ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

УДК 351.078:004.056

Берладинюк Євген Володимирович
здобувач вищої освіти за третім (освітньо-науковим) рівнем вищої освіти Івано-Франківського національного технічного університету нафти і газу
ORCID: 0009-0004-5339-4792

https://doi.org/10.25313/3083-7782-2026-5-35

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ УКРАЇНИ ПІД ЧАС ВОЄННИХ ТА КРИЗОВИХ ВИКЛИКІВ

Анотація. *Вступ. У статті проаналізовано еволюцію архітектури цифрової безпеки системи публічного управління України в умовах повномасштабної війни. Доведено, що стратегічна трансформація підходів до захисту інформації – від фізичного розміщення серверів до використання хмарних технологій та концепції «нульової довіри» – стала ключовим чинником забезпечення безперервності державного управління та надання публічних послуг під час безпрецедентних кіберзагроз.*

Метою статті є комплексний аналіз інституційних, технологічних та управлінських механізмів забезпечення цифрової стійкості органів державної влади та місцевого самоврядування, а також окреслення перспектив переходу від реактивної до проактивної моделі кіберзахисту.

Матеріали та методи. Дослідження ґрунтується на аналізі нормативно-правової бази, стратегій цифровізації та досвіду функціонування критичної інформаційної інфраструктури України у воєнний період. Використано методи системного та структурного аналізу, моделювання управлінських процесів, а також синтезу кращих практик міжнародної співпраці у сфері кіберзахисту.

Результати. Досліджено інституційну архітектуру системи кібербезпеки та роль ключових суб'єктів (ДССЗЗІ, Мінцифри, СБУ, НКЦК). Виокремлено технологічні вектори захисту, зокрема успішне впровадження екосистеми «Дія» та системи «Трембіта». Ідентифіковано критичні вразливості системи, серед яких – кадровий дефіцит, технологічна застарілість інфраструктури на місцях та енергетична нестабільність. Обґрунтовано необхідність впровадження моделі «нульової довіри» (Zero Trust), створення національного кіберрезерву та інтеграції алгоритмів штучного інтелекту в системи моніторингу загроз.

Перспективи. Подальші дослідження варто зосередити на імплементації європейських директив, зокрема NIS2, розвитку вітчизняних технологічних рішень для зниження залежності від зовнішніх постачальників та формуванні культури «кіберстійкості як повсякденної норми» через розвиток професійних компетенцій державних службовців.

Ключові слова: *публічне управління, цифрова безпека, кіберстійкість, воєнний стан, хмарні технології, нульова довіра (Zero Trust), державні реєстри, «Трембіта», кібергігієна, критична інфраструктура.*

Постановка проблеми. Повномасштабна військова агресія проти України виявила критичну вразливість традиційних підходів до забезпечення цифрової безпеки в системі публічного управління, що базувалися на жорсткій фізичній локалізації державних інформаційних ресурсів. Радикальна зміна безпекового ландшафту, що супроводжується постійними кібератаками на критичну

інфраструктуру, дефіцитом кваліфікованих ІТ-кадрів, технологічною застарілістю засобів захисту в органах місцевого самоврядування та енергетичною нестабільністю, потребує невідкладного переосмислення інституційних та технологічних механізмів цифрового захисту. Відсутність цілісної проактивної стратегії в умовах гібридної війни створює ризики порушення безперервності функціонування органів публічної влади, що вимагає переходу від реактивного реагування до системного впровадження інноваційних рішень, таких як «хмарна» інфраструктура, концепція «нульової довіри» (Zero Trust) та поглиблена міжнародна інтеграція у сфері кіберзахисту.

Аналіз останніх досліджень і публікацій. Сучасний етап розвитку кібербезпеки в Україні характеризується інтенсивною трансформацією нормативно-правової бази та впровадженням інноваційних технологічних рішень для захисту критичної інфраструктури та державних інформаційних ресурсів в умовах воєнного стану [1; 5]. Значну увагу приділено оптимізації архітектури кіберзахисту, зокрема через діяльність команди реагування CERT-UA, яка забезпечує координацію та аналіз кіберінцидентів на національному рівні [2]. У сфері державного управління та електронної взаємодії ключовим елементом залишається розвиток системи «Трембіта» як інструменту інтеграції державних реєстрів [3], а також адаптація стратегічних підходів до цифровізації, зокрема концепції «Cloud First», яка активно імплементується для підвищення стійкості державних систем [4]. Важливим вектором стало посилення безпеки кінцевих цифрових продуктів, таких як застосунок «Дія», де застосовуються багаторівневі методи шифрування та регулярні аудити захищеності [7]. Особливе місце в сучасних дискурсах посідає впровадження моделі «нульової довіри» (Zero Trust) як фундаментального підходу до управління доступом у розподілених інформаційних середовищах [9]. Водночас інституційна спроможність держави посилюється через інтеграцію з міжнародними безпековими структурами, зокрема отримання доступу до Резерву кібербезпеки ЄС [10] та розширення співпраці в межах Таллінського механізму [8]. Практичний інструментарій кіберзахисту доповнюється легалізацією програм Bug Bounty для державних систем, що дозволяє залучати «білих хакерів» для пошуку вразливостей за чітко визначеними правилами [6]. Таким чином, сучасні публікації свідчать про перехід до проактивної моделі кіберстійкості, яка поєднує нормативне регулювання, міжнародну технічну допомогу та впровадження сучасних ІТ-стандартів.

Метою статті є теоретичне обґрунтування та комплексний аналіз інституційних, технологічних та управлінських механізмів забезпечення цифрової стійкості органів державної влади та місцевого самоврядування України в умовах воєнних та кризових викликів.

Виклад основного матеріалу. Основою механізму забезпечення цифрової безпеки в системі публічного управління України є інтегрована інституційно-технологічна архітектура, діяльність якої регламентується оновленою нормативно-правовою базою та підпорядковується завданню підтримання безперервності державного управління в умовах воєнних загроз. Після 2022 року державне регулювання інформаційної безпеки в Україні зазнало не лише технічного, а й управлінського переосмислення. Повномасштабне вторгнення стало чинником, який прискорив перегляд підходів до захисту державних даних, резервування критичних реєстрів, безперервності надання адміністративних послуг і координації між суб'єктами кібербезпеки.

До початку повномасштабної війни значна частина державної цифрової інфраструктури функціонувала за відносно консервативною логікою, яка передбачала фізичне розміщення серверів із критичними даними переважно на території України. В умовах масованих ракетних ударів, окупації частини територій і ризику фізичного знищення дата-центрів така модель виявила системну вразливість. Тому стратегічним рішенням стало нормативне врегулювання можливості перенесення державних інформаційних ресурсів до захищених хмарних середовищ за межами країни [1]. За відкритими даними, до липня 2022 року було перенесено понад 10 PB даних, що створило передумови для збереження функціональності державних реєстрів, освітніх, банківських та управлінських сервісів у період високої невизначеності.

У межах цього дослідження механізм цифрової безпеки публічного управління доцільно розглядати не як сукупність окремих технічних рішень, а як формалізовану управлінсько-технологічну модель повного циклу. Умовно її можна подати у вигляді такої послідовності:

$$МЦБ = \{N \to I \to T \to M \to R \to A \to S\},$$

де N — нормативно-правове регулювання; I — інституційна координація; T — технологічна інфраструктура; M — моніторинг загроз; R — реагування на інциденти; A — аудит і відновлення; S — стратегічне вдосконалення.

У графічному вигляді модель може бути представлена так:

Нормативне регулювання → Інституційна координація → Технологічна інфраструктура → Моніторинг → Реагування → Відновлення й аудит → Стратегічне вдосконалення.

На першому етапі держава формує правові правила захисту інформації, використання хмарних технологій, резервного копіювання, доступу до даних і відповідальності посадових осіб. На другому етапі визначаються повноваження ключових суб'єктів кібербезпеки. На третьому — впроваджуються технологічні рішення: хмарна інфраструктура, шифрування, системи резервного копіювання, EDR, SOC, захищений

обмін даними через «Трембіту». На четвертому етапі здійснюється постійний моніторинг кіберзагроз. На п'ятому — оперативне реагування та локалізація інцидентів. На шостому — відновлення функціонування сервісів, аудит причин інциденту та усунення вразливостей. На сьомому — оновлення політик, стандартів, навчальних програм і технологічних протоколів відповідно до нових загроз.

Інституційний механізм цифрової стійкості реалізується через багаторівневу взаємодію суб'єктів національної системи кібербезпеки. Центральне місце у цій архітектурі посідає Державна служба спеціального зв'язку та захисту інформації України, яка виконує роль регулятора у сфері захищеного урядового зв'язку, технічного захисту інформації та координації реагування на кіберінциденти. Її важливою складовою є команда CERT-UA, що здійснює виявлення, технічний аналіз, попередження та нейтралізацію кіберзагроз [2]. Міністерство цифрової трансформації України відповідає за формування політики цифровізації, розвиток електронних сервісів і впровадження безпечних архітектурних рішень у сфері цифрового врядування. Служба безпеки України фокусується на протидії кібертероризму, кібершпигунству та інформаційно-психологічним операціям противника. Національний координаційний центр кібербезпеки при РНБО забезпечує стратегічну координацію, формування спільного бачення загроз і обмін аналітичною інформацією.

Запропонована модель передбачає, що кожен інституційний суб'єкт відповідає не за ізольовану ділянку, а за конкретний елемент єдиного циклу цифрової безпеки. ДССЗЗІ та CERT-UA забезпечують технічне реагування; Мінцифра — цифрову трансформацію та архітектуру сервісів; СБУ — контррозвідувальний і безпековий компонент; РНБО та НКЦК — стратегічну координацію; органи місцевого самоврядування — практичне впровадження вимог кібербезпеки на рівні громад. Саме така взаємодія створює передумови для переходу від фрагментарного реагування до системного управління кіберризиками.

Особливого значення в умовах воєнного стану набуває кібербезпека органів місцевого самоврядування. Саме на цьому рівні найгостріше проявляються недоліки попередніх підходів до державного регулювання інформаційної безпеки. Центральні органи виконавчої влади мають більше можливостей для залучення міжнародної допомоги, переходу на захищені хмарні рішення та підключення до центрів моніторингу. Натомість значна частина територіальних громад стикається з дефіцитом фінансування, нестачею штатних фахівців із кібербезпеки, застарілим обладнанням, слабкою дисципліною оновлення програмного забезпечення та недостатньою культурою кібергігієни. Так це підвищує ризик того, що муніципальні мережі можуть бути використані як проміжна ланка для атак на ширші державні інформаційні системи.

Для оцінювання ефективності механізму цифрової безпеки необхідно застосовувати не лише описові характеристики, а й систему вимірюваних показників. До ключових KPI кіберстійкості публічного управління доцільно віднести: середній час виявлення інциденту; середній час реагування на інцидент; частку критичних сервісів із резервним копіюванням; рівень доступності державних електронних сервісів; кількість успішно нейтралізованих атак; частку органів влади, підключених до SOC-моніторингу; частку посадових осіб, які пройшли навчання з кібергігієни; кількість проведених аудитів інформаційної безпеки; частку усунутих вразливостей після аудиту; кількість транзакцій, здійснених через захищені канали міжвідомчої взаємодії.

Для узагальненої оцінки пропонується використовувати інтегральний індекс кіберстійкості публічного управління:

$$ІКС = \Sigma\, w_i \times K_i,$$

де *ІКС* — інтегральний індекс кіберстійкості; K_i — нормалізоване значення окремого *KPI* у межах від 0 до 1; w_i — вага відповідного показника; $\Sigma\, w_i = 1$.

Для показників-стимуляторів, де більше значення є кращим, нормалізація може здійснюватися за формулою:

$$K_i = X_i / X_{max}, \text{ якщо } X_i \le X_{max},$$
$$K_i = 1, \text{ якщо } X_i > X_{max}.$$

Для показників-дестимуляторів, де менше значення є кращим, наприклад часу реагування або часу відновлення, доцільно застосовувати формулу:

$$K_i = X_{min} / X_i, \text{ якщо } X_i > X_{min},$$
$$K_i = 1, \text{ якщо } X_i \le X_{min}.$$

Наприклад, для пілотного оцінювання цифрової стійкості системи міжвідомчої взаємодії можна використати три доступні показники: кількість транзакцій, кількість підключених органів та установ, а також квартальну інтенсивність обміну даними. Якщо встановити цільові значення: 7 млрд. транзакцій, 230 підключених інституцій і 790 млн. транзакцій за квартал, то за умови досягнення цих параметрів частковий індекс масштабованості системи становитиме:

$$I_м = 0{,}4 \times 1 + 0{,}3 \times 1 + 0{,}3 \times 1 = 1{,}0.$$

Так цей розрахунок не є повною оцінкою кібербезпеки, оскільки не враховує закриті технічні показники, зокрема кількість інцидентів, час реагування або показники вразливостей. Однак він демонструє, як описові характеристики цифрової інфраструктури можуть бути переведені у вимірювану аналітичну площину. Для

повної валідації моделі необхідно поєднувати відкриті статистичні дані з внутрішніми журналами SOC, результатами аудитів і звітами про кіберінциденти.

Технологічний вимір цифрової безпеки публічного управління базується на принципах децентралізації, резервного копіювання, наскрізного шифрування, сегментації доступу та мінімізації концентрації критичних даних в одному центрі. Одним із прикладів такого підходу є система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» [3]. Її архітектура не передбачає створення єдиної централізованої бази даних, яка могла б стати критичною мішенню для противника. Натомість «Трембіта» забезпечує захищений обмін інформацією між автономними реєстрами різних органів влади. Дані передаються через захищені канали лише в момент конкретного запиту, що зменшує ризик масового витоку інформації внаслідок компрометації одного елемента системи.

Емпіричне значення цієї системи підтверджується масштабом її використання: у II кварталі 2024 року через «Трембіту» було здійснено понад 790 млн. транзакцій, а станом на 30 червня 2024 року загальна кількість транзакцій від запуску системи перевищила 6,2 млрд. За даними розробників і партнерів системи, через «Трембіту» обмінюються даними понад 230 українських державних і приватних інституцій, а загальний обсяг транзакцій перевищив 7 млрд. Ці показники дають підстави розглядати «Трембіту» не лише як технічний інструмент, а як інфраструктурний елемент цифрової стійкості публічного управління.

Причинно-наслідковий зв'язок між архітектурою «Трембіти» та зниженням кіберризиків полягає у трьох аспектах. По-перше, відсутність єдиної централізованої бази зменшує потенційний масштаб шкоди у разі компрометації окремого реєстру. По-друге, обмін даними за запитом знижує потребу в дублюванні великих масивів персональної інформації. По-третє, стандартизовані канали взаємодії дають змогу простіше фіксувати, контролювати та аналізувати міжвідомчі транзакції. Отже, ефект цифрової безпеки виникає не лише через технічне шифрування, а через зміну самої логіки обміну даними.

Політика пріоритету хмарних технологій стала ще одним важливим напрямом трансформації цифрової безпеки. Її сутність полягає у переході від моделі фізичної концентрації даних на локальних серверах до гібридної інфраструктури, де частина даних обробляється локально, а критичні реєстри та резервні копії можуть розміщуватися у захищених дата-центрах країн-партнерів [4]. Такий підхід зменшує залежність державного управління від фізичної цілісності окремого дата-центру. Якщо локальна інфраструктура пошкоджується внаслідок ракетного удару, кібератаки або енергетичної кризи, наявність резервних копій і хмарної інфраструктури підвищує ймовірність швидкого відновлення роботи сервісів.

Причинний механізм впливу хмарної міграції на зниження ризиків можна описати через базову формулу кіберризику:

$$R = P \times I \times V,$$

де R — рівень ризику; P — імовірність реалізації загрози; I — потенційний вплив інциденту; V — рівень вразливості системи.

У традиційній локальній моделі фізичне знищення дата-центру може одночасно підвищувати всі три складові ризику: імовірність втрати доступу до сервісу, масштаб наслідків і залежність від конкретної інфраструктурної точки. У гібридній хмарній моделі ймовірність повної втрати даних зменшується завдяки географічному резервуванню, вплив інциденту обмежується наявністю альтернативних середовищ, а рівень вразливості знижується через використання розподіленої архітектури. Наприклад, якщо умовно оцінити ризик втрати доступності сервісу в локальній моделі як $R1 = 0{,}35 \times 0{,}90 \times 1{,}00 = 0{,}315$, а після переходу до хмарно-резервної моделі як $R2 = 0{,}10 \times 0{,}70 \times 0{,}50 = 0{,}035$, то відносне зниження ризику становитиме приблизно 88,9%. Такий розрахунок має ілюстративний характер, але демонструє логіку кількісного аналізу ефективності управлінського рішення.

Водночас первинне проникнення у державні мережі часто відбувається не лише через складні технічні вразливості, а й через людський фактор: фішингові листи, заражені вкладення, підроблені повідомлення, слабкі паролі або недотримання правил кібергігієни. Саме тому в органах публічного управління дедалі активніше впроваджуються системи виявлення та реагування на кінцевих точках — EDR. Їхнє завдання полягає у моніторингу поведінки комп'ютерів, автоматичному блокуванні шкідливого програмного забезпечення, ізоляції заражених пристроїв і передачі даних до центрів моніторингу. У межах запропонованої моделі EDR є не самостійним інструментом, а частиною ширшого циклу: виявлення загрози — локалізація — аналіз — відновлення — оновлення правил безпеки. Управлінські процеси та протоколи реагування є не менш важливими, ніж технологічні рішення. Створення мережі галузевих і регіональних центрів оперативного реагування на кіберінциденти, зокрема SOC, дає змогу централізовано моніторити трафік державного сектору, виявляти аномальні активності, накопичувати інформацію про інциденти та передавати попередження іншим органам влади [5]. У такій системі важливою є не лише наявність технічної платформи, а й чіткий управлінський регламент: хто фіксує інцидент, хто ухвалює рішення про ізоляцію системи, хто відповідає за комунікацію з користувачами, хто проводить аудит і хто контролює усунення вразливостей. Без процедурної логіки навіть сучасне обладнання не гарантує належного рівня кіберстійкості.

Окреме місце у механізмі цифрової безпеки посідає людський капітал. Людський фактор залишається однією з найвразливіших ланок у системі публічного управління, оскільки більшість посадових осіб не є фахівцями з кібербезпеки, але щодня працюють із документами, персональними даними, електронною поштою та державними інформаційними системами. Тому програми з кібергігієни мають розглядатися не як формальний елемент підвищення кваліфікації, а як інструмент зниження операційних ризиків. Їхню ефективність можна вимірювати через такі KPI: частку працівників, які пройшли навчання; кількість симуляцій фішингових атак; відсоток працівників, які правильно реагують на підозрілі повідомлення; зменшення кількості інцидентів, спричинених людською помилкою. Регулярний аудит інформаційної безпеки має доповнюватися контролем виконання рекомендацій, інакше він залишатиметься лише діагностичною процедурою.

Важливим інструментом підвищення стійкості є також залучення «білих» хакерів до пошуку вразливостей у державних електронних сервісах за фінансову винагороду [6]. Така практика свідчить про перехід від закритої бюрократичної моделі безпеки до відкритішої, партнерської та проактивної моделі, у якій держава визнає цінність зовнішньої експертизи. У цьому контексті цифрова безпека перестає бути виключно внутрішньою функцією державного апарату й перетворюється на сферу взаємодії публічного сектору, приватних технологічних компаній, громадянського суспільства, міжнародних партнерів і професійної кіберспільноти.

Окремим прикладом цифрової стійкості є екосистема «Дія». Її значення полягає не лише у зручності надання електронних послуг, а й у специфічній архітектурі безпеки. Застосунок не зберігає персональні дані громадян у класичному розумінні — ані на мобільному пристрої, ані у вигляді єдиної централізованої бази. Він працює як транзитний інтерфейс, який формує захищений запит до відповідних державних реєстрів і відображає результат користувачеві [7]. Така архітектура знижує ризик масового викрадення персональних даних у разі компрометації окремого елемента інфраструктури. Масштаб системи підтверджує її управлінське значення: у 2025 році кількість користувачів «Дії» перевищила 23 млн., що робить її одним із центральних каналів взаємодії громадян із державою.

Кейс «Дії» може бути використаний для емпіричного вимірювання цифрової стійкості. Доцільно застосовувати такі KPI: кількість активних користувачів; кількість доступних цифрових документів і послуг; стабільність роботи застосунку під час пікових навантажень; час відновлення після збоїв; кількість успішних запитів до реєстрів; рівень довіри громадян; кількість інцидентів, що не призвели до масового витоку даних. Наприклад, якщо як цільовий показник охоплення населення цифровим сервісом умовно встановити 25 млн. користувачів, а фактичне значення становить 23 млн., то нормалізований показник цифрового охоплення дорівнює:

$$K_{\text{охоплення}} = 23 / 25 = 0{,}92.$$

Так це свідчить про високий рівень проникнення цифрового сервісу, але не є самодостатнім доказом його кіберстійкості. Для повної оцінки цей показник має бути поєднаний із технічними індикаторами: uptime, кількістю інцидентів, часом реагування, часом відновлення, результатами аудитів і показниками захищеності реєстрів. Саме така комбінація дає змогу уникнути декларативності й перейти до вимірюваної оцінки ефективності. Порівняльний аналіз показує, що українська модель цифрової безпеки формується під впливом воєнної необхідності, тоді як підходи ЄС і НАТО більше орієнтовані на нормативну гармонізацію, стандартизацію процедур, оперативну сумісність і колективну стійкість. Для ЄС характерним є акцент на захисті критичної інфраструктури, відповідальності операторів цифрових послуг, захисті персональних даних і стандартизованому управлінні ризиками. Для НАТО важливими є стійкість комунікацій, захищеність військово-цивільної взаємодії, обмін інформацією про загрози та спроможність діяти в умовах гібридних атак. Українська модель має спільні риси з цими підходами, однак відрізняється вищим рівнем адаптивності, оскільки цифрові рішення впроваджуються в умовах постійних кібератак, фізичного руйнування інфраструктури та потреби швидкого відновлення управлінських функцій [8].

Водночас для подальшого наближення до європейських і євроатлантичних підходів Україні доцільно посилити стандартизацію KPI, запровадити регулярну незалежну оцінку кіберстійкості органів влади, уніфікувати протоколи реагування на інциденти та розширити практику обміну даними про загрози між державним і приватним секторами. Саме порівняння з підходами ЄС і НАТО дозволяє визначити не лише сильні сторони української системи, а й напрями її інституційного вдосконалення. З огляду на сучасні виклики стратегічний розвиток системи цифрової безпеки потребує переходу від реактивної до проактивної моделі управління. Центральним напрямом такої трансформації має стати впровадження концепції нульової довіри — Zero Trust — в органах державної влади та місцевого самоврядування [9]. Її сутність полягає у тому, що жоден користувач, пристрій або запит не вважається безпечним автоматично. Кожна дія має проходити багатофакторну перевірку, контроль прав доступу, моніторинг поведінки та фіксацію в журналах безпеки.

Причинно-наслідковий вплив Zero Trust на зниження кіберризиків полягає в обмеженні можливостей зловмисника після первинного проникнення. Якщо в традиційній моделі компрометація одного облікового

запису може надати доступ до значної частини внутрішньої мережі, то в моделі Zero Trust кожен запит перевіряється окремо, що зменшує ймовірність горизонтального переміщення зловмисника, скорочує потенційний масштаб шкоди та підвищує якість аудиту дій користувачів. У кількісному вимірі ефект Zero Trust може бути оцінений через зменшення кількості несанкціонованих доступів, скорочення середнього часу виявлення інциденту, зниження частки привілейованих облікових записів і збільшення частки дій, які проходять багатофакторну перевірку. Перспективним напрямом є також інтеграція алгоритмів штучного інтелекту до державних центрів моніторингу кіберзагроз. В умовах кадрового дефіциту такі інструменти можуть автоматизувати первинний аналіз інцидентів, виявляти нетипові патерни поведінки, ранжувати загрози за рівнем критичності та допомагати фахівцям швидше ухвалювати рішення. Водночас використання штучного інтелекту не має замінювати експертний контроль, оскільки помилки автоматизованих систем можуть призвести як до пропуску небезпечних атак, так і до блокування легітимної діяльності органів влади.

Оцінка економічного ефекту кібербезпеки також має бути включена до аналізу цифрової стійкості. Економічний ефект можна визначати як різницю між потенційними втратами від кіберінциденту без впровадження заходів безпеки та фактичними витратами на захист і відновлення:

$$Ек = L0 — L1 — C,$$

де $Ек$ — економічний ефект; $L0$ — прогнозовані втрати без заходів кіберзахисту; $L1$ — залишкові втрати після впровадження заходів; C — вартість впровадження та підтримки заходів кібербезпеки.

Наприклад, якщо потенційні втрати від зупинки державного сервісу оцінюються в 10 млн. грн, після впровадження резервування та SOC-моніторингу залишкові втрати становлять 2 млн. грн, а витрати на захист — 3 млн. грн, то економічний ефект дорівнює:

$$Ек = 10 – 2 – 3 = 5 \text{ млн. грн.}$$

Приклад демонструє, що кібербезпека має розглядатися не лише як витратна стаття, а як інструмент зниження потенційних збитків, підтримання довіри громадян і забезпечення безперервності публічних послуг.

Для подолання кадрової кризи доцільним є створення національного кіберрезерву — спеціального механізму легального та оперативного залучення фахівців приватного сектору, науковців, експертів із кібербезпеки та сертифікованих етичних хакерів до захисту державних електронних ресурсів у кризових ситуаціях [10]. Такий резерв міг би функціонувати за аналогією з мобілізаційними або волонтерськими моделями, але з чітким правовим статусом, процедурами доступу до інформації, відповідальністю та системою компенсацій. Так це дало б змогу державі швидше нарощувати експертні спроможності без необхідності постійно утримувати надмірно великий штат фахівців. Наукова новизна запропонованого підходу полягає у тому, що цифрова безпека публічного управління розглядається як формалізований управлінський механізм, який поєднує інституційні, технологічні, кадрові, процедурні, економічні та міжнародні компоненти. На відміну від підходів, що зосереджуються переважно на описі суб'єктів кібербезпеки або окремих цифрових сервісів, у цьому дослідженні запропоновано модель повного циклу цифрової безпеки: від нормативного регулювання та ідентифікації загроз до реагування, відновлення, аудиту й стратегічного вдосконалення. Додатковим елементом новизни є введення інтегрального індексу кіберстійкості, який дозволяє оцінювати ефективність цифрової безпеки через вимірювані показники: час реагування, рівень доступності сервісів, кількість транзакцій, частку усунутих вразливостей, рівень охоплення працівників навчанням із кібергігієни та масштаб підключення до захищених каналів обміну даними.

Таким чином, цифрова безпека публічного управління України в умовах війни має розглядатися не як сукупність технічних заходів, а як багаторівнева система управління ризиками. Її ефективність залежить від здатності держави поєднувати нормативне регулювання, інституційну координацію, технологічну модернізацію, кадрову підготовку, міжнародну підтримку та регулярне вимірювання результатів. Запропонована модель, інтегральний індекс кіберстійкості та пілотні розрахунки на прикладі «Трембіти», «Дії» й хмарної міграції державних даних створюють основу для подальшої емпіричної перевірки та практичного застосування в системі публічного управління України.

Висновки і перспективи подальших досліджень. Проведене дослідження дозволяє стверджувати, що забезпечення цифрової безпеки в системі публічного управління України трансформувалося з допоміжної технічної функції у фундаментальний чинник державного суверенітету та стійкості в умовах гібридної війни. Стратегічний перехід від консервативної моделі фізичного розміщення серверів до гнучкої хмарної архітектури та децентралізованого обміну даними виявився критично важливим для збереження безперервності управління під час масованих ворожих атак. Інституційна взаємодія ключових суб'єктів довела свою здатність до оперативної мобілізації ресурсів, проте виявила низку системних вразливостей, зокрема на рівні органів місцевого самоврядування, де відчувається гостра нестача кваліфікованих кадрів, застаріле матеріально-технічне забезпечення та недостатня фінансова автономія. Аналіз показав, що поточна парадигма реагування має бути змінена на проактивну модель, що базується на концепції «нульової довіри» (Zero Trust). Впровадження цієї моделі вимагає перегляду управлінської філософії: кожен запит до державних

даних повинен підлягати багатофакторній верифікації, а моніторинг інфраструктури — здійснюватися в режимі реального часу за допомогою алгоритмів штучного інтелекту. Ключовим інструментом для подолання кадрового дефіциту в державному секторі має стати створення національного кіберрезерву, що дозволить легально та гнучко залучати провідних експертів приватного IT-сектору до захисту державних ресурсів у критичні періоди.

Перспективи подальших досліджень доцільно спрямувати на вирішення завдань нормативно-правової гармонізації, зокрема імплементацію вимог європейської Директиви NIS2 у національне законодавство, що забезпечить синхронізацію стандартів безпеки з країнами ЄС та НАТО. Важливим вектором є розвиток технологічної автономії шляхом дослідження можливостей розробки та впровадження вітчизняних програмно-апаратних комплексів кіберзахисту для зменшення залежності від зовнішніх постачальників. Також потребує уваги формування культури безпеки через розробку методології переходу від формальних інструктажів до впровадження «кіберстійкості як повсякденної норми», а також моделювання фінансової стійкості громад через механізми цільового фінансування та субвенційної підтримки для оновлення їхньої IT-інфраструктури. Підсумовуючи, слід наголосити, що кіберпростір для сучасної України є зоною постійного конфлікту. Формування однієї з найбільш захищених систем публічного управління у світі можливе лише за умови консолідації зусиль усіх рівнів влади, постійного впровадження інновацій та швидкої адаптації до динамічних викликів сучасної гібридної війни.

ДОДАТКОВА ІНФОРМАЦІЯ

ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем та публічних електронних реєстрів в умовах воєнного стану. *Офіційний вебпортал парламенту України.* URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення: 20.04.2026).

2. Про CERT-UA. *CERT-UA*. URL: https://cert.gov.ua/about-us (дата звернення: 23.04.2026).

3. Система електронної взаємодії органів виконавчої влади «Трембіта». *Електронне урядування Дніпропетровської області*. URL: https://egov.dp.gov.ua/services/sistema-trembita (дата звернення: 23.04.2026).

4. Як розвивається Стратегія Cloud First в різних країнах світу. *De Novo.* URL: https://denovo.ua/blog/cloud-first-v-mire (дата звернення: 15.04.2026).

5. Про внесення змін до Порядку ведення Єдиного державного реєстру ветеранів війни. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 15.04.2026).

6. Уряд легалізував Bug Bounty для державних систем. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/uryad-legalizuvav-bug-bounty-dlya-derzhavnikh-sistem (дата звернення: 23.04.2026).

7. Як ми забезпечуємо безпеку «Дії». *Міністерство цифрової трансформації України.* URL: https://thedigital.gov.ua/news/technologies/bezpeka-mobilnogo-zastosunku-diya (дата звернення: 10.04.2026).

8. Таллінський механізм: два роки міжнародної підтримки кіберстійкості України. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/tallinnskii-mekhanizm-dva-roki-mizhnarodnoyi-pidtrimki-kiberstiikosti-ukrayini (дата звернення: 22.04.2026).

9. Що таке модель нульової довіри (Zero Trust) і навіщо вона потрібна. *GigaTrans.* URL: https://gigatrans.ua/ua/news/chto-takoe-model-nulevogo-doveriya-zero-trust-i-zachem-ona-nuzhna (дата звернення: 07.04.2026).

10. Україна отримала доступ до Резерву кібербезпеки ЄС. *Міністерство цифрової трансформації України.* URL: https://digitalstate.gov.ua/uk/news/govtech/ukraine-gains-access-to-the-eu-cybersecurity-reserve-operational-support-in-the-event-of-large-scale-attacks (дата звернення: 05.04.2026).

References

1. Cabinet of Ministers of Ukraine. (2022). *Deiaki pytannia zabezpechennia funktsionuvannia informatsiino-komunikatsiinykh system, elektronnykh komunikatsiinykh system ta publichnykh elektronnykh reiestriv v umovakh voiennoho stanu*. Retrieved from https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text [in Ukrainian].

2. CERT-UA. (n.d.). *Pro CERT-UA*. Retrieved from https://cert.gov.ua/about-us [in Ukrainian].

3. Dnipropetrovsk Regional State Administration. (n.d.). *Systema elektronnoi vzaiemodii orhaniv vykonavchoi vlady "Trembita"*. Retrieved from https://egov.dp.gov.ua/services/sistema-trembita [in Ukrainian].

4. De Novo. (2026). *Yak rozvyvaietsia Stratehiia Cloud First v riznykh krainakh svitu*. Retrieved from https://denovo.ua/blog/cloud-first-v-mire [in Ukrainian].

5. Cabinet of Ministers of Ukraine. (2025). *Pro vnesennia zmin do Poriadku vedennia Yedynoho derzhavnoho reiestru veteraniv viiny*. Retrieved from https://zakon.rada.gov.ua/laws/show/1533–2025-%D0%BF#Text [in Ukrainian].

6. State Service of Special Communications and Information Protection of Ukraine. (2026). *Uriad lehalizuvav Bug Bounty dlia derzhavnykh system*. Retrieved from https://cip.gov.ua/ua/news/uryad-legalizuvav-bug-bounty-dlya-derzhavnikh-sistem [in Ukrainian].

7. Ministry of Digital Transformation of Ukraine. (2026). *Yak my zabezpechuiemo bezpeku "Dii"*. Retrieved from https://thedigital.gov.ua/news/technologies/bezpeka-mobilnogo-zastosunku-diya [in Ukrainian].

8. State Service of Special Communications and Information Protection of Ukraine. (2026). *Tallinnskyi mekhanizm: dva roky mizhnarodnoi pidtrymky kiberstiikosti Ukrainy*. Retrieved from https://cip.gov.ua/ua/news/tallinnskii-mekhanizm-dva-roki-mizhnarodnoyi-pidtrimki-kiberstiikosti-ukrayini [in Ukrainian].

9. GigaTrans. (2026). *Shcho take model nuliovoi doviry (Zero Trust) i navishcho vona potribna*. Retrieved from https://gigatrans.ua/ua/news/chto-takoe-model-nulevogo-doveriya-zero-trust-i-zachem-ona-nuzhna [in Ukrainian].

10. Ministry of Digital Transformation of Ukraine. (2026). *Ukraina otrymala dostup do Rezervu kiberbezpeky Ye* S. Retrieved from https://digitalstate.gov.ua/uk/news/govtech/ukraine-gains-access-to-the-eu-cybersecurity-reserve-operational-support-in-the-event-of-large-scale-attacks [in Ukrainian].

Дата першого надходження статті до видання: 25.04.2026
Дата прийняття статті до друку після рецензування: 19.05.2026
Дата публікації: 28.05.2026

ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

Berladinyuk Yevhen
higher education Student at the third (educational and scientific) level of higher education
Ivano-Frankivsk National Technical University of Oil and Gas

MECHANISMS FOR ENSURING DIGITAL SECURITY IN THE PUBLIC ADMINISTRATION SYSTEM OF UKRAINE DURING MILITARY AND CRISIS CHALLENGES

Summary. *Introduction. The article analyzes the evolution of the digital security architecture of the public administration system of Ukraine in the conditions of a full-scale war. It is proven that the strategic transformation of approaches to information protection – from the physical placement of servers to the use of cloud technologies and the concept of "zero trust" – has become a key factor in ensuring the continuity of public administration and the provision of public services during unprecedented cyber threats.*

The purpose of the article is a comprehensive analysis of institutional, technological and managerial mechanisms for ensuring the digital resilience of state authorities and local governments, as well as outlining the prospects for the transition from a reactive to a proactive model of cyber defense.

Materials and methods. The study is based on the analysis of the regulatory framework, digitalization strategies and the experience of the functioning of the critical information infrastructure of Ukraine during the war period. The methods of system and structural analysis, modeling of management processes, as well as the synthesis of best practices of international cooperation in the field of cyber defense were used.

Results. The institutional architecture of the cybersecurity system and the role of key actors (DSSZZI, Ministry of Digital, SBU, NCCC) were studied. Technological vectors of protection were identified, in particular, the successful implementation of the "Diya" ecosystem and the "Trembita" system. Critical vulnerabilities of the system were identified, including staff shortages, technological obsolescence of local infrastructure, and energy instability. The need to implement the "Zero Trust" model, create a national cyber reserve, and integrate artificial intelligence algorithms into threat monitoring systems was substantiated.

Prospects. Further research should focus on the implementation of European directives, in particular NIS2, the development of domestic technological solutions to reduce dependence on external suppliers, and the formation of a culture of "cyber resilience as an everyday norm" through the development of professional competencies of civil servants.

Key words: *public administration, digital security, cyber resilience, martial law, cloud technologies, Zero Trust, state registers, "Trembita", cyber hygiene, critical infrastructure.*