

*Олешко О.Ю., здобувач, Національний університет цивільного захисту
України, Харків, Україна.
ORCID: 0009-0004-6834-1669*

*Oleshko O., Postgraduate Student, National University of Civil Defence of
Ukraine, Kharkiv, Ukraine*

ФАКТОРИ ЦИФРОВОЇ ГОТОВНОСТІ РЕГІОНАЛЬНОГО УПРАВЛІННЯ

FACTORS OF DIGITAL READINESS OF REGIONAL GOVERNANCE

Статтю присвячено систематизації факторів цифрової готовності регіонального управління. Запропоновано розуміти цифрову готовність як здатність органів влади та регіональної інституційної системи ініціювати, впроваджувати, безпечно використовувати й удосконалювати цифрові рішення для виконання публічних функцій. Фактори поділено на зовнішні та внутрішні, ресурсні та процесні, стимулювальні та обмежувальні. Виокремлено інфраструктурний, інституційний, нормативний, кадровий, фінансовий, інформаційний, сервісний, безпековий, соціальний та інноваційний блоки. Показано, що наявність інтернет-доступу та комп'ютерної техніки не гарантує готовності, якщо відсутні якісні дані, управлінське лідерство, навички, міжвідомча взаємодія й довіра користувачів. Обґрунтовано необхідність оцінювати не лише середній регіональний стан, а внутрішньорегіональні цифрові розриви між обласним центром, малими містами та сільськими територіями. Запропоновано послідовність діагностики: інвентаризація ресурсів, оцінювання зрілості процесів, аналіз бар'єрів користувачів, визначення ризиків, формування профілю готовності та вибір адресних заходів. Визначено ризики низької готовності: фрагментацію систем, залежність від постачальника, витік

даних, цифрове виключення, формальну автоматизацію і нестійкість результатів.

Ключові слова: цифрова готовність, регіональне управління, цифровий розрив, інформаційна інфраструктура, людський капітал, кібербезпека, електронні послуги.

The article systematizes the factors of digital readiness of regional governance. Digital readiness is defined as the capacity of public authorities and the regional institutional system to initiate, implement, securely use and continuously improve digital solutions for public functions. Factors are classified as external and internal, resource-based and process-based, enabling and constraining. Infrastructure, institutional, legal, human-capital, financial, information, service, security, social and innovation blocks are identified. Internet access and computer equipment are shown not to guarantee readiness when high-quality data, managerial leadership, skills, inter-agency cooperation and user trust are absent. The assessment should cover not only the regional average but also internal digital divides among the regional capital, small towns and rural areas. A diagnostic sequence is proposed: inventory of resources, assessment of process maturity, analysis of user barriers, risk identification, construction of a readiness profile and selection of targeted measures. Key risks of low readiness include fragmented systems, vendor lock-in, data leakage, digital exclusion, formal automation and the unsustainability of results.

Keywords: digital readiness, regional governance, digital divide, information infrastructure, human capital, cybersecurity, electronic services.

Постановка проблеми. Поширення цифрових технологій створює для регіональних органів влади можливість швидшого обміну інформацією, дистанційного надання послуг і аналітичного супроводу рішень. Проте однаковий програмний продукт або нормативна вимога дають різний результат у регіонах із неоднаковою інфраструктурою, кадровим потенціалом і організаційною культурою. Тому перед упровадженням

масштабних проєктів необхідно оцінити цифрову готовність - сукупність умов і спроможностей, від яких залежить практичне використання технологій.

Цифрову готовність часто помилково зводять до кількості комп'ютерів, рівня підключення до інтернету або наявності офіційного вебсайту. Такі показники відображають ресурсну основу, але не показують, чи переглянуті процедури, чи сумісні інформаційні системи, чи володіють працівники необхідними навичками, чи захищені дані та чи здатні громадяни завершити послугу дистанційно. Відсутність системного підходу призводить до формальної цифровізації, коли техніка використовується для відтворення паперових процесів без зміни результату.

Аналіз останніх публікацій за проблематикою. Концепція розвитку цифрової економіки та суспільства України визначила інфраструктуру, цифрові навички, стимули й розвиток цифрових технологій як взаємопов'язані напрями [1]. Законодавство про захист інформації та електронні довірчі послуги закріпило безпекові й довірчі передумови електронної взаємодії [2; 3]. Отже, готовність має оцінювати не лише можливість підключення, а здатність використовувати цифрові інструменти у правомірний і безпечний спосіб.

Світовий банк у доповіді про цифрові дивіденди наголосив, що технологічний ефект залежить від так званих аналогових доповнень: інституцій, навичок і підзвітності [4]. Огляд електронного урядування ООН 2018 року поєднує онлайн-послуги, телекомунікаційну інфраструктуру та людський капітал [5]. Ці підходи підтверджують, що регіональна цифрова готовність є багатовимірною характеристикою, а не одиничним технічним індикатором.

Постановка завдання. Метою статті є систематизація факторів цифрової готовності регіонального управління та формування логіки їх діагностики. Для досягнення мети необхідно визначити сутність готовності, класифікувати фактори, розкрити взаємозв'язки між ними, встановити

основні ризики та запропонувати послідовність формування регіонального профілю, придатного для вибору управлінських заходів.

Виклад основного матеріалу. Цифрову готовність регіонального управління пропонується розуміти як здатність органів влади, підпорядкованих установ і партнерської мережі регіону планувати, упроваджувати, безпечно експлуатувати та вдосконалювати цифрові рішення, які забезпечують виконання публічних функцій і доступність послуг. Це визначення включає не лише вихідні ресурси, а й організаційну здатність перетворювати їх на стійкий результат.

Фактори готовності можна класифікувати за джерелом впливу. Зовнішні фактори формуються загальнодержавною політикою, ринком телекомунікацій, доступністю технологій, економічною кон'юктурою і нормативними змінами. Внутрішні залежать від керівництва регіону, якості процесів, компетенцій, фінансового планування та взаємодії установ. За характером фактори поділяються на ресурсні - інфраструктура, фінанси, кадри - і процесні - координація, управління даними, проєктна дисципліна, навчання і зворотний зв'язок.

Інфраструктурний фактор охоплює доступність широкосмугового зв'язку, надійність мереж, робочі місця, обчислювальні потужності, засоби електронної ідентифікації, резервне копіювання й технічну підтримку. Важливим є не лише середній рівень покриття, а фактична можливість доступу в окремих громадах і установах. Нерівномірність інфраструктури створює внутрішньорегіональний цифровий розрив, коли жителі обласного центру мають значно ширші можливості, ніж населення віддалених територій.

Нормативний фактор визначає, чи дозволяють правила завершити процес у цифровій формі, використати електронний документ, ідентифікувати особу та обмінятися даними. Наявність загального закону не завжди усуває відомчі вимоги щодо паперових копій або особистого звернення. Тому регіональна готовність включає інвентаризацію локальних регламентів і приведення їх у відповідність до електронної взаємодії.

Правова невизначеність змушує посадових осіб дублювати паперові процедури та зменшує довіру до цифрового результату.

Інституційний фактор характеризує лідерство, розподіл відповідальності й здатність координувати різні структурні підрозділи. Якщо цифрові проєкти віднесені виключно до технічного підрозділу, вони не змінюють галузеві процеси. Власником трансформації має бути керівник відповідної функції, а ІТ-фахівці забезпечують технологічну реалізацію. На регіональному рівні потрібен координаційний механізм, який погоджує стандарти, портфель проєктів, архітектуру даних і пріоритети підтримки громад.

Кадровий фактор охоплює базову цифрову грамотність, спеціалізовані технічні компетенції та управлінські навички. Для керівників важливо розуміти можливості й обмеження технологій, формулювати результат і управляти змінами. Для державних службовців потрібні навички роботи з електронними документами, даними й захистом інформації. Для проєктних команд необхідні бізнес-аналіз, управління закупівлями, тестування і комунікація з користувачами. Дефіцит хоча б однієї групи компетенцій робить систему залежною від зовнішнього постачальника.

Фінансовий фактор визначає не лише стартове фінансування, а спроможність підтримувати систему впродовж життєвого циклу. До витрат належать інтеграція, ліцензування, захист, оновлення, навчання, резервування, технічна підтримка та міграція даних. Бюджетування лише на створення продукту формує ризик припинення роботи після завершення проєкту. Водночас надмірна децентралізація фінансування може призвести до багаторазового придбання подібних рішень різними громадами.

Інформаційний фактор охоплює повноту, точність, актуальність і сумісність даних. Цифровий сервіс не може бути якіснішим за дані, на яких він працює. Поширеними бар'єрами є різні довідники, відсутність унікальних ідентифікаторів, дублювання записів і невизначеність власника. Оцінювання готовності має включати реєстр основних наборів даних, визначення

відповідальних, правила оновлення й аналіз законних підстав обміну. Відкритість даних не скасовує вимог до захисту персональної інформації.

Сервісний фактор відображає зрілість процедур і орієнтацію на користувача. Послуга є цифровою готовою, якщо її правові та організаційні етапи можуть бути виконані без зайвого дублювання, результат надається у визначений строк, статус звернення відстежується, а користувач отримує допомогу. Часткова електронна форма, після якої необхідно особисто принести документи, свідчить про низьку процесну зрілість. Тому слід аналізувати весь маршрут, а не окрему точку контакту.

Безпековий фактор включає політику доступу, автентифікацію, журналювання, резервування, реагування на інциденти та навчання персоналу. Технологічний захист неефективний без організаційних правил: працівники можуть передавати паролі, використовувати незахищені носії або надавати надмірні права. Довіра до електронної взаємодії залежить від здатності органу пояснити, які дані збираються, для чого використовуються, хто має доступ і як особа може виправити помилку або оскаржити рішення.

Соціальний фактор охоплює цифрові навички населення, доступність пристроїв, мотивацію, довіру й потребу в онлайн-взаємодії. Навіть досконала система не створює суспільного ефекту, якщо значна частина користувачів не може нею скористатися. Регіональна політика повинна передбачати допоміжні точки доступу, консультації, просту мову, доступність для людей з інвалідністю й збереження альтернативних каналів. Цифрова готовність влади й цифрова готовність населення мають оцінюватися взаємопов'язано.

Інноваційний фактор характеризує здатність експериментувати, оцінювати й поширювати рішення. Організація з низькою толерантністю до обґрунтованого експерименту схильна відтворювати застарілі процедури. Водночас інноваційність не означає безконтрольного впровадження. Потрібні обмежені пілоти, критерії припинення, перевірка безпеки, аналіз ефекту та документування досвіду. Регіон може створювати середовище обміну практиками між громадами, університетами, бізнесом і громадськими організаціями.

Фактори взаємодіють і можуть посилювати або нейтралізувати один одного. Розвинена інфраструктура не дає ефекту без навичок і процесної зміни. Сильне керівництво не компенсує відсутності правової підстави для обміну даними. Достатнє фінансування може бути неефективним за низької якості технічного завдання. Тому інтегральна готовність не повинна визначатися простим підсумовуванням ресурсів: необхідно виявляти критичні мінімальні умови, дефіцит яких блокує всю систему.

Діагностику доцільно проводити у шість етапів. Перший - інвентаризація інфраструктури, систем, даних, кадрів і бюджетів. Другий - опис ключових процедур і рівня їх цифрової зрілості. Третій - аналіз користувацьких бар'єрів та внутрішньорегіональних розривів. Четвертий - оцінка безпеки, залежності від постачальників і стійкості. П'ятий - формування профілю за блоками без приховування слабких місць одним середнім балом. Шостий - вибір адресного пакета заходів і встановлення показників прогресу.

Основними ризиками низької готовності є фрагментація систем, повторне введення даних, технологічна залежність, незаплановані витрати, витік інформації, цифрове виключення і втрата довіри. Окремим ризиком є формальна автоматизація неефективного процесу, яка робить його швидшим, але не простішим. Профіль готовності має використовуватися не для публічного таврування регіонів, а для визначення послідовності інвестицій, підтримки та навчання.

Організаційна культура є наскрізним фактором готовності. Працівники можуть формально пройти навчання, але продовжувати уникати електронних процедур через страх помилки, додатковий контроль або звичку до паперового погодження. Керівництво має пояснювати мету змін, переглядати посадові функції, створювати безпечний простір для повідомлення про проблеми та винагороджувати не кількість нових систем, а поліпшення процесів. Без управління змінами цифровий проєкт сприймається як додаткове навантаження.

Територіальний фактор потребує аналізу не лише інфраструктурного покриття, а повного маршруту доступу. У сільській місцевості цифрова послуга може компенсувати значну відстань, але її використання залежить від зв'язку, пристрою, навичок і можливості отримати консультацію. У великих містах обмеженням може бути фрагментація установ і високе навантаження. Тому однаковий показник використання має різну інтерпретацію, а заходи повинні відповідати конкретній комбінації бар'єрів.

Профіль готовності доцільно будувати як матрицю рівнів, а не як один рейтинг. Для кожного блоку визначаються базовий, функціональний, інтегрований і трансформаційний рівні. Базовий означає наявність мінімальних ресурсів і правил; функціональний - стабільне виконання окремих електронних операцій; інтегрований - міжвідомчу взаємодію та спільні дані; трансформаційний - постійне вдосконалення на основі аналітики й зворотного зв'язку. Така матриця показує реальний напрям переходу між станами.

Моніторинг готовності має бути регулярним, але не надмірно звітним. Інфраструктурні показники можуть оновлюватися щорічно, дані про використання послуг - щоквартально або щомісячно, інформація про інциденти - оперативно. Після кожного значного проєкту необхідно повторно оцінювати відповідні блоки й перевіряти, чи усунуто початковий бар'єр. Якщо ресурс створено, але користування не зросло, слід аналізувати процес, комунікацію та довіру, а не автоматично збільшувати фінансування.

Порівняння регіонів має враховувати вихідні умови та функціональні особливості. Високий рівень використання онлайн-послуг у великому місті може бути результатом концентрації населення й установ, тоді як менший показник у сільському регіоні не завжди свідчить про слабе управління. Доцільно порівнювати території за подібними профілями, аналізувати динаміку та оцінювати, наскільки управлінські рішення компенсують об'єктивні обмеження. Це запобігає перетворенню готовності на формальний рейтинг без практичного змісту.

Для кожного виявленого дефіциту потрібно визначати відповідального суб'єкта й доступний інструмент. Проблема зв'язку може потребувати інфраструктурної програми, нестача навичок - навчання й методичної підтримки, низька якість даних - призначення власників і стандартизації, а недовіра - прозорості комунікації та механізму виправлення помилок. Один універсальний захід не здатний одночасно усунути різні причини. Саме причинна прив'язка перетворює профіль готовності з описового документа на основу управлінського рішення.

Результати діагностики доцільно відображати у регіональній дорожній карті. Вона має містити послідовність кроків, залежності між проєктами, мінімальні умови запуску, джерела фінансування, відповідальних і показники. Наприклад, електронний сервіс не слід масштабувати до завершення очищення даних, узгодження регламенту й навчання працівників. Дорожня карта дозволяє уникнути паралельних ініціатив і спрямувати обмежені ресурси на ті компоненти, без яких подальша трансформація буде нестійкою.

Висновки. Цифрова готовність регіонального управління є багатовимірною спроможністю, що поєднує інфраструктуру, правові умови, інституції, кадри, фінанси, дані, зрілість послуг, безпеку, соціальну доступність та інноваційність. Технічне оснащення є необхідним, але недостатнім. Визначальним є здатність перетворити ресурси на законний, безпечний, доступний і стійкий управлінський результат.

Діагностика має бути територіально деталізованою та орієнтованою на виявлення критичних обмежень. Запропонована послідовність дозволяє перейти від загального переліку проблем до профілю готовності й адресного пакета заходів. Подальші дослідження доцільно спрямувати на формування набору вимірюваних індикаторів і перевірку їх придатності для порівняння різних типів регіонів України.

Список використаних джерел:

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо

її реалізації: розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. URL: <https://zakon.rada.gov.ua/go/67-2018-%D1%80>

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80>

3. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/go/2155-19>

4. World Bank. World Development Report 2016: Digital Dividends. Washington, DC: World Bank, 2016. URL: <https://www.worldbank.org/en/publication/wdr2016>

5. United Nations. E-Government Survey 2018: Gearing E-Government to Support Transformation towards Sustainable and Resilient Societies. New York: United Nations, 2018. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018>

References:

1. On Approval of the Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020 and the Action Plan for Its Implementation: Order of the Cabinet of Ministers of Ukraine of 17 January 2018 No. 67-r. URL: <https://zakon.rada.gov.ua/go/67-2018-%D1%80>

2. On Information Protection in Information and Telecommunication Systems: Law of Ukraine of 5 July 1994 No. 80/94-VR. URL: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80>

3. On Electronic Trust Services: Law of Ukraine of 5 October 2017 No. 2155-VIII. URL: <https://zakon.rada.gov.ua/go/2155-19>

4. World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. URL: <https://www.worldbank.org/en/publication/wdr2016>

5. United Nations. (2018). E-Government Survey 2018: Gearing E-Government to Support Transformation towards Sustainable and Resilient Societies. New York: United Nations. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018>