УДК 351.74+342.95

https://doi.org/10.52058/3041-1254-2025-7(17)-795-806

Шевченко Сергій Олексійович доктор наук з державного управління, професор, професор кафедри управління та адміністрування, Дніпропетровський державний університет внутрішніх справ, м. Дніпро, https://orcid.org/0000-0002-0079-3069,

Помаза-Пономаренко Аліна Леонідівна доктор наук з державного управління, старший дослідник, завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту Національного університету цивільного захисту України, м. Харків, https://orcid.org/0000-0001-5666-9350

НАПРЯМКИ ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В КОНТЕКСТІ ТРАНСФОРМАЦІЇ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ ТА ВПЛИВУ КІБЕРТРЕНДІВ

Анотація. Доведено, що державна інформаційна політика в Україні та її регіонах потребує вдосконалення з позиції застосування синергетичного підходу. Він передбачає впровадження низки публічно-управлінських заходів на тлі трансформації системи публічного управління. Аргументована реалізація цих публічно-управлінських заходів на центральному та регіональному рівнях. Зазначені заходи передбачають, з одного боку, покращення ресурсного забезпечення та надання методичної підтримки регіонам і громадам. А з другого боку, підвищення їх інституційної спроможності під час реалізації державної інформаційної політики.

Акцентовано на особливій ролі кіберзахисту як складової державної інформаційної політики. Виявлено глобальні кібертренди, які обґрунтовано співвідносити з особливостями реалізації державної інформаційної політики. Серед цих кібертрендів визначено такі, що формують ланшафдт кібербезпеки: 1) Zero Trust Architecture як модель нульової довіри, що базується на постійній верифікації користувачів і пристроїв у будь-якому цифровому середовищі; 2) AI-driven Security, що передбачає використання штучного інтелекту для виявлення кіберзагроз у реальному часі; 3) Cyber Resilience, що зорієнтоване не лише на кіберзахист, але й на створення умов для швидко відновлення інфраструктури та регіонів після кібератак; 4) кібергігієна користувачів і публічних службовців; 5) інтеграція безпеки на етапі проєктування (security-by-design), що вимагає впровадження безпекових елементів у цифрові сервіси регіонів.

Обґрунтовано концепт основних векторів удосконалення державної інформаційної політики в Україні та її регіонах. Серед цих векторів виокремлено

такі: 1) розробка й упровадження регіональних інформаційних стратегій; 2) формування інституційної спроможності регіонів загалом і громад зокрема; 3) підвищення цифрової грамотності населення та публічних службовців; 4) забезпечення фінансування регіональних IT-ініціатив на регіональному рівні; 5) створення центрів кіберзахисту на регіональному рівні.

Ключові слова: публічне управління, трансформація системи публічного управління, інституційна спроможність, державна інформаційна політика, комунікаційна політика, інформаційна безпека, кібербезпека, кібертренди, регіони, органи державної влади, регіональні центри кіберзахисту, публічні службовці.

Shevchenko Serhiy Alekseevich Doctor of Science in Public Administration, Professor, Professor of Department of the Department of Management and Administration of the Dnipropetrovsk State University of Internal Affairs, Dnipro, https://orcid.org/0000-0002-0079-3069,

Pomaza-Ponomarenko Alina Leonadivna Doctor of Sciences in Public Administration, Senior Researcher, Head of the Scientific Department for State Security Problems of Research Centre of the National University of Civil Protection of Ukraine, Kharkiv, https://orcid.org/0000-0001-5666-9350

DIRECTIONS FOR IMPROVING STATE INFORMATION POLICY IN THE CONTEXT OF TRANSFORMATION OF THE PUBLIC ADMINISTRATION SYSTEM AND THE INFLUENCE OF CYBERTRENDS

Abstact. It is proven that the state information policy in Ukraine and its regions needs to be improved from the standpoint of applying a synergistic approach. It involves the implementation of a number of public management measures against the background of the transformation of the public management system. The implementation of these public management measures at the central and regional levels is substantiated. These measures provide, on the one hand, for improving resource provision and providing methodological support to regions and communities. And on the other hand, for increasing their institutional capacity during the implementation of the state information policy.

The special role of cyber protection as a component of the state information policy is emphasized. Global cyber trends are identified that can reasonably be correlated with the features of the implementation of the state information policy. Among these cyber trends, the following are identified that form the cybersecurity landscape: 1) Zero Trust Architecture as a zero trust model based on constant verification of users and devices in any digital environment; 2) AI-driven Security, which involves the use of artificial intelligence to detect cyber threats in real time;

3) Cyber Resilience, which is focused not only on cyber defense, but also on creating conditions for the rapid restoration of infrastructure and regions after cyber attacks; 4) cyber hygiene of users and public servants; 5) integration of security at the design stage (security-by-design), which requires the implementation of security elements in digital services of regions.

The concept of the main vectors of improving state information policy in Ukraine and its regions is substantiated. Among these vectors, the following are distinguished: 1) development and implementation of regional information strategies; 2) formation of institutional capacity of regions in general and communities in particular; 3) increasing digital literacy of the population and public servants; 4) ensuring financing of regional IT initiatives at the regional level; 5) creation of cyber defense centers at the regional level.

Keywords: public administration, transformation of the public administration system, institutional capacity, state information policy, communication policy, information security, cybersecurity, cyber trends, regions, state authorities, regional cyber defense centers, public servants.

Постановка проблеми. Державна інформаційна політика та кібербезпека є ключовими компонентами ефективного публічного управління в умовах цифрової трансформації та гібридних загроз. Особливої ваги ці питання набувають на регіональному рівні, де спостерігається брак системності публічного управління, ресурсів і стратегічного бачення. З огляду на це набувають актуальності дослідження, присвячені розгляду сучасних викликів у цій сфері, визначенню напрямів удосконалення державної інформаційної політики, якому має передувати проведення порівняльного аналізу стану реалізації ІТ-компонентів на центральному та регіональному рівнях.

Аналіз останніх досліджень і публікацій. Правові, організаційні, інформаційні, кадрові та інші ресурсні аспекти державної політики у сфері інформаційної безпеки досліджували вчені С. Бєлай, А. Бойко, В. Бондаренко, О. Бондаренко, Л. Воронова, Ю. Горбань, І. Гриценко, М. Дмитренко, О. Довгань, В. Кривошеїн, О. Крюков, Ф. Медвідь, А. Пишна, Я. Михальский, О. Черевко, Г. Ситник, Д. Смотрич, Т. Француз-Яковець, І. Шинкаренко, І. Залєвська, Г. Удренас, Л. Мазуренко та ін. Незважаючи на значну кількість наукових досліджень, присвячених управлінським аспектам у сфері інформаційної безпеки, можемо відзначити, що потребують комплексного вирішення та висвітлення проблемні питання, пов’язані з удосконаленням державної інформаційної політики України на рівні її регіонів крізь призму окреслення наявних кібертрендів.

Постановка завдання. Мета статті полягає у визначенні напрямків удосконалення державної інформаційної політики в Україні та її регіонах, а також обґрунтуванні шляхів забезпечення на належному рівні кібербезпеки.

Виклад основного матеріалу. Стан реалізації державної інформаційної політики на регіональному рівні характеризується недосконалим функціонуванням цифрової інфраструктури, слабким кадровим потенціалом і низьким рівнем кіберзахисту. Незважаючи на успішні заходи центральної влади (створення Мінцифри, реалізація проєкту «Дія» тощо), ці ініціативи часто не мають належного продовження в громадах. Відсутність регіональних стратегій, відповідних фахівців, цільового фінансування інформаційної сфери створюють цифровий розрив та зумовлюють вразливість перед інформаційними атаками.

На рис. 1 представлено порівняльний аналіз особливостей реалізації ключових ІТ-компонентів між центральним та регіональним рівнями. Оцінювання здійснено за 5-бальною шкалою (1 – дуже низький рівень, 5 – дуже високий рівень). Відзначимо, що на центральному рівні державна інформаційна політика демонструє високі показники з усіх критеріїв, зокрема у створенні цифрової інфраструктури, забезпеченні належного фінансування інфосфери. Натомість на регіональному рівні спостерігається дефіцит ресурсів, інституційної підтримки та персоналу з кіберзахисту. Це обмежує ефективність реалізації державної інформаційної політики в масштабах держави та підвищує ризики кристалізації наявних в її межах проблем.

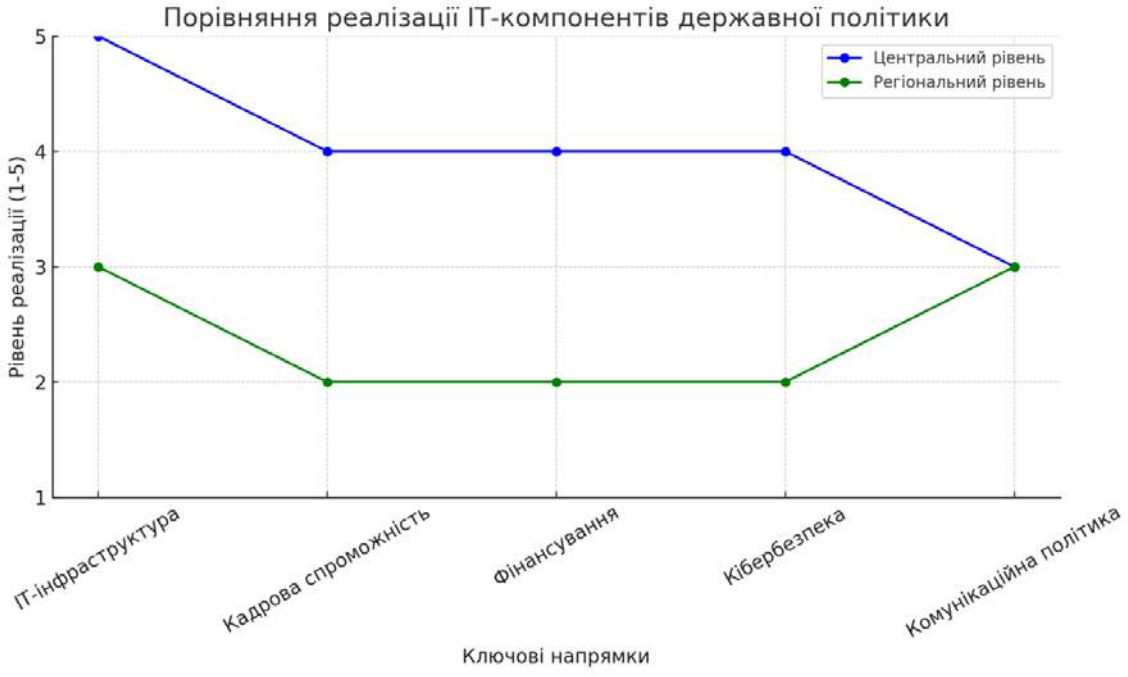

Рис. 1. Порівняння стану реалізації ІТ-компонентів державної інформаційної політики між центральним та регіональним рівнями

Джерело: авторська розробка

На цій підставі можемо вказати на ключові напрями вдосконалення державної інформаційної політики в Україні та її регіонах, а саме:

1. Розробка та впровадження регіональних інформаційних стратегій, узгоджених з національними пріоритетами.

2. Формування інституційної спроможності громад через створення структур з інформаційної політики.

3. Підвищення цифрової грамотності працівників місцевої влади.

4. Забезпечення фінансової підтримки регіонів через державні субвенції та партнерські програми.

5. Створення центрів кіберзахисту на базі обласних державних адміністрацій.

Очевидно, що вдосконалення державної інформаційної політики та кібербезпеки в регіонах України вимагає застосування комплексного підходу. Центральні органи виконавчої влади (загальної та спеціальної компетенції) повинні не лише задавати напрям, а й надавати підтримку у формі методичних рекомендацій, фінансування та навчання кадрового корпусу на місцях. Лише за умови налагодженої координації та децентралізації державної інформаційної політики можливо досягти підвищення рівня інформаційної безпеки на всій території України. Розглянемо більш детально вищенаведені напрямки вдосконалення державної інформаційної політики:

1. Розробка та впровадження регіональних інформаційних стратегій, узгоджених з національними пріоритетами інформаційної безпеки України. Однією з основних проблем сучасної інформаційної політики нашої держави є відсутність скоординованого бачення її реалізації на регіональному рівні. Національні документи, зокрема Доктрина інформаційної безпеки України та Стратегія цифрової трансформації, визначають загальні вектори, але не мають чіткого механізму імплементації в регіонах. У той же час, потреби областей є специфічними, залежними від рівня розвитку IT-інфраструктури, соціально-економічного середовища та кадрового потенціалу. Упровадження регіональних стратегій, синхронізованих із національними пріоритетами інформаційної безпеки, дозволить адаптувати державну політику до місцевих умов, уникнути дублювання, підвищити ефективність бюджетного планування та моніторингу результатів.

2. Формування інституційної спроможності регіонів загалом і громад зокрема через створення між секторальних координуючих структур у сфері реалізації державної інформаційної політики. Інституційна спроможність є фундаментом для реалізації будь-якої державної політики [3; 4]. У більшості громад відсутні спеціалізовані підрозділи або відповідальні фахівці з ефективної реалізації інформаційної політики. Це унеможливлює як розробку стратегічних документів, так і реалізацію навіть базових заходів – від забезпечення доступу до публічної інформації до цифрової (кібербезпеки) безпеки. Створення профільних інституцій або призначення відповідальних осіб у структурах місцевого самоврядування сприятиме формуванню компетентних команд, здатних взаємодіяти з центральною владою, залучати ресурси, координувати

місцеві інформаційні ініціативи та реалізовувати проєкти цифрового розвитку.

3. Підвищення цифрової грамотності працівників місцевої влади. Цифрова трансформація неможлива без компетентних кадрів, які є запорукою формування потужного корпусу сектора безпеки й оборони. Рф не посягнула б на цілісність України та її суверенітет якби в неї були сумніви щодо стану захищеності українських кордонів та не був підготовлений відповідний інформаційний плацдарм для наступу. У багатьох громадах працівники місцевих адміністрацій не володіють достатніми знаннями в галузі інформаційних технологій, цифрових сервісів, захисту даних. Це не лише знижує ефективність публічного управління в інформаційній сфері, а й створює ризики для безпеки інформаційного середовища (простору). Реалізація навчальних програм з цифрової грамотності, зокрема, у межах партнерства з освітніми та науковими закладами й установами, міжнародними організаціями та проєктами технічної допомоги, дозволить підвищити якість управлінських рішень, запроваджувати інноваційні інструменти, підвищити довіру населення до органів влади.

4. Забезпечення фінансової підтримки регіонів через державні субвенції та партнерські програми. Нерівномірність фінансування реалізації державної інформаційної політики – це одна з головних перешкод на шляху до ефективної інфополітики в регіонах. Більшість громад не мають змоги самостійно інвестувати в ІТ-інфраструктуру, електронне урядування або захист даних. Запровадження цільових державних субвенцій, грантів та механізмів співфінансування (наприклад, у співпраці з міжнародними донорами чи приватним сектором) створить умови для більш рівномірного розвитку, дозволить реалізовувати проєкти на зразок цифрових муніципалітетів, ситуаційних центрів, публічних комунікаційних платформ.

5. Створення центрів кіберзахисту на базі обласних адміністрацій. Кібербезпека є критично важливою складовою державної інформаційної політики, особливо в умовах гібридної війни. Наразі лише центральні органи виконавчої влади мають належну інфраструктуру та протоколи реагування на кіберінциденти. Регіони залишаються при цьому практично беззахисними перед кібератаками, фішинговими кампаніями, витоками інформації. Формування регіональних центрів кіберзахисту на базі обласних державних адміністрацій або ситуаційних центрів дозволить створити горизонтальну мережу обміну інформацією, швидкого реагування, моніторингу загроз. Такі центри можуть також виконувати навчально-методичну функцію, підтримуючи громади та установи освіти, охорони здоров’я, критичної та кіберінфраструктури. Створення центрів кіберзахисту на базі обласних (військових) державних адміністрацій або регіональних ситуаційних центрів дозволить посилити кіберстійкість, здійснювати оперативне реагування, взаємодіяти з Держспецзв’язку, СБУ та іншими структурами. Такі центри також можуть виконувати навчально-координаційну функцію.

Варто зауважити, що у XXI столітті питання інформаційної та кібербезпеки набувають особливого значення в умовах зростання гібридних загроз, кібератак, дезінформації та цифровізації всіх сфер життя. Особливо вразливими до кіберзагроз є регіональні системи управління, інфраструктура органів місцевого самоврядування та інших інституції, які забезпечують публічні сервіси. У зв'язку з цим актуалізується необхідність переосмислення підходів до реалізації державної інформаційної політики в регіонах України.

Серед глобальних трендів кіберзахисту можна виокремити ті, що формують контекст, у якому повинна функціонувати й українська система. На наше переконання, до ключових трендів належать такі:

1. Zero Trust Security – модель нульової довіри, яка передбачає перевірку кожного доступу, незалежно від місця розташування користувача.

2. Кібергігієна на рівні користувача – навчання населення базовим принципам цифрової безпеки.

3. Інтеграція штучного інтелекту (AI) у сферу кіберзахисту – використання алгоритмів для виявлення аномалій та атак у реальному часі.

4. Кіберстійкість критичної інфраструктури – перехід від простої захищеності до здатності швидко відновлюватися після атак [1; 4; 5; 6].

Очевидно, що сучасні кібертренди повинні перегукуватись із векторами розвитку державної інформаційної політики, яка реалізується на центральному та регіональному рівнях (рис. 2, табл. 1). На цій підставі відзначимо лакуни реалізації такої політики та забезпечення кібербезпеки: 1) децентралізація цифрових рішень – передача частини цифрових функцій на рівень регіонів і громад; 2) повсюдне впровадження публічних ІТ-платформ для підвищення результативності взаємодії з громадянами, що (платформи) передбачають активну реалізацію відкритих бюджетів, електронних звернень тощо; 3) дієва реалізація ініціатив «розумного міста», що вимагає втілення smart-рішень у великих містах (для прикладу таких, як Вінниця, Дніпро, Львів, Харків та ін. [2]); 4) формування локальних (регіональних) центрів кіберзахисту – в межах обласних державних (військових) адміністрацій або ситуаційних центрів. При цьому важливо забезпечити підключення громад до національної кіберзахисної системи через платформу Національного координаційного центру кібербезпеки; 5) цифрова освіта населення загалом і підвищення цифрової грамотності публічних службовців зокрема.

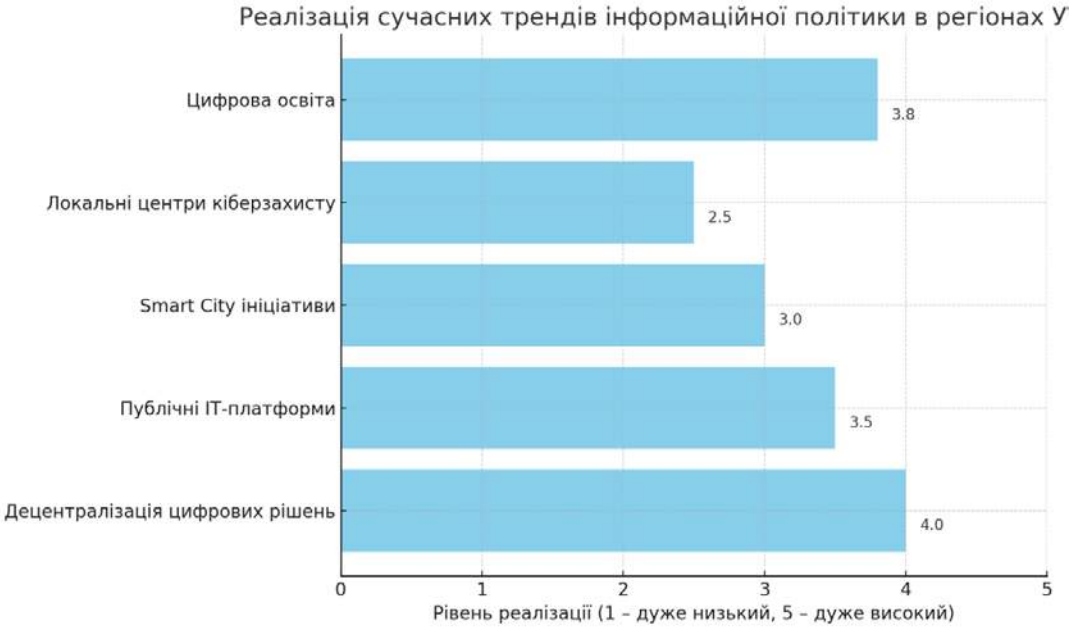

Рис. 2. Аналіз сучасних кібертрендів у співвіднесенні їх з особливостями реалізації державної інформаційної політики в Україні

Джерело: авторська розробка

Представлені на рис. 2 кібертренди у взаємозв'язку зі станом функціонування вітчизняної державної інформаційної політики дозволяють визначити такі вектори її розвитку:

1. Децентралізація цифрових рішень. Після реалізації реформи децентралізації влади в Україні більшість її громад отримали значну автономію у впровадженні цифрових сервісів. Цей тренд сприяє розвитку місцевих систем публічного управління та підвищенню прозорості влади.

2. Публічні IT-платформи для взаємодії з громадянами. Поширення платформ електронної демократії, відкритих бюджетів та електронних звернень посилює довіру населення до місцевої влади.

3. Ініціативи «розумного міста» (Smart City). У великих містах реалізуються smart-рішення з управління трафіком, безпекою, ЖКГ та комунікаціями, хоча в малих громадах цей напрям менш активний.

4. Формування локальних центрів кіберзахисту. Деякі українські регіони розпочали створення осередків захисту інформаційного простору, проте поширення таких центрів потребує централізованої підтримки.

5. Цифрова освіта громадян і підвищення цифрової грамотності публічних службовців. Навчальні програми для таких службовців та населення в цілому стають основою інформаційної безпеки й ефективного публічного управління в цифровому середовищі.

Регіони України поступово інтегрують сучасні практики державної інформаційної політики, проте її розвиток на місцях є нерівномірним. Необхідна

підтримка з боку держави, типізація моделей цифрового розвитку та кіберзахисту, розбудова кіберзахисної інфраструктури та збільшення обсягів залучених інвестицій у цифрову освіту для підвищення загальної інформаційної стійкості України.

Таблиця 1

Співвіднесення кібертрендів з практиками реалізації державної інформаційної політики в Україні

№ з/п	Кібертренд	Стан упровадження в Україні	Рекомендації
1	Zero Trust Architecture	Частково реалізовано в урядових IT-системах	Потребує розширення в регіонах
2	Штучний інтелект у безпеці	В процесі апробації в нац. CERT-UA та приватному секторі	Вимагає масштабування
3	Кіберстійкість	Акцент у Стратегії кібербезпеки	Немає механізмів реалізації на місцях
4	Кібергігієна	Окремі програми за підтримки донорів	Недостатнє охоплення населення
5	Security-by-design	Частково в держсервісах (наприклад, «Дія»)	Потребує стандартизації на рівні законодавства

Джерело: авторська розробка

Сучасні кібертренди формують нову парадигму державної інформаційної політики, яка має бути не лише захисною, а й адаптивною, інтегрованою у всі рівні публічного управління. Для України це означає необхідність: стандартизації кіберпротоколів для регіональних і місцевих структур; масштабного просвітницького компоненту щодо кібергігієни; інституційної інтеграції підходу Zero Trust на всіх рівнях влади; розробки регіональних стратегій кібербезпеки в координації з національними документами; інвестування у застосування ШІ в аналітиці кіберінцидентів. Саме скоординоване впровадження трендових підходів забезпечить довгострокову інформаційну стійкість держави та її регіонів [1].

Власне кажучи, ключові кібертренди формують сучасний ландшафт кібербезпеки, серед яких варто виділити декілька основних напрямів. Перш за все, архітектура Zero Trust, що базується на принципі нульової довіри, передбачає постійну перевірку користувачів і пристроїв незалежно від їхнього розташування в цифровому середовищі. Друга тенденція передбачає формування системи безпеки за допомогою виваженого застосування штучного інтелекту (AI-driven Security). Це змогу оперативно виявляти кіберзагрози завдяки аналізу даних у реальному часі. Третій важливий аспект – кіберстійкість (Cyber Resilience), яка орієнтована не лише на протистояння загрозам, а й на забезпечення швидкого відновлення критичної інфраструктури та регіонів після

атак. Додатково фокус уваги зосереджується на кібергігієні, яка охоплює як поведінку звичайних користувачів, так і посадових осіб, задіяних у публічних службах. Крім тогог, набирає популярності принцип інтегрування безпеки ще на ранніх етапах розробки (security-by-design), що передбачає впровадження елементів кіберзахисту безпосередньо в процес створення цифрових сервісів, зокрема для регіональних потреб.

Отже, ефективність державної інформаційної політики в регіонах України залежить від здатності синхронізувати національні пріоритети з локальними потребами, посилювати кадровий, фінансовий, науковий і технічний потенціал на місцях, а також впроваджувати глобальні практики кіберзахисту з урахуванням українських реалій. Без розвитку регіональної складової неможливо забезпечити сталу інформаційну безпеку держави.

Висновки. На підставі проведеного аналізу можемо зробити такі висновки щодо напрямків удосконалення державної інформаційної політики в Україні та її регіонах:

1. Державна інформаційна політика потребує зміщення від декларативності до практичного впровадження. При цьому необхідна синергія зусиль, що передбачає таке: центральні органи виконавчої влади надають ресурси та методичну підтримку, а регіони – адаптують і реалізують результативно державну інформаційну політику на місцях. Особливої уваги слід надати кіберзахисту, як одному з критичних компонентів сучасної інформаційної безпеки. Визначено глобальні кібертренди й обґрунтовано особливості їхнього врахування на вітчизняних теренах. Це зреалізовано з позиції проаналізованих сучасних кібертрендів й особливостей реалізації державної інформаційної політики в Україні.

2. Представлено концепт ключових напрямів удосконалення державної інформаційної політики в Україні та її регіонах, що (напрямки) передбачають:

1. Розробку й упровадження регіональних інформаційних стратегій. Вони дозволять адаптувати національну політику до потреб регіонів з урахуванням їхньої цифрової та іншої інфраструктурної, кадрової та соціально-економічної специфіки. Це забезпечить узгодженість дій між центром і регіонами, підвищивши дієвість упровадження цифрових рішень.

2. Формування інституційної спроможності регіонів загалом і громад зокрема. Відсутність організаційних структур, відповідальних за державну інформаційну політику, є бар’єром для системного соціально-економічного розвитку. Створення спеціалізованих інституцій на рівні регіонів і громад забезпечить сталість та координацію заходів цифровізації.

3. Підвищення цифрової грамотності населення та публічних службовців. Недостатній рівень цифрових навичок у працівників органів публічної влади на місцях гальмує процес трансформації системи публічного управління загалом. Відтак, необхідно впроваджувати навчальні програми, тренінги, онлайн-курси, які охоплюватимуть не лише технічні знання, а й аспекти інформаційної безпеки.

4. Забезпечення фінансування регіональних ІТ-ініціатив на регіональному рівні. Місцеві органи публічної влади обмежені в ресурсах. Держава має запровадити цільові субвенції, підтримку з боку міжнародних донорів і стимулювання державно-приватного партнерства для впровадження інновацій.

5. Створення центрів кіберзахисту на регіональному рівні. Обласні державні (військові) адміністрації мають стати опорними пунктами для кібербезпеки в регіонах. Центри кіберзахисту забезпечать моніторинг загроз, реагування на інциденти та підтримку місцевих структур.

Література:

1. Галушко С.П. Модель функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації та впливу її технологій // Вісник Національного університету цивільного захисту України. Серія: Державне управління. Вип. 2 (21). 2024. С. 102–109.

2. Король А.П., Помаза-Пономаренко А.Л., Ахмедова О.О. Інвестиційно-інноваційний розвиток регіонів в Україні як перспективний напрям удосконалення системи публічного управління // Державне управління: удосконалення та розвиток. 2025. № 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/6160.

3. Лопатченко І.М., Помаза-Пономаренко А.Л., Батир Ю.Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану // Вісник Національного університету цивільного захисту України. 2024. № 1 (20). С. 14–24.

4. Помаза-Пономаренко А.Л., Тарадуда Д.В. Особливості управління й експлуатації об’єктів критичної інфраструктури в контексті забезпечення інформаційної безпеки // Успіхи і досягнення у науці. 2024. № 3(3). Том 2. С. 208-220.

5. Farrakhov O., Lefterov O., Strelets V., Pecheny V., Pomaza-Ponomarenko A. Uniqueness Ensuring of Theoretical Solution to the Problem of Image Reconstructing of an Air Target Attacking Protected Object of Ukraine’s Critical Infrastructure // Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control. 2025. Vol. 596. P. 163–172.

6. Pomaza-Ponomarenko A., Taraduda D., Kravchuk O., Moroz S., Akhmedova O., Poroka S. National Security Management: Organizational, Legal, Informational, and Human Resource Dimensions // Transatlantic Policy Quarterly. 2025. Vol. 23. No. 4. Spring 2025. URL: http://transatlanticpolicy.com/article/1293/national-security-management-organizational-legal-informational-and-human-resource-dimensions. https://doi.org/10.5281/zenodo.15714998.

References:

1. Galushko, S.P. (2024). [Model of functioning of public administration mechanisms in the sphere of national security in the conditions of digitalization and the influence of its technologies]. *Bulletin of the National University of Civil Protection of Ukraine. Series: State Administration.* 2 (21). 102–109. [in Ukrainian].

2. Korol, A.P., Pomaza-Ponomarenko, A.L. & Akhmedova, O.O. (2025). [Investment and innovation development of regions in Ukraine as a promising direction for improving the public administration system]. *State Administration: Improvement and Development*. 4. Retrieved from https://www.nayka.com.ua/index.php/dy/article/view/6160. [in Ukrainian].

3. Lopatchenko, I.M., Pomaza-Ponomarenko, A.L & Batyr, Y.G. (2024). [State regulation in the sphere of information security of Ukraine under martial law]. Bulletin *of the National University of Civil Defense of Ukraine*. 1 (20). 14–24. [in Ukrainian].

4. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). [Features of management and operation of critical infrastructure facilities in the context of ensuring information security]. *Successes and achievements in science*. 3(3). 208-220. [in Ukrainian].

5. Farrakhov, O., Lefterov, O., Strelets, V., Pecheny, V. & Pomaza-Ponomarenko, A. (2025). [Uniqueness Ensuring of Theoretical Solution to the Problem of Image Reconstructing of an Air Target Attacking Protected Object of Ukraine's Critical Infrastructure]. *Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control*. 596. 163–172. [In English].

6. Pomaza-Ponomarenko, A., Taraduda, D., Kravchuk, O., Moroz, S., Akhmedova, O. & Poroka, S. (2025). [National Security Management: Organizational, Legal, Informational, and Human Resource Dimensions]. *Transatlantic Policy Quarterly*. 23 (4). Retrieved from http://transatlantic policy.com/article/1293/national-security-management-organizational-legal-informational-and-human-resource-dimensions. https://doi.org/10.5281/zenodo.15714998. [In English].