрах територіальних громад. Відповідно, забезпечення конфіденційності перетворюється на ключовий обов'язок посадових осіб. Адже від надійності цифрової інфраструктури безпосередньо залежить не лише стабільність роботи ради, а й рівень суспільної довіри до неї.

Поряд із цим, вітчизняне законодавство намагається встановити баланс. Гарантуючи право на доступ до публічної інформації, нормативні акти водночас передбачають обґрунтовані винятки – зокрема, заради захисту національної безпеки, територіальної цілісності чи громадського порядку. Як наслідок, діяльність виконавчого апарату відбувається на постійному перетині двох вимог: забезпечення відкритості влади та захисту приватного життя. Саме тут криється головна практична колізія, з якою працівники стикаються щодня: як зберегти максимальну прозорість підготовки проєктів рішень, не порушивши при цьому законодавство про захист персональних даних.

Сьогодні пошук цього компромісу є одним із пріоритетних завдань для місцевої влади. Запровадження надійних механізмів інформаційної безпеки дозволяє раді залишатися підзвітною громаді і водночас гарантувати збереження чутливих відомостей. Підтверджуючи цю тезу, Л. Сорокіна у своєму дослідженні правового регулювання цифровізації наголошує: сучасна управлінська практика вимагає від посадовців надзвичайної виваженості та суворого дотримання регламентів під час роботи з електронними реєстрами [46].

З одного боку, діяльність місцевих рад чітко регулюється законами України «Про інформацію» [34] та «Про доступ до публічної інформації» [29]. Ці норми вимагають відкритості. Органи місцевого самоврядування зобов’язані своєчасно оприлюднювати проєкти рішень, бюджетні звіти, протоколи засідань постійних комісій та містобудівну документацію. Така публічність – фундамент громадського контролю. Аналізуючи цей вектор, І. О. Кульчій справедливо зазначає, що належне виконання законодавства про доступ до інформації виступає одним із найдієвіших інструментів запобігання корупції у владних

інституціях [17]. Прозорість мінімізує ризики. Більше того, без відкритих механізмів комунікації неможливо сформувати ефективний виконавчий апарат, якому б дійсно довіряла громада.

З іншого боку, ради є найбільшими розпорядниками баз даних з обмеженим доступом. Тут у дію вступають суворі вимоги законодавства щодо захисту персональних даних [32]. На практиці це створює постійні колізії. Фахівці відділу організаційного забезпечення або юридичної служби щодня балансують на межі. Готуючи документи до публікації на офіційному сайті чи в системі е-документообігу, вони змушені буквально вручну розмежовувати суспільно важливі відомості та конфіденційні дані. Помилка тут неприпустима. Розголошення адрес проживання, медичних діагнозів у рішеннях про виділення матеріальної допомоги чи даних дітей-сиріт є прямим порушенням закону. Як акцентує увагу П. В. Мельник, нехтування цими регламентами гарантовано веде до жорсткої адміністративної чи кримінальної відповідальності посадових осіб [22].

Закон «Про основні засади забезпечення кібербезпеки України» [37] став поворотним моментом, перетворивши кіберзахист із суто технічного завдання на пріоритет національної стратегії та суверенітету. Це замінило фрагментарне регулювання цілісною державною політикою, оскільки стабільність владних інституцій тепер прямо залежить від захищеності їхньої цифрової інфраструктури.

У законодавстві з часом з’явилися чіткі визначення для об’єктів критичної інфраструктури та їхньої цифрової складової. Для нас ключовим є те, що інформаційні системи місцевих рад тепер офіційно належать до цієї категорії. Важливо розуміти, що зупинка серверів мерії чи обласної адміністрації - це не просто «завислий комп’ютер» чи втрата кількох файлів. На практиці це може обернутися справжнім паралічем життєво важливих служб: від збоїв у подачі води та тепла до хаосу в роботі громадського транспорту. Коли під загрозою опиняється звичний побут і безпека тисяч людей, кіберзахист перетворюється з технічної опції на питання виживання громади. Відповідно, вимоги до захисту

таких об’єктів значно посилилися, що знайшло своє відображення у Постанові Кабінету Міністрів України № 518, якою затверджено Загальні вимоги з кіберзахисту об’єктів критичної інфраструктури [33].

Нормативне закріплення технічних параметрів безпеки здійснюється відповідно до профільного Закону України «Про захист інформації в інформаційно-комунікаційних системах» [31]. Цей акт встановлює безапеляційну умову: обробка чутливих відомостей чи державних реєстрів у муніципальних мережах є легітимною виключно за умови розгортання атестованої комплексної системи захисту інформації. Проте в практичній площині для левової частки новоутворених територіальних громад виконання цієї норми виявилося об'єктивно неможливим. Створення захисних систем - це багатогранний та високовартісний процес, що охоплює професійні експертизи та закупівлю спеціалізованого обладнання. Для багатьох громад витрати у сотні тисяч гривень є надмірними, а через брак цільової підтримки з боку держави ці законодавчі вимоги часто залишаються лише на папері.Закон України «Про хмарні послуги» [40] запровадив принцип «Cloud First», надавши муніципалітетам можливість мігрувати дані до захищених дата-центрів замість розбудови вразливих локальних систем. Це дозволило оптимізувати витрати та підвищити рівень безпеки за рахунок експертизи провайдерів. Логічним доповненням став Закон «Про електронні комунікації» [30], який оновив правила захищеного обміну даними та адміністрування мереж. Аналіз нормативного середовища вимагає обов'язкового врахування кардинальних змін, зумовлених повномасштабною збройною агресією рф. Введення правового режиму воєнного стану повністю переформатувало архітектуру публічного адміністрування. Як підкреслюють у своїх працях Г. М. Куц та інші науковці, робота владних інституцій у воєнний час потребує нетипових рішень та максимальної оперативності в реагуванні на небезпеки [20]. У площині захисту даних це відобразилося через відчутний курс держави на централізацію управлінських процесів.

За спостереженнями О. В. Ніцевича, бойові дії змусили уряд докорінно змінити підходи до відкритості даних [24]. Задля протидії ворожій розвідці та запобігання коригуванню ударів, військові адміністрації обмежили доступ до ключових державних реєстрів, включаючи кадастрові та містобудівні дані. У воєнний час цифрова зручність поступилася місцем фізичній безпеці, перетворивши відкриті дані на потенційну вразливість. Паралельно було посилено роль Держспецзв'язку, який тепер може оперативно втручатися в роботу муніципальних мереж для нейтралізації кіберзагроз. С. Ю. Бойко та А. В. Маринів констатують: хоча подібні кроки об'єктивно звужують автономію місцевих рад, вони є єдиним легітимним інструментом збереження державної цілісності в умовах тотальної війни [2].

Євроінтеграція та статус кандидата в ЄС стимулюють повну адаптацію українського законодавства до європейських стандартів. У кіберзахисті це означає перехід від застарілих норм до інноваційних правил, де безпека даних стає фундаментом демократії. Така модернізація забезпечує прозорість цифрової інфраструктури для партнерів та суттєво зміцнює стійкість держави. Досліджуючи цей напрям, С. Кавин звертає увагу на складність майбутньої імплементації Директиви про мережеву та інформаційну безпеку [10]. Проте головним випробуванням для територіальних громад стане перехід на стандарти Загального регламенту про захист даних. Як наголошує І. О. Кульчій, європейська практика вимагає створення реальних інституційних запобіжників, зокрема обов'язкового запровадження посади Офіцера із захисту даних у структурі кожного органу влади [16]. Аналізуючи перспективи вітчизняного кіберпростору, І. О. Кульчій спільно з Є. О. Бітюгою доводять необхідність повної концептуальної перебудови українського законодавства, оскільки косметичні зміни вже не є ефективними [18]. П. В. Цимбал також поділяє цю позицію, вказуючи на гостру потребу посилення публічно-правового захисту інформації саме за стандартами ЄС [49].

Розуміння нормативної бази вимагає аналізу її впровадження на рівні місцевого самоврядування, де державні рамки стають реальними інструментами.

Муніципалітети адаптують теорію до практики через інструкції з е-діловодства та правила цифрової поведінки службовців. Саме якість цих локальних актів визначає, чи буде система безпеки дієвою, чи залишиться лише декларацією.

Найкраще такий системний підхід ілюструють комплексні регіональні стратегії. Показовим прикладом є реалізація програми «Цифрова Полтавщина» на період 2024–2026 років [39]. Цей документ є не просто набором гасел, а деталізованим планом дій, який регламентує фінансування ІТ-інфраструктури області та алгоритми взаємодії місцевої влади із силовими структурами. Впровадження подібних ініціатив підтверджує, що надійність цифрового контуру сьогодні безпосередньо гарантує збереження життєдіяльності та легітимності влади в умовах інформаційного суспільства.

Підбиваючи підсумки, можна сказати, що Україна збудувала серйозну та динамічну юридичну базу для захисту інформації в регіонах. Ми подолали великий шлях - від загальних гасел до конкретного «кіберзаконодавства». Незважаючи на це, практична реалізація інформаційної безпеки в органах місцевого самоврядування ускладнюється трьома ключовими проблемами:

1. Складність балансування між відкритістю влади та безпекою під час війни.
2. Дефіцит коштів на виконання дорогих технічних вимог держави.
3. Необхідність постійної модернізації під суворі європейські стандарти.

Наразі юридичний простір зазнає безперервних трансформацій через чинник війни. Такий стан зобов’язує керівників не лише орієнтуватися в нормах, а й проявляти адаптивність та вміння негайно інтегрувати актуальні безпекові засади в професійні процеси.

РОЗДІЛ 2. АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ

2.1. Аналіз діяльності органів місцевого самоврядування із забезпечення захисту інформаційних ресурсів в умовах воєнного стану.

В умовах воєнного стану державний апарат стикається з новими безпековими викликами. На тлі повномасштабної збройної агресії рф ці виклики цифрової епохи стали ще гострішими [8]. Воєнний стан змусив докорінно переформатувати саму архітектуру публічного адміністрування, якщо раніше держава орієнтувалася переважно на планове розширення зручних онлайн-сервісів, то зараз абсолютним пріоритетом стали тотальний кіберзахист і фізичне збереження даних.

Цей екстраординарний режим безпосередньо вплинув на роботу органів місцевого самоврядування. Він змінив їхні повноваження та формати взаємодії з держсектором. Найбільше це відчувається у прифронтових зонах: там повноцінно виконувати самоврядні функції вкрай складно через постійну загрозу бойових дій [2].

Модернізацію управління публічними даними довелося почати з перегляду політики відкритості. Щоб зберегти національний суверенітет, уряд був змушений терміново обмежити доступ до базових систем - зокрема, до порталу відкритих даних, кадастрових та майнових реєстрів. Згортання такої транспарентності виявилося фактично єдиним можливим кроком для блокування ворожого кібершпигунства. Вільний обіг інформації створював надто серйозні ризики: від випадкового розкриття даних військовослужбовців до пошуку вразливостей у комунальній інфраструктурі міст.

Водночас таке різке закриття даних спровокувало певні інституційні суперечності. На муніципальному рівні вони проявилися чи не найгостріше. Змінилися вектори комунікації між депутатським корпусом та військовими адміністраціями. Наразі в Україні досі немає якоїсь уніфікованої моделі їхньої

координації, а на практиці все залежить від безпекового статусу конкретного регіону та його близькості до лінії фронту [20].

Окрім ризику маніпуляцій, українські платформи зіткнулися з реальними і дуже масштабними кібератаками з боку агресора. Це і масовані DDoS-атаки, і застосування шкідливих програм-вайперів, що змусило швидко переходити до проактивного ризик-менеджменту [24]. До того ж, з'явилася цілком реальна фізична (кінетична) загроза серверам у містах. Стратегічним виходом для порятунку баз даних стала фундаментальна зміна архітектури їх збереження - легалізація підходу «Cloud First», тобто першочергового використання хмарних технологій [40]. Це дозволило перенести критичні реєстри на хмарні сервери світових гігантів, таких як AWS, Microsoft Azure та Google Cloud. Систематизацію цих змін наведено у таблиці 2.1.

Таблиця 2.1

Порівняльна характеристика політики управління державними інформаційними ресурсами

Параметр	*До повномасштабного вторгнення*	*В умовах воєнного стану*
Основний вектор розвитку	Планове вдосконалення сервісів	Тотальний кіберзахист та фізичне збереження даних
Рівень відкритості	Контрольована відкритість даних та відповідність критеріям українських рейтингів ефективності	Блокування відкритого доступу до Кадастрової карти та ДРПРА як вимушений крок для протидії ворожій розвідці
Пріоритет безпек	Підтримка базових протоколів цифрової безпеки	Режим превентивного захисту та перехід до "Cloud First"
Модель управління	Централізована/планова	Гнучка, адаптивна та проактивна

Розроблено автором за матеріалом [2, 20, 24]

Дані з таблиці 2.1 чітко показують, як саме змінився управлінський вектор. З початком великої війни вимога бути публічно прозорими відійшла на другий

план, повністю поступившись місцем жорсткій кіберстійкості та інформаційній закритості. Впровадження хмарних рішень фактично врятувало стабільну роботу місцевого самоврядування. Навіть якби сервери в якійсь громаді були фізично знищені, доступ до ключових реєстрів все одно залишався б безперебійним.

Такий підхід не просто захистив стратегічні дані від ракетних ударів, а й загалом посилив кібербезпеку національної мережі. Муніципалітети змогли продовжувати роботу в найбільш критичні моменти, адже їхня життєво важлива інформація більше не залежала від вразливого локального обладнання. Як наслідок, фізична адреса органу влади перестала бути критичною точкою вразливості.

Ще одним важливим досягненням стала неймовірна стійкість екосистеми «Дія». Замість прогнозованого падіння, електронні платформи навпаки перетворилися на головний вузол зв'язку між державою і суспільством. Автоматизація послуг, як-от оформлення статусу ВПО чи виплати «єПідтримка», дуже сильно розвантажила територіальні громади та ЦНАПи. Електронні паспорти спростили мобільність біженців, а система довела, що здатна витримувати пікові навантаження. Щоправда, окремим випробуванням стали обстріли енергетики у 2022–2023 роках. Вони показали, що навіть найкращі хмарні сервіси не будуть працювати без локальної автономності на місцях (наявності генераторів та терміналів Starlink). Межа між суто технічним ІТ-забезпеченням та загальною логістикою на певний час просто зникла.

Загалом можна констатувати, що державні ресурси пройшли етап адаптації успішно. Однак на місцевому рівні ситуація куди складніша і залишається зоною підвищеного ризику. Саме в територіальних громадах концентрується найбільше чутливих соціальних даних. Але при цьому їм катастрофічно бракує фінансів та техніки для забезпечення нормального рівня безпеки.

Свого часу децентралізація передала на місця величезні масиви інформації: містобудівні бази, реєстри пацієнтів та мешканців, дані ЦНАПів. Тепер ці відомості зосереджені на місцевих серверах, що робить їх привабливою ціллю для російських кібервійськ. На жаль, більшість місцевих рад стикається з

великими перешкодами, намагаючись захиститися від цих загроз. Воєнний стан створив для них подвійне навантаження: потрібно одночасно надавати критичні публічні послуги людям і екстрено відбиватися від хакерських атак [12]. Цілком логічно, що гроші йдуть передусім на оборону та соціальну підтримку, тоді як цифрова безпека фінансується за залишковим принципом [45]. Багато громад фізично не можуть дозволити собі закупити дороге ліцензійне програмне забезпечення чи системи запобігання вторгненням (IDS/IPS).

Окрім хронічного недофінансування, є ще один гострий виклик - дефіцит профільних айтівців. ОМС не здатні конкурувати із зарплатами в комерційному секторі. Через це функції кіберзахисту часто просто скидають на звичайних системних адміністраторів. Їхніх навичок зазвичай вистачає лише на базове оновлення антивірусів, чого абсолютно недостатньо для протидії серйозним цілеспрямованим APT-загрозам. Ситуацію також ускладнює дія Закону України «Про захист інформації в ІКС» [31]. Він вимагає обов'язкової наявності атестата на Комплексну систему захисту інформації. Процедура ця настільки довга і дорога, що чимало рад роками працюють у юридичній «сірій зоні», залишаючись відкритими для атак.

Але найсприятливіше підґрунтя для нападів формує так званий людський фактор - низький рівень цифрової гігієни самих службовців [48]. Ігнорування правил інформаційної дисципліни здатне звести нанівець навіть найпотужніший технічний захист [6]. Ворожі хакери дуже активно цим користуються. Вони розсилають вірусні листи, майстерно замасковані під офіційні директиви від ОВА чи СБУ (спірфішинг). Оскільки мережі в міськрадах часто не сегментовані, один необачний клік може миттєво інфікувати всі комп'ютери місцевої ради. Головна ціль таких атак під час війни - цифровий терор. Тобто використання програм-вайперів для того, щоб безповоротно знищити бази даних. Коли ЦНАП чи управління соцзахисту не може працювати, це паралізує роботу влади та підриває довіру громадян до держави.

Паралельно ворог використовує OSINT-інструменти розвідки на основі відкритих джерел [43]. Уважно аналізуючи загальнодоступний контент (рішення

рад чи навіть соцмережі посадовців), супротивник конструює вузькоспрямовані сценарії вторгнень.

Незважаючи на всі ці виклики, безпекові стратегії на місцях поступово покращуються. Завдяки спільній роботі з Держспецзв'язку та CERT-UA, громади вчаться моніторити аномалії в мережі. Визначальним кроком стала міграція муніципальних реєстрів у хмарні інфраструктури [46]. Це зняло ризик втрати даних під час блекаутів і спростило процедуру отримання КСЗІ, адже хмарні провайдери вже мають усі необхідні сертифікати. Також варто згадати нові регіональні програми інформатизації, як-от «Цифрова Полтавщина» [39]. У них нарешті почали закладати цільове фінансування саме на кібероборону.

Проте в Україні досі зберігається глибока структурна нерівність. Існує справжня прірва між потужними міськими радами (які мають власні IT-департаменти і працюють за стандартом ISO 27001) та невеликими громадами, де весь кіберзахист тримається на старих серверах. Цю тенденцію добре видно з таблиці 2.2.

Таблиця 2.2

Порівняльна характеристика підходів до кіберзахисту: великі міста vs малі громади

Параметр порівняння	*Великі міські ради*	*Малі територіальні громади*
Кадрове забезпечення	Наявність власних IT-департаментів.	Відповідальність покладена на системних адміністраторів або загальні відділи.
Стандартизація	Впровадження міжнародних стандартів ISO/IEC 27001.	Процеси захисту перебувають у зародковому стані.
Технологічний рівень	Можливість утримання власних захищених серверів або хмарних рішень.	Залежність від фізично зношених серверів (до моменту міграції в хмару).
Шляхи розвитку	Самостійна розбудова комплексних систем.	Міжмуніципальне співробітництво; послуги MSSP-провайдерів

Розроблено автором на результатах дослідження [48]

Така асиметрія підштовхує до логічного висновку: громадам треба шукати консолідовані формати оборони. Зокрема, розвивати міжмуніципальне партнерство та делегувати питання безпеки стороннім профільним структурам.

Підбиваючи підсумки, можна стверджувати, що система місцевого самоврядування в Україні зараз проходить через надзвичайно складний етап трансформації. Реалії воєнного часу оголили давні проблеми з бюджетами і нестачею фахівців. Але, з іншого боку, саме ці виклики змусили органи влади швидко реагувати і переводити свої дані в безпечні хмарні середовища.

2.2. Дослідження ключових проблем та вразливостей у системі інформаційної безпеки Полтавської обласної ради

Діяльність Полтавської обласної ради у поточному безпековому середовищі відбувається в умовах небувалих випробувань та ризиків. Згідно з висновками С. Ю. Бойка та А. В. Маринiва, запровадження правового режиму воєнного стану кардинально змінює конфігурацію потенційних загроз, що спонукає інституції місцевого самоврядування до динамічного коригування власних управлінських підходів [2].

Полтавський регіон наразі виконує функцію опорного тилового хабу, який забезпечує інтеграцію релокованих підприємств та адаптацію значних потоків внутрішньо переміщених осіб. Така специфіка посилює вимоги до стабільності, безперервності та захищеності комунікаційних систем місцевої влади. Зараз виконавчий орган облради координує роботу з великими обсягами стратегічних даних - від оборонних програм та фінансування бюджету до особистої таємної інформації громадян. Оцінка архітектури інформаційної інфраструктури органу дає змогу ідентифікувати організаційні, технологічні та кадрові вразливості, котрі створюють передумови для кіберінцидентів і потребують оптимізації. Аналіз поточної ситуації свідчить, що статус Полтавщини як стратегічного тилового хабу вимагає від органів місцевого самоврядування особливої уваги до цілісності інформаційних потоків. Проте існуюча модель безпеки в обласній раді наразі характеризується багатовекторністю вразливостей, які мають як технічне,

так і управлінське походження. Зокрема, поєднання фрагментарної ІТ-інфраструктури з недосконалими процедурами внутрішнього діловодства створює передумови для реалізації кіберзагроз різного рівня складності. Щоб впорядкувати виявлені ризики та визначити пріоритети для посилення захисту, їх згруповано за функціональними категоріями. Результати систематизації наведено в таблиці 2.3.

Таблиця 2.3

Класифікація вразливостей інформаційної інфраструктури Полтавської обласної ради

Категорія вразливості	*Опис конкретної проблеми*	*Наслідки для безпеки*
Технологічна	Фрагментація інфраструктури та відсутність єдиного системного підходу до інтеграції комплексів.	Зниження рівня захищеності відомостей та підвищення ризику несанкціонованого доступу.
Організаційна	«Гібридний» характер діловодства (поєднання паперових та цифрових носіїв).	Мультиплікація ризиків людського фактора та спотворення змісту документації.
Комунікаційна	Використання «Тіньового ІТ»: Telegram, Viber, приватні пошти.	Вихід процесів за межі захищеного периметра, неможливість застосування DLP-систем.
Доступ і привілеї	Відсутність концепції «нульової довіри»; надання прав доступу цілим підрозділам.	Можливість автоматичного розширення доступу зловмисників до масивів даних у разі компрометації однієї станції.
Нормативна	Дефіцит актуальних інструкцій з реагування на інциденти.	Неможливість швидкої ізоляції загрози (наприклад, вірусу-вимагача) технічним персоналом.

Розроблено автором за матеріалом [6, 39]

Зібрані дані чітко показують, що проблеми безпеки обласної ради виникають не лише через технології, а й через її організаційну структуру. Ці недоліки накопичилися та створили серйозні ризики. Тому необхідно ретельно вивчити щоденні процеси: як ведуться документи та канали зв'язку для співробітників. Ключовим документом, який визначив напрямок розвитку цього ІТ-регіону, став регіональний план «Цифрова Полтава» на 2024-2026 роки [39]. План показав, що влада усвідомлювала серйозність загроз і була готова змінити свій підхід. Основна увага зосереджувалася вже не лише на закупівлі технологій, а на створенні єдиної екосистеми, в якій безпечні сервери та цифрова грамотність співробітників були нероздільними.

Реалізації цієї мети на практиці перешкоджав хаос. Роками різні відомства використовували різні програми та комп'ютери. Сьогодні інтеграція всього цього в надійну мережу є критичним, але технічно складним завданням. Таке розмаїття призвело до вразливостей та ускладнило швидкий захист від хакерських атак. Поряд з цим, обласна рада також підтримує тісний контакт з Радою національної-безпеки і оборони та 60 місцевими громадами.

Дослідницька група під керівництвом Д. Тищенка зазначила, що відсутність єдиної системи зв'язку між відомствами всіх рівнів є основною проблемою, яка знижує рівень безпеки [48]. Найбільший ризик виникає під час передачі електронних документів. Документи легко перехоплюються, коли вони передаються з регіональних відомств до невеликих громад зі слабким рівнем безпеки. Багато вразливостей приховано в щоденній діяльності відомств, що чітко демонструє приклад відділів організаційної підтримки. Спостереження за реальним процесом підготовки засідань, роботи постійних комітетів та складання проектів резолюцій виявляє очевидний факт: незважаючи на впровадження систем електронного документообігу, персонал все ще змушений працювати в «гібридному» режимі, постійно повторюючи цифрові процеси та ручні перевірки паперових документів.

На практиці це призводить до того, що працівники апарату змушені витрачати левову частку свого робочого часу на механічну рутину. Йдеться,

зокрема, про постійну візуальну звірку паперових оригіналів документів із їхніми електронними версіями в системі. Класичним прикладом такого "вузького місця" є процедура ручного перенесення правок, погоджень чи резолюцій від уповноважених осіб та профільних комісій до загальної цифрової бази.

Така подвійна робота свідчить про функціонування так званого "гібридного" документообігу, коли електронна система існує, але паралельно дублюється папером. Відсутність послідовності єдиного цифрового процесу не просто уповільнює підготовку проєктів рішень. Вона у разі підвищує ризики, пов'язані з людським фактором, оскільки через звичайну втому чи неуважність персоналу виникають механічні помилки під час ручного вводу.

Не менш важливою проблемою є загроза цілісності даних. Переривчастий потік інформації та наявність кількох розбіжних копій (паперової та цифрової) формують ідеальне середовище для маніпуляцій. Саме на етапі такого "ручного перенесення" виникає найбільша ймовірність того, що зміст документа буде навмисно чи випадково викривлено ще на етапі його погодження, тобто задовго до офіційного оприлюднення фінального тексту на веб–ресурсах ради.Водночас, на переконливу думку А. В. Кузьменка, який досліджував специфіку інформаційної безпеки в системі публічного управління, застосування несертифікованих комунікаційних каналів становить одну з найбільш гострих проблем для сучасних владних інституцій [13]. Попередні проєкти нормативних актів, робочі драфти рішень та внутрішня службова кореспонденція в апараті ради доволі часто передаються за допомогою загальнодоступних месенджерів (зокрема Telegram чи Viber), а також через приватні електронні поштові скриньки працівників. Практика залучення подібних інструментів «тіньового ІТ» задля прискорення обміну інформацією фактично виводить вагому частку внутрішньоорганізаційних процесів за межі захищеного периметра установи. Це унеможливлює функціонування механізмів запобігання витокам відомостей, а також прямо суперечить чинним нормативно-правовим імперативам у сфері захисту службової інформації.

Стихійне впровадження моделі BYOD 84 депутатами Полтавської обласної ради, які використовують власні гаджети для роботи з документацією, створює критичні безпекові прогалини. Через неможливість встановлення єдиних корпоративних стандартів захисту та шифрування на приватних пристроях виникає масштабна поверхня атаки. За таких умов компрометація навіть одного пристрою дозволяє зловмисникам отримати доступ до службових даних, фактично нівелюючи ешелоновану систему захисту центральних серверів установи. Вагомою проблемою залишається забезпечення захисту публічних електронних ресурсів, серед яких ключове місце посідає офіційний вебсайт Полтавської обласної ради [25]. З одного боку, норми вітчизняного законодавства імперативно вимагають підтримання прозорості діяльності влади шляхом регулярного оприлюднення нормативних актів, фінансової звітності та поіменних результатів волевиявлення депутатів. Проте в реаліях збройного конфлікту така інформаційна відкритість генерує латентні безпекові ризики.

Як обґрунтовано доводять у своїх працях Д. С. Афонін та Н. П. Свиридюк, надлишкова деталізація оприлюднених даних формує сприятливе середовище для здійснення розвідки за відкритими джерелами (OSINT), інструментарій якої інтенсивно експлуатується ворожими спецслужбами [43]. Розміщені на вебпорталі контактні відомості очільників структурних підрозділів, розклади прийому громадян та розгорнута організаційна схема виконавчого апарату слугують базою для конструювання вузькоспрямованих (таргетованих) фішингових кампаній проти конкретних посадовців. Поряд із цим, офіційні вебресурси місцевої влади перманентно стають мішенями для масованих DDoS-атак, що своєю чергою актуалізує потребу в гарантуванні відмовостійкості серверного хостингу та систематичному оновленні архітектури систем управління контентом. Окрему групу викликів становлять ризики, зумовлені залученням приватних технічних засобів у робочі процеси та необхідністю забезпечення публічної діяльності ради. Систематизацію цих специфічних загроз наведено нижче (табл. 2.4).

Таблиця 2.4

Аналіз ризиків моделі BYOD та функціонування публічних вебресурсів

Об'єкт аналізу	Ключові чинники ризику	Прогнозовані загрози та наслідки
Депутатський корпус (Модель BYOD)	Використання 84 депутатами власних лептопів та смартфонів для роботи з документами без відриву від основної роботи1.	Неможливість впровадження єдиних стандартів антивірусного захисту; компрометація одного гаджета відкриває шлях до серверів ради.
Офіційний вебсайт ради	Законодавча вимога щодо оприлюднення фінансової звітності, контактів та персональних даних посадовців.	Використання даних для OSINT-розвідки, підготовка таргетованого фішингу проти керівництва, ризик DDoS-атак.
Системи управління	Необхідність постійного оновлення архітектури сайтів та забезпечення відмовостійкості.	Технологічні вразливості, що можуть призвести до зупинки роботи офіційних ресурсів або спотворення інформації.

Складено автором за матеріалом [43, 25]

Зіставлення цих чинників вказує на надзвичайну масштабність поверхні атаки, що виникає через складність контролю приватних пристроїв та надмірну відкритість оприлюднених даних. Це підкреслює потребу в переході від ситуативного захисту до ешелонованої системи безпеки, здатної нейтралізувати загрози навіть у разі компрометації окремих точок доступу.

Оцінюючи внутрішню політику розмежування прав доступу в апараті ради, варто відзначити відсутність жорстко регламентованих механізмів. Надання дозволів на роботу з файловими архівами та локальними базами здебільшого здійснюється на рівні цілих структурних підрозділів, тоді як концепція «нульової довіри» та принцип мінімально необхідних привілеїв для кожного конкретного службовця відповідно до його посадової інструкції фактично не реалізуються. Як наслідок, у ситуації компрометації робочої станції окремого співробітника (зокрема, через активацію фішингового повідомлення,

стилізованого під директиву Полтавської ОВА), кіберзлочинці отримують можливість автоматично розширити свій доступ до всього масиву документації відповідного управління.

Водночас найбільш вразливим елементом безпекової архітектури продовжує виступати людський фактор. Це цілком узгоджується з позицією Ю. Д. Гундертайло, яка наголошує, що в реаліях воєнного стану дотримання правил цифрової гігієни перетворюється на життєво важливий імператив [6]. Посадові особи загального відділу, підрозділу роботи зі зверненнями громадян та інших структурних ланок, які у щоденному режимі опрацьовують значні обсяги зовнішньої кореспонденції, стають пріоритетними цілями для застосування методів соціальної інженерії. Дефіцит регулярних практичних навчань та відсутність періодичних симуляцій кібернетичних інцидентів позбавляють персонал можливості сформувати стійкі компетенції щодо оперативного виявлення латентних загроз під час виконання рутинних операцій.

Останнім критичним аспектом, що потребує уваги, виступає нормативно-процедурна незахищеність. У межах інформаційної інфраструктури представницького органу фіксується гострий дефіцит актуалізованих та доведених до відома кожного співробітника інструкцій з реагування на безпекові події. Чинні внутрішні документи, якими регламентується експлуатація цифрового обладнання в обласній раді, переважно є застарілими і не відповідають стрімкій еволюції новітніх кібернетичних викликів. За відсутності деталізованих алгоритмів щодо першочергових дій у критичні хвилини після ідентифікації вірусу-вимагача або факту масштабної компрометації баз даних, нетехнічний персонал об'єктивно не зможе швидко ізолювати проблему. Як наслідок, це генерує пряму загрозу цілковитої зупинки операційної діяльності органу місцевого самоврядування.

Підбиваючи підсумки проведеного аналізу, варто наголосити, що архітектура інформаційної безпеки Полтавської обласної ради характеризується багатовекторними вразливостями. Спектр ідентифікованих загроз охоплює недоліки гібридного формату діловодства, неконтрольовану реалізацію моделі

BYOD серед депутатського корпусу, а також складний баланс між законодавчою вимогою публічності офіційного вебпорталу та ризиками ворожої розвідки за відкритими джерелами (OSINT). Ефективне нівелювання цих фундаментальних викликів, механізми подолання яких частково закладені у стратегічні орієнтири регіональної програми «Цифрова Полтавщина» [39], зумовлює нагальну потребу відмовитися від ситуативних заходів захисту на користь формування цілісної та багаторівневої системи управління інформаційною безпекою установи.

Реалії воєнного стану переорієнтували державну інформаційну політику з відкритості на тотальну кіберстійкість, де реалізація принципу «Cloud First» та адаптивність екосистеми «Дія» убезпечили критичні реєстри від кінетичних і цифрових ударів. Проте в муніципальному сегменті зберігається значна безпекова асиметрія порівняно з центром: через фінансовий дефіцит, кадровий голод та низьку цифрову гігієну персоналу громади залишаються вразливими до фішингу та соціальної інженерії. Подолання цього розриву потребує переходу до консолідованої оборони, зокрема шляхом розвитку міжмуніципального співробітництва та ширшого масштабування хмарних рішень на місцях.

Практичний аудит системи інформаційної безпеки Полтавської обласної ради дозволив ідентифікувати комплекс специфічних вразливостей, що мають багатовекторний характер. Найбільш критичними ризиками визначено «гібридний» формат діловодства, стихійне використання депутатами моделі BYOD та залучення незахищених каналів комунікації (месенджерів) для службової переписки. Відсутність чіткої стратегії «нульової довіри» та застарілі регламенти реагування на інциденти суттєво розширюють поверхню можливих атак, створюючи загрозу цілісності стратегічних даних. Таким чином, встановлено, що забезпечення кіберстійкості представницького органу вимагає негайного переходу від ситуативних заходів до формування цілісної багаторівневої системи управління інформаційною безпекою.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

3.1. Адаптація міжнародного досвіду в сфері інформаційної безпеки в органах місцевого самоврядування.

Рівень захищеності, конфіденційності та доступності інформаційних масивів у розподілених мережах нині є головним мірилом ефективності державного менеджменту, що чітко простежується у працях М. Білецького [1, с. 58]. В епоху тотальної цифровізації та постійних кібератак, зумовлених військовою агресією, безпека ресурсів ОМС переросла рівень суто локальних ІТ–завдань. За визначенням Ю. В. Гончарука [5, с. 49], цей процес став невід'ємною частиною стратегічного захисту країни.

Стратегічним орієнтиром для нормативно–правової модернізації українських громад є досвід Європейського Союзу, що базується на пріоритеті прав людини. Стрижнем цієї системи, як досліджує О. Дєгтяр, є Загальний регламент про захист даних та імплементована ним концепція «Privacy by Design» [7, с. 224]. Цей підхід передбачає інтеграцію засобів захисту в архітектуру муніципальних платформ ще на стадії їх проєктування. Для українських реалій, за висновками Л. Сорокіної [46] та І. О. Кульчій [14], це означає необхідність адаптації законодавства до європейських вимог щодо обігу електронних даних та встановлення персональної відповідальності керівників. Додатково С. Кавин доводить високу результативність створення автономних посад Офіцерів із захисту даних усередині владних структур [10, с. 145]. Водночас Директива ЄС про мережеву та інформаційну безпеку встановлює принцип «негайного реагування» з обов'язковим повідомленням про інцидент протягом 24 годин.

У технологічному вимірі еталоном децентралізованої безпеки є досвід естонського проєкту e–Estonia та платформи міжвідомчої взаємодії X–Road. Ця модель переконливо доводить, що розподілене зберігання даних в окремих

органах влади та їх обмін виключно зашифрованими каналами запобігає каскадному зламу всієї мережі у разі компрометації одного з її сегментів. Для українських муніципалітетів в умовах воєнного стану такий підхід є критично важливим, оскільки він повністю ліквідує концепцію «єдиної точки відмови» (single point of failure). Фізичне пошкодження або кіберзлам локального сервера в одній громаді за такої архітектури не призводить до колапсу всієї системи публічного управління. Додатковим інноваційним інструментом верифікації та контролю цілісності реєстрів в Естонії виступає технологія KSI Blockchain. Вона дозволяє фіксувати кожну операцію з даними через створення унікальних незмінних цифрових «хешів». Це унеможливлює будь–яке несанкціоноване втручання, ретроактивну підробку чи приховане видалення відомостей, гарантуючи органам місцевого самоврядування абсолютну достовірність їхньої цифрової історії.

Паралельно з децентралізацією значний інтерес викликає сінгапурська стратегія «Smart Nation», яка демонструє переваги практичного впровадження архітектури «нульової довіри». Основний імператив цієї концепції базується на принципі «нікому не довіряй, завжди перевіряй», що повністю виключає автоматичне надання системних привілеїв будь–якому користувачу чи пристрою всередині мережевого периметра. Автоматизований інтелектуальний моніторинг поведінкових аномалій у Сінгапурі дозволяє миттєво блокувати підозрілу активність навіть легітимних посадовців, мінімізуючи як зовнішні загрози, так і внутрішні ризики, пов’язані з компрометацією облікових записів чи діями інсайдерів.

Адаптуючи цей передовий міжнародний досвід до сучасних вітчизняних реалій, як зазначають Д. Тищенко, М. Чорний та Я. Шестак та [48, с. 1540], безальтернативним пріоритетом для українських ОМС стає повна відмова від вразливих локальних серверів на користь розбудови Комплексних систем захисту інформації та масштабної міграції муніципальних реєстрів до хмарних середовищ. Дослідники наголошують, що утримання фізичного серверного обладнання в межах адміністративних будівель місцевих рад створює подвійну

небезпеку: кінетичну та технічну. Перенесення критично важливих масивів інформації – містобудівних кадастрів, баз даних ЦНАПів та соціальних реєстрів – у захищені урядові або сертифіковані комерційні «хмари» гарантує безперервність надання публічних послуг за будь–яких умов. Водночас обов'язкове розгортання атестованих КСЗІ для кожного інформаційно–комунікаційного вузла дозволяє юридично легалізувати ці процеси, створюючи цілісний, нормативно та технічно захищений контур муніципальної кібербезпеки.

У контексті стратегічного планування вагомим для вітчизняної практики є досвід США. Зокрема, розроблений Національним інститутом стандартів і технологій уніфікований фреймворк дій. Який переорієнтовує муніципалітети з концепції «глухої оборони» на забезпечення кіберстійкості. З метою комплексного відображення процесів безпекового оновлення в органах місцевого самоврядування, ключові вектори модернізації відповідної державної політики доцільно структурувати у вигляді цілісної моделі (див. табл. 3.1).

Таблиця 3.1

Стратегія кібербезпеки для місцевої влади

Етап	*Назва кроку*	*Основна мета та дії*	*Зв'язок із джерелами*
1	Визначення активів	Ідентифікація критично важливих даних, систем та інфраструктури громади.	Початок системного аналізу структури.
2	Захист	Створення багаторівневих бар'єрів захисту	Забезпечення стабільності інфраструктури.
3	Виявлення	Безперервний моніторинг для швидкої ідентифікації аномалій або фактів вторгнення.	Боротьба з загрозами у реальному часі.
4	Реагування	Чіткий алгоритм дій для локалізації загрози та мінімізації наслідків атаки.	Захист управлінських процесів від збоїв.
5	Відновлення	Повернення систем до нормального функціонування та аналіз помилок.	Гарантування безперервності надання послуг («Держава у смартфоні»)

Розроблено автором за матеріалом [1, 7]

Практична реалізація цих стратегій неможлива без відповідного фінансового забезпечення. Британська програма «Cyber Essentials» засвідчує, що переважна більшість успішних атак на муніципалітети спричинена порушенням базової цифрової гігієни. З метою стимулювання дисципліни британський уряд надає державне фінансування муніципалітетам лише за умови впровадження ними базових стандартів кіберзахисту. Для України це означає необхідність розробки механізму цільових субвенцій для малозабезпечених громад. Важливим інструментом нівелювання нестачі бюджетних коштів є обґрунтована М. Криштановичем модель колективного захисту MS–ISAC та застосування Crowd–технологій [11, с. 188]. Впровадження в ОМС України офіційної співпраці з ІТ–спільнотою через ініціативи Bug Bounty дозволить превентивно закривати «діри» в системах.

У цьому контексті фінансова модернізація державної політики має базуватися на принципі «безпека в обмін на інвестиції», що дозволить безпосередньо адаптувати британський досвід у вітчизняну практику публічного управління. Розподіл цільових державних субвенцій на цифровізацію ОМС не повинен бути автоматичним чи зрівнялівським; його варто чітко пов’язати з виконанням громадами обов’язкового безпекового мінімуму – від обов’язкового впровадження двофакторної автентифікації для всіх службовців до регулярного резервного копіювання реєстрів у хмарні сховища. Крім того, подолання дефіциту ресурсів у невеликих територіальних громадах потребує нормативного врегулювання моделей міжмуніципального співробітництва у сфері ІТ. Замість неефективного фінансування окремого системного адміністратора в кожній сільській чи селищній раді, доцільно запровадити практику спільного утримання або аутсорсингу послуг єдиного профільного центру кіберзахисту (MSSP–провайдера) для кількох суміжних громад. Такий підхід дозволить значно оптимізувати обмежені бюджетні видатки ОМС, забезпечить професійний рівень цілодобового моніторингу мережевих аномалій та допоможе ліквідувати існуючий цифровий розрив між великими містами та фінансово спроможними регіонами.

Жодна технологічна модернізація не забезпечить бажаного результату без мінімізації «людського фактора», який залишається однією з головних уразливостей у системі захисту муніципальних інформаційних ресурсів. Сучасна практика доводить, що навіть найдорожчі ліцензійні інструменти захисту чи системи виявлення вторгнень втрачають ефективність, якщо посадові особи ігнорують правила базової інформаційної дисципліни. Цим активно користуються зловмисники, застосовуючи методи соціальної інженерії та розсилаючи шкідливе програмне забезпечення під виглядом офіційних директив.

Спираючись на міжнародний досвід (зокрема, практику країн Скандинавії), М. Вовжиняк [3] та Я. Ю. Цимбаленко [50] наголошують, що цифрова грамотність має стати обов'язковим кваліфікаційним критерієм при прийнятті громадян на службу в органи влади. При цьому процес підвищення кваліфікації персоналу повинен вийти за межі формального прослуховування лекцій. Муніципальні службовці мають проходити регулярні практичні стрес–тести наприклад, отримувати від внутрішніх ІТ–відділів імітовані фішингові листи для перевірки їхньої пильності в реальному часі. Посадовці, які демонструють низький рівень цифрової гігієни під час таких перевірок, повинні в обов'язковому порядку направлятися на додаткові практичні навчання.

Крім того, в умовах гібридної агресії кіберзахист ОМС тісно переплітається з протидією інформаційно–психологічним операціям ворога, спрямованим на підрив управлінських процесів на місцях. Як стверджують О. В. Литвинчук та Н. В. Гришина, здатність місцевої влади до прозорої антикризової комунікації з населенням після кіберінцидентів значно підвищує довіру до державних інституцій [21]. Оперативне й чесне інформування громади про причини тимчасових технічних збоїв (наприклад, у роботі сервісів ЦНАП через масовані DDoS–атаки чи пошкодження локальної інфраструктури) дозволяє уникнути управлінського вакууму. Такий відкритий діалог мінімізує ризики поширення панічних настроїв серед мешканців, блокує ворожі маніпуляції в медіапросторі та демонструє готовність системи до подолання кризових ситуацій.

Для комплексного вирішення проблеми кадрового дефіциту та посилення інституційної координації, відповідно до Стратегії кібербезпеки України [47], доцільним є розгортання регіональних центрів кіберзахисту на базі обласних військових адміністрацій. Узагальнення проаналізованого міжнародного досвіду дозволяє сформувати цілісну концепцію реформування сектору безпеки в українських муніципалітетах (табл. 3.2).

Таблиця 3.2

Вектори модернізації державної політики у сфері муніципальної кібербезпеки

Вектор модернізації	*Зміст та стратегічні пріоритети*	*Очікуваний результат для громад*
Нормативно–правовий	Імплементація стандартів ЄС та GDPR4, впровадження жорстких протоколів обробки даних та персональної відповідальності керівників3.	Створення уніфікованого та захищеного правового поля для роботи з реєстрами.
Технологічний	Відмова від локальних систем на користь централізованих архітектур, розбудова КСЗІ5 та міграція в урядові хмарні середовища6.	Технічна стійкість інфраструктури та гарантоване збереження даних.
Фінансово–ресурсний	Запровадження цільових державних субвенцій для покриття ІТ–видатків малозабезпечених громад7.	Подолання «цифрового розриву» між великими містами та сільськими радами.
Інноваційний	Використання Crowd–технологій та залучення ІТ–спільноти до аудиту вразливостей через ініціативи Bug Bounty8.	Превентивне виявлення «дірок» у системі до моменту їх використання ворогом.
Інституційний	Розгортання регіональних хабів кіберзахисту на базі ОВА для методологічного супроводу ОМС.	Вирішення проблеми кадрового дефіциту через централізовану експертну підтримку.

Розроблено автором за матеріалом [11, 40, 47]

Підсумовуючи, формування нових підходів до захисту муніципальних даних вимагає відходу від фрагментарності. Запропоновані вектори модернізації формують багаторівневий захисний контур, де нормативні обмеження органічно підкріплюються технологічною досконалістю та ресурсною спроможністю. Такий підхід трансформує систему місцевого самоврядування з пасивного об'єкта атак на активного учасника національної системи безпеки, створюючи надійний фундамент для цифрової трансформації регіонів.

3.2. Пріоритети удосконалення напрямів інформаційної безпеки України та Полтавської області

Практична площина публічного управління диктує нові умови: сьогодні загальнонаціональні стратегії кібербезпеки не працюватимуть без їх жорсткої прив'язки до реалій конкретних регіонів та громад. Затяжний воєнний стан довів, що територіальні громади є справжнім фундаментом національної стійкості. Проте цей статус має і зворотний бік: муніципальні інформаційні мережі автоматично опинилися під прицілом ворожих кібератак та цілеспрямованих інформаційно–психологічних операцій. Аналізуючи цей феномен, І. Єфіменко справедливо наголошує на необхідності розбудови децентралізованого, багатоешелонованого захисту [8, с. 102]. Суть такого підходу полягає в тому, щоб кожен регіон міг автономно відбивати цифрові загрози, залишаючись при цьому невід'ємною частиною загальнонаціонального безпекового контуру. Для Полтавщини цей виклик є безпрецедентно гострим. Узявши на себе роль одного з ключових гуманітарних, логістичних та військово–адміністративних хабів країни, область об'єктивно потребує термінового перегляду механізмів захисту даних в органах місцевого самоврядування. Практичним майданчиком для такої модернізації та посилення інституційної спроможності місцевих рад має стати цілеспрямоване виконання заходів регіональної програми «Цифрова Полтавщина» на 2024–2026 роки [39].

Базовим пріоритетом технологічного оновлення на рівні регіону стає забезпечення безперебійної роботи органів місцевого самоврядування та

недоторканності їхніх інформаційних активів. Цю тезу переконливо підтверджують А. Круглашов та С. Швидюк [12, с. 241]. Дослідники слушно зауважують: виживання муніципального сектору в екстремальних умовах війни напряму залежить від того, чи зможе влада на місцях зберегти керованість критичними процесами. Якщо перенести цей принцип на реалії Полтавської обласної ради та громад регіону, вимальовується чіткий імператив – необхідно терміново відмовлятися від застарілої звички тримати локальні сервери просто в адміністративних будівлях.

Спираючись на можливості Закону України «Про хмарні послуги» [40], логічним та єдиним надійним кроком є масштабна міграція систем внутрішнього документообігу і муніципальних реєстрів у захищені хмарні середовища. Більше того, управлінська політика області має стимулювати розгортання географічно розподілених систем резервного копіювання. Тільки такий формат архітектури гарантуватиме, що навіть у випадку фізичного пошкодження чи знищення інфраструктури ОМС, доступ до життєво важливих баз даних буде відновлено практично миттєво.

Управлінським фундаментом для втілення цих ініціатив безпосередньо в області слугує Регіональна програма інформатизації «Цифрова Полтавщина» на 2024–2026 роки [39]. Важливо підкреслити, що цей документ є знаковим: він концептуально переформатовує саму архітектуру цифрового розвитку регіону. У ньому безпекові вимоги вперше закріплені не як додаткова опція, а як обов’язковий, наскрізний елемент кожного без винятку проєкту цифровізації. На практиці програма задає чіткі організаційно–фінансові вектори. Левова частка уваги приділяється осучасненню телекомунікацій: розгортанню захищених вузлів інтернету та побудові закритих, ізольованих каналів зв’язку. Ця захищена мережа має надійно об’єднати ключові інституції – Полтавську обласну раду, обласну військову адміністрацію, районні ланки та апарати найменших сільських чи селищних громад. Завдяки такій жорсткій сегментації вирішується критично важливе завдання. Навіть якщо зловмисникам вдасться здійснити успішну кібератаку на одну з базових громад, інцидент буде локалізовано на

ранній стадії. Це надійно убезпечує суміжні державні бази даних від масового компрометування за принципом «ланцюгової реакції».

Окрім технологічних інновацій, критичної ваги набуває наведення ладу у внутрішніх нормативних документах безпосередньо в органах місцевого самоврядування. Досліджуючи особливості правового регулювання кіберпростору, І. О. Кульчій та Є. О. Бітюга цілком слушно застерігають: будь–які масштабні оборонні ініціативи держави будуть зведені нанівець, якщо на локальному рівні бракуватиме жорстких регламентів [18, с. 158]. Для муніципалітетів Полтавщини це означає нагальну потребу розробити та затвердити власні, індивідуальні Політики інформаційної безпеки. Такі розпорядчі акти повинні не просто формально існувати, а детально регламентувати щоденну рутину апарату. Зокрема, йдеться про впровадження жорстких матриць доступу посадовців до баз даних, встановлення правил для корпоративної пошти та категоричну заборону на обробку службових документів на особистих гаджетах. Крім того, кожен працівник повинен мати під рукою чіткий покроковий алгоритм дій на випадок хакерської атаки. Зрештою, управлінська практика доводить: без такої базової локальної нормотворчості будь–які інвестиції у найдорожчі програмні комплекси будуть марними, адже систему завжди компрометуватиме неконтрольований людський фактор.

Ще одна критична площина – безпека офіційних каналів комунікації, адже від їхньої стабільної роботи напряму залежить легітимність рішень місцевої влади та рівень довіри суспільства. Якщо прискіпливо проаналізувати структуру й функціонал офіційного сайту Полтавської обласної ради [25], вимальовується чіткий пріоритет: портал потребує надійного захисту як від виснажливих DDoS–атак, так і від спроб ворожого дефейсу (несанкціонованої підміни контенту). Щоб протистояти цим викликам, вебплатформи ОМС і прив’язані до них системи електронного документообігу мусять спиратися виключно на сертифіковані технології. Обов’язковою та беззаперечною вимогою тут залишається використання засобів кваліфікованого електронного підпису. Щодо подальшої практичної модернізації вебресурсів обласної ради, необхідні цілком

прагматичні кроки. Йдеться про запровадження суворої дворівневої автентифікації для всіх адміністраторів системи та налаштування безперервного моніторингу трафіку для фіксації будь–яких мережевих аномалій. Саме такий підхід гарантуватиме, що процес інформування мешканців Полтавщини не буде зірвано навіть під час цілеспрямованих кіберударів.

Поряд із захистом електронного документообігу, окремим надскладним викликом для Полтавщини залишається безпека комунальної критичної інфраструктури. Оскільки водоканали, підприємства теплоенергетики та муніципальні лікарні перебувають у власності територіальних громад, саме місцева влада повинна взяти на себе лідерство в питаннях їхнього кіберзахисту. Нормативне підґрунтя для цього вже сформоване. Спираючись на Постанову Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури» [33], органи місцевого самоврядування мають терміново ініціювати глибокий технічний аудит автоматизованих систем управління технологічними процесами на підпорядкованих об’єктах. Головна мета таких заходів є максимально прагматичною – це повна, безкомпромісна фізична та логічна ізоляція технологічних комп’ютерних мереж від глобального Інтернету. У цій сфері ціна помилки вимірюється вже не просто втратою інформації: ворожий злам комунальних систем управління здатний спровокувати реальні техногенні аварії та повністю паралізувати життєзабезпечення міст області.

Варто виділити ще один критичний вимір інформаційної безпеки, де технологічні аспекти тісно переплітаються із соціальними. Йдеться про налагодження стратегічних комунікацій та активну протидію ворожій дезінформації. Як слушно зауважують О. Проніна та Л. Оленковська, в умовах повномасштабної війни інституційна стійкість місцевого самоврядування має пряму кореляцію з рівнем суспільної довіри [41, с. 427]. Практика показує, що сучасні кібератаки дедалі рідше зводяться лише до викрадення баз даних. Їхньою паралельною, а подекуди й головною метою стає злам офіційних ресурсів для вкидання фейків та штучного провокування паніки на місцях.

З огляду на це, перед Полтавською обласною радою постає виклик – сформувати розгалужену екосистему верифікованих каналів зв'язку, насамперед у популярних соціальних мережах та месенджерах. Сьогодні такі платформи мають працювати не просто як статичні дошки оголошень, а як інструменти кризового менеджменту: оперативно транслювати правду, миттєво розвінчувати маніпулятивні вкиди та підтримувати безперервний, живий діалог із мешканцями громад.

На основі аналізу поточних викликів стає очевидним, що захист цифрового простору Полтавщини потребує комплексного підходу, де технологічні рішення нерозривно пов'язані з організаційними регламентами та соціальною взаємодією. Для того, щоб децентралізований захист був ефективним, кожен регіон має діяти як автономний, але інтегрований вузол загальнонаціональної системи безпеки1. Систематизація ключових завдань, що стоять перед органами влади та громадами області, дозволяє виділити п'ять магістральних напрямів, які формують фундамент регіональної стійкості в умовах воєнного стану(рис. 3.1).

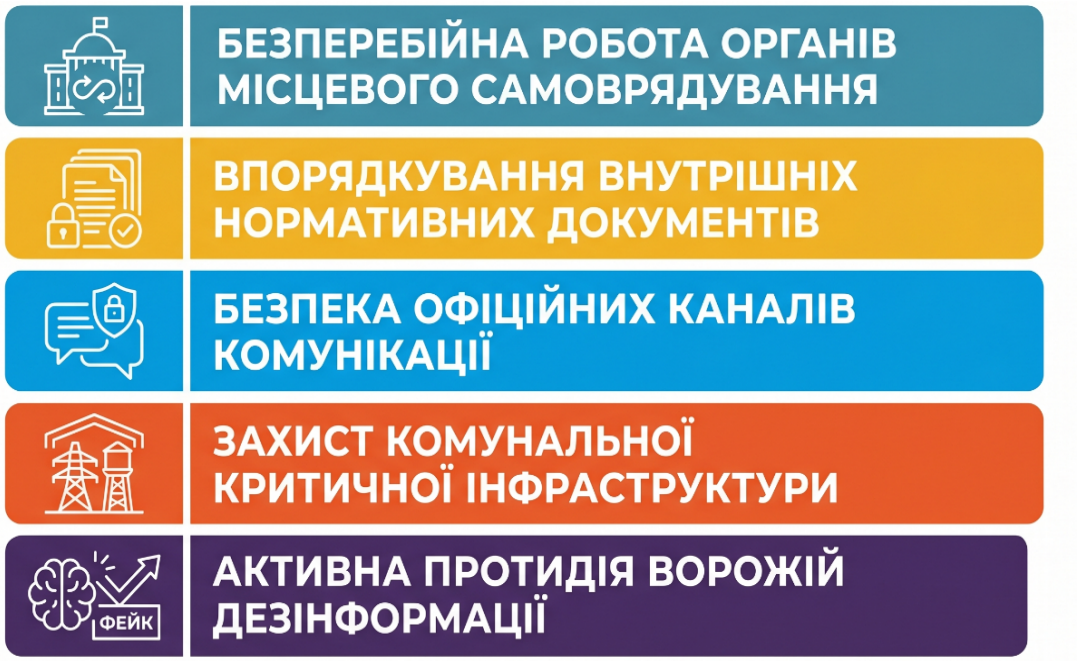

Рисунок 3.1. Основні пріоритети інформаційної безпеки Полтавщини

(Сформовано автором на основі матеріалів [12], [18], [25], [33], [39], [40], [41])

Наведений перелік пріоритетів підтверджує, що інформаційна безпека держави та Полтавської області є абсолютно нерозривними і потребують виключно прикладного, а не теоретичного підходу. Практична реалізація цих напрямів має відбуватися через заходи програми «Цифрова Полтавщина», яка закріплює безпекові вимоги як обов'язковий елемент кожного проєкту цифровізації.

Отже, проведений аналіз дає підстави для чіткого висновку: пріоритети розбудови інформаційної безпеки держави та Полтавської області є абсолютно нерозривними і потребують виключно прикладного підходу. Сьогодні регіональна політика має остаточно відійти від інертного теоретичного планування. Натомість фокус управлінської уваги слід змістити на безкомпромісну практичну реалізацію заходів програми «Цифрова Полтавщина» [39].

Щоб ця концепція запрацювала, необхідна сувора концентрація фінансових ресурсів на кількох векторах. Насамперед йдеться про масову міграцію муніципальних даних до хмарних сховищ та тотальну сертифікацію систем місцевого самоврядування за стандартами КСЗІ. Паралельно з цим має відбуватися обов'язковий технічний аудит критичної комунальної інфраструктури, що супроводжуватиметься наведенням жорсткого нормативного ладу всередині самих рад.

Систематизація вищезазначених викликів дозволяє стверджувати, що кожна сфера діяльності муніципалітету – від ведення реєстрів до комунікації з мешканцями – має власний унікальний профіль вразливостей. Ефективність регіональної політики безпеки залежить від того, наскільки точно підібрано технічні та організаційні інструменти для нейтралізації конкретних загроз. Для наочного представлення взаємозв'язку між критичними ризиками цифрового простору Полтавщини та запропонованими заходами з їх мінімізації, доцільно використовувати матрицю практичних рішень (див. табл. 3.3).

Таблиця 3.3

Матриця цифрових ризиків та прикладних заходів безпеки для громад Полтавської області

Об'єкт / Сфера захисту	*Ключовий ризик (загроза)*	*Практичний захід (інструментарій)*
Інформаційні активи та реєстри	Фізичне знищення серверів або втрата доступу через бойові дії.	Масштабна міграція у хмарні середовища та розподілене резервне копіювання.
Регіональна мережа зв'язку	Компрометування всієї системи за принципом «ланцюгової реакції».	Побудова ізольованих каналів та сегментація мережі для локалізації інцидентів.
Внутрішній менеджмент (персонал)	Неконтрольований «людський фактор», витік даних через особисті гаджети.	Впровадження індивідуальних Політик інформаційної безпеки та жорстких матриць доступу.
Офіційні вебресурси	DDoS–атаки та ворожий дефейс (підміна контенту).	Запровадження дворівневої автентифікації та моніторинг аномалій трафіку.
Критична інфраструктура (водоканали, ТЕЦ)	Техногенні аварії внаслідок зламу систем управління.	Повна фізична та логічна ізоляція технологічних мереж від мережі Інтернет.
Суспільна довіра	Поширення фейків та провокування паніки через злам каналів зв'язку.	Створення розгалуженої екосистеми верифікованих каналів у соцмережах та месенджерах

Розроблено автором на основі матеріалів дослідження [39]

Дана матриця демонструє, що безпека Полтавщини в цифровому вимірі базується на переході від пасивного спостереження до активної побудови багаторівневої архітектури захисту. Кожен із наведених заходів є не лише технічною вимогою, а й необхідною умовою збереження керованості регіоном в екстремальних умовах. Саме така деталізація інструментарію дозволяє перетворити стратегічні цілі програми «Цифрова Полтавщина» на реальний механізм стримування агресора в інформаційному просторі. Це закладає фундамент для того, щоб область могла функціонувати як автономний та стійкий вузол загальнонаціональної системи кібербезпеки.

Тільки завдяки формуванню такої багаторівневої, ешелонованої оборонної архітектури Полтавщина здатна успішно мінімізувати наявні цифрові

вразливості. У підсумку це дозволить регіону не лише захистити власні громади, а й закріпити за собою статус надійної опорної ланки в загальнонаціональній системі кібернетичного опору.

Таким чинок, узагальнення стратегічних напрямів модернізації державної політики свідчить, що в умовах війни захист муніципальних даних став невід'ємним складником національної безпеки. Пріоритетними кроками у цій сфері мають стати оновлення нормативно–правової бази через впровадження уніфікованих протоколів, перехід на європейські стандарти захисту персональних даних та законодавче закріплення персональної відповідальності керівників за виток інформації. Технологічне переоснащення вимагає відмови від локальних рішень на користь централізованих архітектур, обов'язкової побудови Комплексних систем захисту інформації та активного залучення інноваційних інструментів, зокрема «хмарних» технологій та механізмів незалежного аудиту вразливостей.

Аналіз пріоритетів безпеки на регіональному рівні, зокрема на прикладі Полтавської області, демонструє необхідність переходу від теоретичного планування до практичної реалізації заходів програми «Цифрова Полтавщина» [39]. Ключовий акцент зміщується на створення багатоешелонованої оборони, що включає міграцію реєстрів до захищених хмарних середовищ, посилення кіберзахисту об'єктів комунальної критичної інфраструктури та забезпечення стабільної роботи офіційних каналів комунікації. Ефективність цих заходів на місцях безпосередньо залежить від впровадження жорстких внутрішніх регламентів та політик інформаційної безпеки, які дозволяють мінімізувати технічні ризики та локалізувати можливі інциденти на ранніх стадіях.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Проведене дослідження теоретико–методологічних засад доводить, що розуміння інформаційної безпеки в системі публічного управління остаточно вийшло за межі суто технічних завдань. Класична модель захисту, відома як тріада «конфіденційність, цілісність, доступність», для органів місцевого самоврядування є базовою, але неповною. У сучасних умовах вона об’єктивно розширюється специфічними управлінськими критеріями: верифікованістю електронних документів, підконтрольністю дій персоналу та загальною операційною витривалістю апарату. Тобто безпека цифрового простору муніципалітету формується лише через поєднання надійної інфраструктури, чітких посадових регламентів та високої інформаційної культури службовців.

Аналіз нормативно–правового забезпечення виявив глибоку практичну суперечність, з якою щодня стикаються місцеві ради, – так звану «дилему прозорості». З одного боку, антикорупційне законодавство вимагає максимальної відкритості та оприлюднення проєктів рішень, а з іншого – посадовці несуть сувору відповідальність за збереження персональних даних громадян. Введення правового режиму воєнного стану змусило державу централізувати цей процес: доступ до багатьох кадастрів та відкритих даних було свідомо обмежено, щоб позбавити ворожу розвідку інструментів для підготовки кінетичних атак та інформаційно–психологічних операцій.

Дослідження специфіки управління даними під час війни показує, що пріоритети місцевого самоврядування кардинально змінилися з планового розвитку е–послуг на екстрене фізичне збереження інформації. Найефективнішим кроком у цій ситуації стала легалізація принципу «Cloud First», яка дала змогу територіальним громадам мігрувати критичні бази до захищених урядових та комерційних дата–центрів. Попри це, в регіонах зберігається відчутна нерівність: малі громади базового рівня продовжують працювати з вразливим локальним обладнанням через хронічний брак фінансування та відсутність у штаті профільних фахівців із кіберзахисту.

Практичний аудит інформаційної інфраструктури Полтавської обласної ради дозволив ідентифікувати низку специфічних проблем, які виникають на перетині технологій та щоденних рутинних процесів. Головну загрозу становить збереження елементів «гібридного» діловодства, стихійне використання депутатами особистих лептопів і смартфонів для роботи з документами (модель BYOD), а також ведення службової комунікації через незахищені публічні месенджери. Крім того, найслабшою ланкою системи залишається людський фактор: за відсутності регулярних практичних перевірок працівники апарату легко піддаються впливу методів соціальної інженерії та таргетованого фішингу.

Вивчення міжнародного досвіду свідчить про необхідність термінового переходу українських муніципалітетів до децентралізованих архітектур захисту. Для вітчизняної практики найбільш показовими є європейська концепція «Privacy by Design» (вбудованої безпеки), естонська технологія розподіленого обміну даними X–Road та архітектура «нульової довіри». Такий підхід здатний ліквідувати небезпеку «єдиної точки відмови», коли злам одного комп'ютера чи локального сервера в окремій сільській раді міг би призвести до каскадного компрометування суміжних державних реєстрів.

Для подолання виявлених ризиків розроблено стратегічну матрицю вдосконалення муніципальної кібербезпеки, яку доцільно імплементувати в межах регіональної програми «Цифрова Полтавщина». Головними пріоритетами для владних інституцій області визначено: стовідсоткову міграцію баз даних у хмару, повну логічну та фізичну ізоляцію систем управління комунальною критичною інфраструктурою від глобальної мережі, а також впровадження жорстких індивідуальних політик безпеки. Паралельно з технічними заходами, місцеві ради мають сформувати розгалужену екосистему верифікованих каналів зв'язку для оперативного антикризового реагування та спростування ворожих маніпуляцій на місцях.

Зважаючи на виявлені вразливості, розроблено комплекс заходів для підвищення інформаційної стійкості органів місцевого самоврядування.

У нормативно–правовій площині необхідно імплементувати вимоги Директиви NIS2 та GDPR. На законодавчому рівні варто закріпити затвердити європейські протоколи добового звітування про кіберінциденти та уточнити критерії комунальних об’єктів критичної інфраструктури.

Технологічний напрям передбачає поступову відмову від фізичних серверних кімнат на користь урядових хмарних рішень (зокрема для баз ЦНАПів та соцзахисту Полтавщини) із надійним резервуванням. Базовою умовою обігу службових даних залишається розбудова атестованих КСЗІ, а для критичних комунальних підприємств – повна фізична і логічна ізоляція виробничих мереж від Інтернету.

У фінансово–управлінському аспекті доцільно запровадити цільові державні субвенції для підтримки кібербезпеки малих громад, але виключно за умови дотримання ними базових ІТ–стандартів. Проблему браку місцевих фахівців варто вирішувати через міжмуніципальне співробітництво, залучення MSSP–провайдерів та створення профільних координаційних кіберхабів.

Для оптимізації внутрішніх процесів (зокрема в апараті Полтавської обласної ради) необхідно ухвалити комплексну Політику інформаційної безпеки на базі архітектури «нульової довіри». Вона має впровадити матриці диференційованого доступу, суворо заборонити пересилку робочих файлів через особисті месенджери та регламентувати дії під час цифрових атак.

Щодо кадрової політики, базова цифрова грамотність має стати обов’язковим критерієм при працевлаштуванні. Теоретичне навчання посадовців слід замінити на регулярні практичні перевірки, щоб мінімізувати вплив людського фактора. Водночас для взаємодії з громадськістю ради мають розгорнути надійні комунікаційні канали для антикризового сповіщення та протидії ворожій дезінформації.

Загалом, кіберзахист громад став стратегічним пріоритетом публічного управління, а не просто технічним питанням. Запропоновані заходи оновлять регіональні програми інформатизації, гармонізують регламенти рад та посилять національну безпеку в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білецький М. Міжнародний досвід використання цифрових технологій в публічному управлінні. *Наукові перспективи (Naukovì perspektivi)*. 2024. № 11(53). URL: https://doi.org/10.52058/2708–7530–2024–11(53)–53–67 (дата звернення: 02.06.2026)

2. Ю., Маринів А. В. Правовий режим воєнного стану та його вплив на місцеве самоврядування. *Вісник Пенітенціарної асоціації України*. 2025. № 1. С. 15–22. URL: https://doi.org/10.34015/2523–4552.2025.1.02 (дата звернення: 02.06.2026).

3. Вовжиняк М. Міжнародний досвід розвитку інформаційної компетентності публічних службовців. *Наукові перспективи (Naukovì perspektivi)*. 2024. № 5(47). URL: https://doi.org/10.52058/2708–7530–2024–5(47)–375–390 (дата звернення: 02.06.2026).

4. Гащук І., Трасковецька Л., Вальчук О. Оцінка ефективності використання державних електронних послуг в умовах воєнного стану. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. 2024. Т. 95, № 2. С. 158–168. URL: https://doi.org/10.32453/3.v95i2.1596 (дата звернення: 02.06.2026).

5. Гончарук Ю. В. Трансформація парадигми інформаційної безпеки в публічному управлінні через зростання загроз кіберпростору. *Efficiency of public administration*. 2025. № 82/83. С. 47–52. URL: https://doi.org/10.36930/508206 (дата звернення: 02.06.2026).

6. Гундертайло Ю. Д. Інформаційна гігієна в умовах воєнного стану. *Медіатворчість в часи війни: протистояння медіатравмі*: матеріали наук.–практ. конф. (м. Київ, 19 черв. – 23 серп. 2023 р.). Київ, 2023. URL: https://doi.org/10.59416/oipv7236 (дата звернення: 02.06.2026).

7. Дєгтяр О. Сучасні підходи до забезпечення інформаційної безпеки в публічному управлінні електронними послугами: світовий досвід. *Наукові перспективи (Naukovì perspektivi)*. 2025. № 1(55). URL:

https://doi.org/10.52058/2708–7530–2025–1(55)–218–230 (дата звернення: 02.06.2026).

8. Єфіменко І. Інформаційна безпека держави в умовах воєнного стану: особливості забезпечення. *Успіхи і досягнення у науці*. 2025. № 10(20). URL: https://doi.org/10.52058/3041–1254–2025–10(20)–96–105 (дата звернення: 02.06.2026).

9. Інформаційна відкритість органів місцевого самоврядування. Посібник для муніципальних посадовців. URL: https://arpi.org.ua/doc2/posibnyk.pdf (дата звернення: 02.06.2026).

10. Кавин С. Нормативно–правове забезпечення інформаційної безпеки України в контексті набуття членства в Європейському Союзі. *Наше право*. 2023. № 3. С. 140–150. URL: https://doi.org/10.32782/np.2023.3.21 (дата звернення: 02.06.2026).

11. Криштанович М. Використання Crowd–технологій у забезпеченні інформаційної безпеки органами місцевого самоврядування. *Актуальні питання у сучасній науці*. 2024. № 1(19). URL: https://doi.org/10.52058/2786–6300–2024–1(19)–185–190 (дата звернення: 02.06.2026).

12. Круглашов А., Швидюк С. Місцеве самоврядування України в умовах війни: адаптація до нових викликів. *Litopys Volyni*. 2025. № 32. С. 238–246. URL: https://doi.org/10.32782/2305–9389/2025.32.39 (дата звернення: 02.06.2026).

13. Кузьменко А. В. Особливості інформаційної безпеки органів публічного управління. *Державне управління: удосконалення та розвиток*. 2025. № 11. URL: https://doi.org/10.32702/2307–2156.2025.11.19 (дата звернення: 02.06.2026).

14. Кульчій І. О. Адаптація досвіду країн ЄС із забезпечення інформаційної безпеки. *Організаційно–правові аспекти публічного управління в Україні* : матеріали XI Міжнар. наук.–практ. Інтернет–конф. (м. Полтава, 25 квіт. 2024 р.). Полтава : Нац. ун–т ім. Юрія Кондратюка, 2024. С. 55–58. (дата звернення: 02.06.2026).

15. Кульчій І. О. Доступ до публічної інформації в контексті реформування органів влади України. *Сучасна парадигма публічного управління* : матеріали І Міжнар. наук.–практ. конф. (м. Львів, 17–18 жовт. 2020 р.) / за наук. ред. А. В. Стасишина. Львів : ЛНУ ім. Івана Франка, 2019. С. 51–54. (дата звернення: 02.06.2026).

16. Кульчій І. О. Механізм державного регулювання у сфері захисту персональних даних в Європейському Союзі. *Публічне управління та адміністрування в Україні: євроінтеграційний поступ* : матеріали І Всеукр. наук.–практ. конф. за міжнар. участю (31 трав. 2024 р.). 2024. (дата звернення: 02.06.2026).

17. Кульчій І. О. Особливості реалізації законодавства в сфері доступу до публічної інформації як чинник запобігання корупції. *Державна служба в Україні: шляхи реформування* : матеріали круглого столу (м. Київ, 22 трав. 2019 р.). Київ : Нац. академія прокуратури України, 2021. С. 98–104. (дата звернення: 02.06.2026).

18. Кульчій І. О., Бітюга Є. О. Правове поле кіберпростору України: сучасний стан та перспективи. *Тези 77–ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів Національного університету «Полтавська політехніка імені Юрія Кондратюка»* (м. Полтава, 16–22 трав. 2025 р.). Полтава : Нац. ун–т ім. Юрія Кондратюка, 2025. Т. 2. С. 158–159. (дата звернення: 02.06.2026).

19. Кушніков В. В. Методи вибору стратегічних напрямів розвитку державної політики України у сфері забезпечення інформаційної безпеки. *Державне управління: удосконалення та розвиток*. 2025. № 7. URL: https://doi.org/10.32702/2307–2156.2025.7.20 (дата звернення: 02.06.2026).

20. Куц Г. М., Пересипкіна І. В., Куц Ю. О. Особливості функціонування органів публічної влади в Україні в умовах воєнного стану: легітимаційний аспект. *Політичне життя*. 2025. № 4. С. 81–87. URL: https://doi.org/10.31558/2519–2949.2025.4.12 (дата звернення: 02.06.2026).

21. Литвинчук О. В., Гришина Н. В. Міжнародний досвід комунікації державних органів, місцевого самоврядування та громадськості. *Сучасні вектори відновлення та розвитку України на засадах сталості та безпеки*. 2023. URL: https://doi.org/10.54929/conf_21_11_2023–02–02 (дата звернення: 02.06.2026).

22. Мельник П. В. Нормативно–правове забезпечення служби в органах місцевого самоврядування України. *Law and Society*. 2024. № 5. С. 544–549. URL: https://doi.org/10.32842/2078–3736/2024.5.79 (дата звернення: 02.06.2026).

23. Мінчеков А. Сутність поняття інформаційна безпека в сучасній науці публічного управління. *Наукові перспективи (Naukovì perspektivi)*. 2024. № 4(46). URL: https://doi.org/10.52058/2708–7530–2024–4(46)–296–307 (дата звернення: 02.06.2026).

24. Ніцевич О. В. Інформаційна безпека України в умовах воєнного стану. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 2. С. 47–54. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/971/943 (дата звернення: 02.06.2026).

25. Офіційний сайт Полтавської обласної ради : вебсайт. URL: https://oblrada–pl.gov.ua (дата звернення: 02.06.2026).

26. Парасюк М. Особливості правового регулювання договору поставки для державних потреб в умовах воєнного стану. *Наукові інновації та передові технології*. 2026. № 2(54). URL: https://doi.org/10.52058/2786–5274–2026–2(54)–3286–3296 (дата звернення: 02.06.2026).

27. Петроє І. Інформаційна безпека в органах публічної влади як наукова проблема та об’єкт публічного управління. *Національні інтереси України*. 2025. № 3(8). URL: https://doi.org/10.52058/3041–1793–2025–3(8)–1046–1059 (дата звернення: 02.06.2026).

28. Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18.09.2019 № 856. URL: https://zakon.rada.gov.ua/laws/show/856–2019–п (дата звернення: 02.06.2026).

29. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939–VI. URL: https://zakon.rada.gov.ua/laws/show/2939–17 (дата звернення: 02.06.2026).

30. Про електронні комунікації : Закон України від 16.12.2020 № 1089–IX. URL: https://zakon.rada.gov.ua/laws/show/1089–20 (дата звернення: 02.06.2026).

31. 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 (дата звернення: 02.06.2026).

32. Про захист персональних даних : Закон України від 01.06.2010 № 2297–VI. URL: https://zakon.rada.gov.ua/laws/show/2297–17 (дата звернення: 02.06.2026).

33. Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518–2019–п (дата звернення: 02.06.2026).

34. Про інформацію : Закон України від 02.10.1992 № 2657–XII. URL: https://zakon.rada.gov.ua/laws/show/2657–12 (дата звернення: 02.06.2026).

35. 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 (дата звернення: 02.06.2026).

36. Про національну безпеку України : Закон України від 21.06.2018 № 2469–VIII. URL: https://zakon.rada.gov.ua/laws/show/2469–19 (дата звернення: 02.06.2026).

37. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163–VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19 (дата звернення: 02.06.2026).

38. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон

України від 23.09.1997 № 539/97–ВР. URL: https://zakon.rada.gov.ua/laws/show/539/97–вр (дата звернення: 02.06.2026).

39. Про регіональну програму інформатизації «Цифрова Полтавщина» на 2024–2026 роки : Рішення Полтавської обласної ради. URL: https://oblrada–pl.gov.ua/sites/default/files/field/docs/19_20.pdf (дата звернення: 02.06.2026).

40. Про хмарні послуги : Закон України від 02.02.2022 № 2024–IX. https://zakon.rada.gov.ua/laws/show/2075–20#Text (дата звернення: 02.06.2026).

41. Проніна О., Оленковська Л. Місцева демократія і стійкість органів місцевого самоврядування під час російського вторгнення. *Наукові перспективи (Naukovì perspektivi)*. 2025. № 5(59). URL: https://doi.org/10.52058/2708–7530–2025–5(59)–421–433 (дата звернення: 02.06.2026).

42. Руденко О. М., Захаров М. В. Стратегічні пріоритети забезпечення інформаційної безпеки в умовах війни. *Public management and administration in Ukraine*. 2024. № 39. С. 208–212. URL: https://doi.org/10.32782/pma2663–5240–2024.39.39 (дата звернення: 02.06.2026).

43. Свиридюк Н. П., Афонін Д. С. OSINT та інформаційна безпека в умовах воєнного стану. *Правове регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно–правового режиму воєнного стану*: колективна монографія. 2025. С. 766–810. URL: https://doi.org/10.61563/978–617–8574–56–7–19 (дата звернення: 02.06.2026).

44. Сердюк І. А. Підходи публічного управління до інформаційної безпеки особистості. *Public management*. 2022. № 3 (31). С. 53–59. URL: https://doi.org/10.32689/2617–2224–2022–3(31)–7 (дата звернення: 02.06.2026).

45. Соколова А. О., Ратошнюк Т. М., Ратошнюк В. І. Оцінка доходів та джерел формування фінансових ресурсів територіальних громад в умовах воєнного стану: регіональні особливості. *Ефективна економіка*. 2026. № 2. URL: https://doi.org/10.32702/2307–2105.2026.2.30 (дата звернення: 02.06.2026).

46. Сорокіна Л. Правові засади цифровізації місцевого самоврядування в Україні. *Наукові перспективи (Naukovì perspektivi)*. 2025. № 1(55). URL:

https://doi.org/10.52058/2708–7530–2025–1(55)–1487–1498 (дата звернення: 02.06.2026).

47. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021–40013 (дата звернення: 02.06.2026).

48. Тищенко Д., Шестак Я., Чорний М. Комплексний підхід до забезпечення безпеки інформаційних систем органів місцевого самоврядування. *Наука і техніка сьогодні*. 2024. № 12(40). URL: https://doi.org/10.52058/2786–6025–2024–12(40)–1535–1545 (дата звернення: 02.06.2026).

49. Цимбал П. В., Лисеюк А. М. Поняття та сутність публічно–правової охорони інформаційної безпеки. *Європейський правничий часопис*. 2023. № 1. С. 21–26. URL: https://doi.org/10.36919/elj.1.2023.21 (дата звернення: 02.06.2026).

50. Цимбаленко Я. Ю. Компетентнісний вимір ролі публічних службовців у формуванні цифрової інклюзивності. *Інвестиції: практика та досвід*. 2025. № 17. С. 304–310. URL: https://doi.org/10.32702/2306–6814.2025.17.304 (дата звернення: 02.06.2026).

51. Rudenko I. Digital transformation of public administration: communication mechanisms, ethical challenges and regulation. *Modern scientific journal*. 2025. Т. 7, № 1. С. 59–69. URL: https://doi.org/10.36994/2786–9008–2025–7–7 (дата звернення: 02.06.2026).

ДОДАТКИ

Додаток А

Наукові праці автора

Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Ghent University (Бельгія)
«1 DECEMBRIE 1918» University of Alba Iulia (Румунія)
UNIVERSITY ISMA (Латвійська республіка)
VARNA FREE UNIVERSITY«CHERNORIZETS HRABAR» (Болгарія)
Академія праці, соціальних відносин та туризму
Київський національний економічний університет імені Вадима Гетьмана
Національний технічний університет «Дніпропетровська політехніка»
Національний університет «Чернігівська політехніка»
Тернопільський національний технічний університет імені Івана Пулюя
Хмельницький університет управління та права імені Леоніда Юзькова

Матеріали XIII Міжнародної
науково-практичної Інтернет-конференції
ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

23 квітня 2026 року

Полтава – 2026

Костенко Дмитро Валентинович,
Кашина Ганна Сергіївна,
РОЗВИТОК ПРОФЕСІЙНИХ КОМПЕТЕНТНОСТЕЙ ДЕРЖАВНИХ СЛУЖБОВЦІВ В УМОВАХ ЄВРОІНТЕГРАЦІЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ 39

Кульчій Інна Олексіївна,
Романенко Олена Михайлівна
ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЄВРОПИ 42

Кутовий Владислав Михайлович
«ТРАНСФОРМАЦІЯ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ЗАСАД НАДАННЯ ПУБЛІЧНИХ ПОСЛУГ В УКРАЇНІ: СВІТОВИЙ ДОСВІД ТА ВЕКТОРИ ВДОСКОНАЛЕННЯ» 44

Лахижа Микола Іванович,
РЕАЛІЗАЦІЯ НАУКОВО-ДОСЛІДНОЇ ТЕМИ «МОДЕРНІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ, АДМІНІСТРУВАННЯ ТА ПРАВА В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ 45

Лебідь Тетяна Ігорівна
КОНСТИТУЦІЙНО-ПРАВОВІ ЗАСАДИ ФУНКЦІОНУВАННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ 47

Лопушинський Іван Петрович
ВПРОВАДЖЕННЯ ПРИНЦИПІВ SIGMA В СИСТЕМУ ДЕРЖАВНОЇ СЛУЖБИУКРАЇНИ: ВІД ДЕКЛАРАЦІЇ ДО ІНСТИТУЦІЙНОЇ СТІЙКОСТІ 50

Підгірний Владислав Олександрович
ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ УПРАВЛІННІ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ 52

Руденко Ольга Мстиславівна
Мирошниченко Аліна Іванівна
СТРАТЕГЕМА НАЦІОНАЛЬНОЇ СТІЙКОСТІ ЯК ФУНДАМЕНТ НОВОЇ ПАРАДИГМИ ПУБЛІЧНОГО УПРАВЛІННЯ 54

Рябоконь Єлизавета Павлівна
ЕТАПИ РОЗВИТКУ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ 56

Смаглюк Вікторія Валеріївна,
Шостака Тетяна Сергіївна
ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ: ЗАРУБІЖНИЙ ДОСВІД ДЛЯ УКРАЇНИ 57

Тарас Христина Іванівна,
ВЗАЄМОЗВ'ЯЗОК МОТИВАЦІЇ ТА ПРОФЕСІЙНОГО РОЗВИТКУ ПЕРСОНАЛУ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ 59

Томчук Олександр
ЦИФРОВІЗАЦІЯ ДІЯЛЬНОСТІ ПЕНСІЙНОГО ФОНДУ УКРАЇНИ В УМОВАХ ЕЛЕКТРОННОГО ВРЯДУВАННЯ 62

Смаглюк Вікторія Валеріївна, Національний університет «Полтавська політехніка імені Юрія Кондратюка» кандидат наук з державного управління, доцент кафедри публічного управління, адміністрування та права

Шостака Тетяна Сергіївна Національний університет «Полтавська політехніка імені Юрія Кондратюка» студентка за освітньою програмою бакалавр, спеціальність 281 Публічне управління та адміністрування

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ: ЗАРУБІЖНИЙ ДОСВІД ДЛЯ УКРАЇНИ

Цифровізація є ключовою тенденцією розвитку сучасного суспільства, яка докорінно змінює механізми управління, роблячи їх більш прозорими, інклюзивними та ефективними. В свою чергу, цифрові технології являють собою систему взаємопов'язаних засобів, за допомогою яких здійснюється збір, обробка, фіксація та зберігання вхідної інформації, а також формування і поширення вихідної інформації специфічним цифровим методом [1]. Для органів місцевого самоврядування та державної влади це означає перехід до нових форматів взаємодії з населенням, що базуються на засадах рівноправного діалогу, колективної відповідальності та партнерства. Ефективність національних рішень часто визначається спроможністю інтегрувати передові міжнародні практики та адаптувати їх до місцевих реалій [2]. Основою продуктивного демократичного управління на місцевому рівні є налагодження двосторонньої симетричної комунікації між владою та суспільством. Наприклад, у Німеччині жоден закон не ухвалюється без попереднього публічного обговорення з громадянами. У Нідерландах політика місцевого самоврядування базується на пошуку консенсусу та постійному моніторингу громадської думки. У США для залучення громадськості успішно функціонує концепція «громадянських журі», а у Великій Британії – «громадянські воркшопи». Широке впровадження систем електронного урядування здійснило справжню революцію у форматі надання публічних послуг. Данія зосередилася на створенні комплексних цифрових порталів, що дозволяє економити 10–20% бюджетних коштів щорічно. Естонія перевела 99% державних послуг в онлайн–формат завдяки безпечній системі електронної ідентифікації. Успіх таких країн, як Сінгапур та Південна Корея, спирається на інтеграцію послуг на централізованих платформах із залученням штучного інтелекту та аналітики великих даних. Водночас стрімка цифровізація супроводжується зростанням серйозних викликів у сфері інформаційної безпеки. Збільшення обсягів даних підвищує ризики кібератак: фішингу, соціальної інженерії та використання шкідливого програмного забезпечення. Особливу небезпеку становить ризик витоку конфіденційних персональних даних. Ці проблеми значно загострюються через низький рівень цифрової грамотності працівників органів влади, використання застарілих ІТ–систем та невідповідність чинного

законодавства темпам технологічного прогресу. Міжнародний досвід доводить необхідність комплексного підходу до захисту інформації, який поєднує технічні, організаційні та управлінські рішення. Естонія гарантує безпеку своїх реєстрів завдяки системі X–Road та впровадженню технології блокчейн. Сполучені Штати роблять акцент на єдиних стандартах безпеки. Країни ЄС діють у межах суворої загальноєвропейської правової бази. З технічної точки зору найбільш дієвими інструментами є впровадження автоматизованих систем виявлення вторгнень та обов'язкова багатофакторна автентифікація. Для України адаптація цього передового досвіду є життєво важливою стратегією, особливо в умовах російсько–української війни. Попри успіх порталу «Дія», Україна має низку сфер для вдосконалення. Необхідно використовувати міжнародний досвід взаємодії органів державної влади та громадськості, адаптуючи його до конкретних умов в Україні. Головна мета знайти розумний компроміс, який можна успішно впровадити в практику державного управління в Україні [3]. Органам місцевого самоврядування варто подолати цифровий розрив та ширше розвивати функціональність електронного цифрового підпису. Важливим кроком є проведення регулярних тренінгів для посадових осіб муніципалітетів. Впровадження міжнародних практик дозволить українським громадам гарантувати безперебійне надання послуг та побудувати надійну екосистему.

Література

1. Білецький М. Міжнародний досвід використання цифрових технологій в публічному управлінні. Наукові перспективи. 2024. № 11(53). С. 53–67. URL: https://doi.org/10.52058/2708–7530–2024–11(53) 53–67

2. Дєгтяр О. Сучасні підходи до забезпечення інформаційної безпеки в публічному управлінні електронними послугами: світовий досвід. Наукові перспективи. 2025. № 1(55). С. 218–230. URL: https://doi.org/10.52058/2708–7530–2025–1(55)–218–230

3. Литвинчук О. В., Гришина Н. В. Міжнародний досвід комунікації державних органів, місцевого самоврядування та громадськості. Сучасні вектори відновлення та розвитку України на засадах сталості та безпеки. 2023. URL: https://doi.org/10.54929/conf_21_11_2023–02–02