Т1. №1(33)’2023 https://doi.org/10.31474/2786-9024/v1i1(33).296433

Інформаційна безпека

КОНЦЕПТУАЛЬНІ ЗАСАДИ ГЛОБАЛЬНОЇ СТІЙКОСТІ СМАРТ-ДЕРЖАВИ

Я.Ю. Дорогий[1], І.О. Бердиченко[2]

[1] Department of Applied Mathematics and Informatics, Donetsk National Technical University, Lutsk, Ukraine
[2] Department of Criminal Law and Procedure, Kyiv University of Law of the National Academy of Sciences of Ukraine
E-mail: yaroslav.dorohyi@donntu.edu.ua

Отримано 31.12.2023
Прийнято до публікації 19.01.2024
Опубліковано 28.03.2024

АНОТАЦІЯ

Ця стаття присвячена розгляду концептуальних засад глобальної стійкості смарт-держави. Автори розглядають сучасний вимір розвитку України у контексті впровадження технологій та інновацій у всі сфери життя. Зокрема, стаття розглядає вплив інформаційних технологій, штучного інтелекту, та інших сучасних технологій на ефективність управління, соціально-економічний розвиток та екологічну сталість.

У статті детально розглядаються основні аспекти створення та функціонування смарт-держав, включаючи роль цифрових інфраструктур, відкритих даних, та електронного уряду. Автори аналізують принципи взаємодії смарт-держави з громадянами, підприємствами та іншими учасниками суспільства для досягнення високого рівня стійкості та розвитку.

Стаття також розглядає виклики та ризики, пов'язані з впровадженням сучасних технологій у державну систему, та пропонує стратегії забезпечення кібербезпеки та захисту приватності в умовах цифрового середовища. Особлива увага приділяється ідеям сталого розвитку та етичним аспектам використання технологій для досягнення глобальної стійкості смарт-держав, розумінню таких дефініцій як цифрова стійкість та глобальна стійкість, і відповідно, визначенню їх структури і закономірностей застосування.

***Ключові слова**: глобальна стійкість, смарт-держава, стійкість, цифрова інфраструктура, сталість, концептуальні засади*

ВСТУП

У сучасному світі стрімкого технологічного прогресу та глибоких змін у соціально-економічній сфері виникає необхідність перегляду та удосконалення парадигм управління державами. Однією з ключових концепцій, що визначає сучасний розвиток, є ідея створення смарт-держав, яка базується на впровадженні інформаційних технологій, штучного інтелекту та інновацій для досягнення вищого рівня ефективності, сталості та розвитку.

Концепція смарт-держави виникла в кінці 1990-х років і стала активно розвиватися в останні роки. Це пов'язано з рядом факторів, включаючи:

- швидкий розвиток технологій, таких як Інтернет, штучний інтелект та блокчейн;
- зростаюче значення сталого розвитку;
- зміна ролі держави в суспільстві.

ISSN 2786-9024

 https://doi.org/10.31474/2786-9024/v1i1(33).296433

Смарт-держава – це держава, яка використовує технології для підвищення ефективності управління, соціально-економічного розвитку та екологічної сталості. Вона характеризується такими основними рисами:

– цифрова інфраструктура, яка забезпечує доступ до інформації та послуг для громадян, підприємств та інших учасників суспільства;

– відкриті дані, які дозволяють використовувати інформацію для прийняття рішень та вирішення проблем;

– електронний уряд, який забезпечує доступ до державних послуг в онлайн-режимі.

Впровадження смарт-держави пов'язане з низкою викликів та ризиків, таких як:

– кібербезпека: загрози порушення конфіденційності та цілісності даних;

– захист приватності: загрози збору та використання персональних даних без згоди громадян;

– нерівність: загрози посилення нерівності в суспільстві через доступ до технологій.

Для забезпечення кібербезпеки та захисту приватності необхідно розробляти чіткі нормативні вимоги, інвестувати у розвиток кібербезпеки та захищати приватність громадян. Для вирішення проблеми нерівності необхідно забезпечити доступ до технологій для всіх громадян, незалежно від їхнього соціального статусу та фінансового становища. До того ж, подолання зазначених викликів вимагає дотримання принципу верховенства права і принципу людиноцентричності в діяльності суб’єктів владних повноважень.

Смарт-держави мають потенціал для створення більш стійких і справедливих суспільств. Технології можуть бути використані для вирішення таких глобальних проблем, як зміна клімату, бідність та голод.

АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

Розглянемо деякі літературні джерела та нормативно-правові акти України, які визначають основну термінологію та місце смарт-держави у розвитку України.

У дослідженні [1] розглядається роль цифрової трансформації у формуванні смарт-держави на прикладі європейського досвіду. Автори визначають, що цифрові технології сприяють перетворенню відносин між державою і громадянами, зокрема підвищенню ефективності управління та соціально-економічного розвитку, і відповідно, створенню успішної інноваційної держави. Вони стверджують, що цифрові трансформації є одним із ключових факторів успішної реалізації цього завдання.

Стаття [2] розглядає проблему кібербезпеки як важливого аспекту глобальної стійкості смарт-держави. Автори визначають, що кібербезпека – це стан захисту інформації та систем від несанкціонованого доступу, використання, розкриття, модифікації або знищення. Вони стверджують, що кібербезпека є ключовим фактором забезпечення ефективності управління, соціально-економічного розвитку та екологічної сталості смарт-держави.

В науковій праці [3] розглядаються етичні аспекти використання технологій у формуванні смарт-держави. Автори визначають, що етичні аспекти використання технологій - це сукупність моральних норм і принципів, які регулюють діяльність людей у сфері технологій. Вони стверджують, що етичні аспекти є важливим фактором забезпечення сталого розвитку смарт-держави.

У статті [4] надається огляд літератури з питань смарт-управління для сталого розвитку. Автори визначають, що смарт-управління - це використання технологій для підвищення ефективності управління та досягнення цілей сталого розвитку. Вони стверджують, що смарт-управління має потенціал для вирішення таких глобальних проблем, як зміна клімату, бідність та голод.

У статті [5] надається огляд літератури з питань смарт-управління для сталого розвитку міст. Автори визначають, що смарт-управління містами - це використання технологій для підвищення ефективності управління містами та досягнення цілей сталого розвитку. Вони стверджують, що смарт-управління містами має потенціал для вирішення таких проблем, як забруднення навколишнього середовища, транспортна інфраструктура та доступність житла.

1 серпня 2022 року European Commission оприлюднила результати Індексу цифрової економіки та суспільства за 2022 рік (Digital Economy and Society Index 2022 (DESI)). Індекс цифрової економіки та суспільства (DESI) – це зведений індекс, який узагальнює відповідні показники з ефективності цифрових технологій у Європі та відстежує еволюцію держав-членів ЄС в області цифрової конкурентоспроможності. Він зараз складається з таких компонентів [6]:

– людський капітал (human capital);

– зв’язок (connectivity);

– інтеграція цифрових технологій (integration of digital technology);

– цифрові державні послуги (digital public setvices).

Далі наведено огляд джерел, які є важливими документами, що визначають напрямок розвитку України в найближчі роки. Вони відображають прихильність

 https://doi.org/10.31474/2786-9024/v1i1(33).296433

українського уряду до інновацій, цифрової трансформації та сталого розвитку.

У контексті теми, що розглядається, ці джерела мають важливе значення. Вони демонструють, що Україна прагне стати сучасною державою, яка використовує технології для підвищення ефективності управління, соціально-економічного розвитку та екологічної сталості:

– програма діяльності Кабінету Міністрів України [7] передбачає підвищення ефективності державного управління, в тому числі за рахунок використання технологій;

– національна стратегія із створення безбар’єрного простору в Україні [8] сприятиме підвищенню доступності технологій для всіх громадян, незалежно від їхнього соціального статусу та фінансового становища;

– державна стратегія регіонального розвитку [9] передбачає використання технологій для розвитку регіонів України;

– стратегія реформування державного управління [10] передбачає підвищення прозорості та підзвітності державного управління, що можна досягти за рахунок використання технологій;

– план дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» [11] сприятиме відкритості та прозорості діяльності органів державної влади;

– розпорядження Кабінет Міністрів України від 17 лютого 2021 р. № 365-р «Деякі питання цифрової трансформації» [12] передбачає створення єдиної цифрової платформи для взаємодії органів державної влади, бізнесу та громадян;

– концепція розвитку системи електронних послуг в Україні [13] передбачає розширення доступу до державних послуг в онлайн-режимі;

– концепція розвитку штучного інтелекту в Україні [14] передбачає використання штучного інтелекту для вирішення таких проблем, як зміна клімату, бідність та голод;

– стратегія розвитку сфери інноваційної діяльності на період до 2030 року [15] передбачає створення сприятливого середовища для розвитку інновацій, включаючи технології;

– дорожня карта реформування ІТ-освіти [16] передбачає підготовку кваліфікованих кадрів для ІТ-індустрії;

– розпорядження КМУ від 12 травня 2021 р. № 438-р «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки» [17] передбачає створення сприятливого середовища для розвитку штучного інтелекту в Україні;

– стратегія кібербезпеки України [18] передбачає захист даних та інфраструктури від кіберзагроз;

– концепція забезпечення національної системи стійкості [19] передбачає використання технологій для підвищення стійкості України до зовнішніх загроз.

У цілому, наведені джерела демонструють, що Україна має амбітні плани щодо розвитку смарт-держави. Реалізація цих планів потребуватиме значних зусиль та ресурсів, але вона має потенціал для створення більш ефективної, справедливої та стійкої держави.

Отож приходимо до висновку, що цифрові трансформації, що охопили світ мають за мету посилення спроможностей щодо забезпечення цифрової та кібербезпеки держави, її цифрового простору, підтримки цифровими засобами та технологіями соціальної та політичної стабільності, оборони держави, захисту державного суверенітету та територіальної цілісності, конституційного ладу, забезпечення прав та свобод кожного громадянина.

Мета статті полягає в дослідженні та розкритті концептуальних засад глобальної стійкості смарт-держави. Ця стаття ставить за мету систематизацію та аналіз ключових аспектів створення та функціонування смарт-держав, зосереджуючись на їхньому впливі на ефективність управління, соціально-економічний розвиток, та екологічну сталість. Додатково, стаття пропонує вивчення викликів і ризиків, пов'язаних із застосуванням інформаційних технологій у державному управлінні, та розглядає стратегії забезпечення кібербезпеки та захисту приватності в умовах цифрового середовища. Крім того, стаття висвітлює ідеї сталого розвитку та етичні аспекти використання технологій для досягнення глобальної стійкості смарт-держав.

Результатом роботи є висновки та рекомендації щодо оптимального впровадження концепції смарт-держав у сучасному світі.

МАТЕРІАЛИ ТА МЕТОДИ ДОСЛІДЖЕНЬ

В роботі використано методи структурного і порівняльного аналізу, з інформаційним і аналітичним підходом розглянуто наукову та методичну літературу, а також онлайн ресурси.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Реалізація таких трансформацій потребує комплексного підходу, і отже на наш погляд, може бути реалізовано через розробку і впровадження в практичну площину Концепції глобальної стійкості Смарт-Держави (далі — Концепція), яка б визначила мету, основні принципи, напрями, механізми і строки запровадження

ISSN 2786-9024

Т1. №1(33)’2023 https://doi.org/10.31474/2786-9024/v1i1(33).296433

та функціонування системи глобальної стійкості, спрямованої на забезпечення здатності держави, бізнесу і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу, але не обмежуючись ними, постійно адаптуватися та трансформуватися шляхом впровадження цифрових технологій в усі процеси та на всіх рівнях діяльності держави та суспільства.

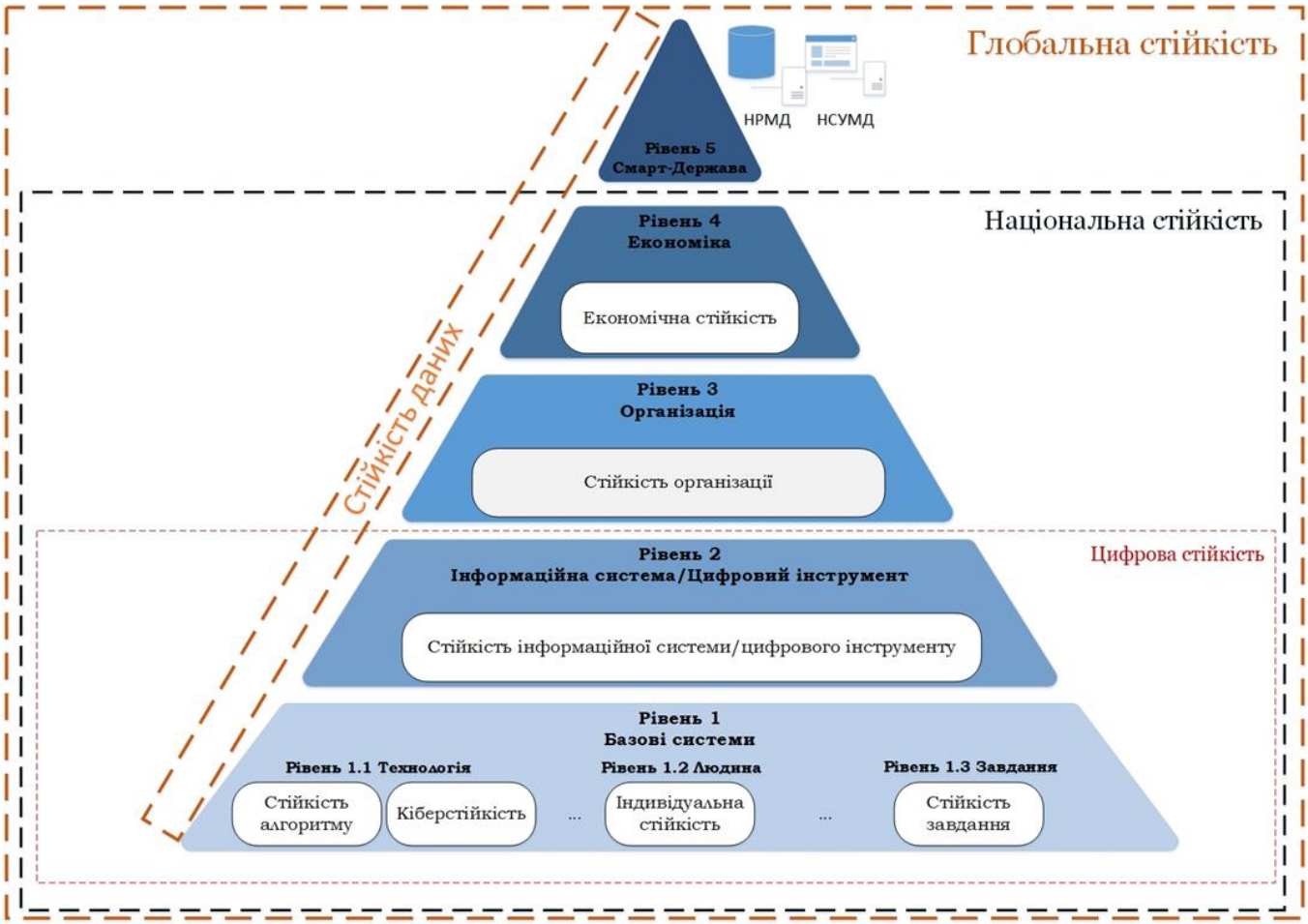

Рис. 1. Концепція глобальної стійкості

Концепція глобальної стійкості Смарт-Держави спрямована на забезпечення здатності держави, бізнесу і суспільства шляхом впровадження цифрових технологій та інструментів на всіх рівнях швидко відновлюватися до первинного стабільного стану або до іншого стабільного стану без втрат або з отриманням зиску і передбачає запровадження відповідних цифрових інструментів на рівні: держави (національна економіка), організації, інформаційної системи/цифрового інструменту та базових систем. Структура рівнів представлена на Рис. 1.

Рівень 1 та 2 передбачають впровадження цифрових інструментів та технологій для досягнення цифрової стійкості. Забезпечення стійкості базових систем рівня 1 напрямỳ впливає на стійкість інформаційних систем та цифрових інструментів рівня 2. Для прикладу, обізнаність людини щодо питань, пов’язаних з кібергігієною, безпосередньо впливає на стійкість її персонального кабінету в банківській установі; стек використовуваних технологій та заходи з кібербезпеки безумовно впливають на стійкість інформаційної системи, яка на них побудована, і таке інше.

Цифрову стійкість можна охарактеризувати за допомогою наступних чотирьох ключових компонентів: кібербезпеки, безперервності процесів, захисту персональних даних та цифрового громадянства.

1) Кібербезпека складається зі стандартів, практики та людських ресурсів, необхідних для підтримки функціонування цифрових систем та забезпечення стану захищеності цифрової екосистеми. Вона включає систему управління ризиками, яка дозволяє особам, що

 https://doi.org/10.31474/2786-9024/v1i1(33).296433

приймають рішення, розраховувати величину ризику, пов'язаного з цифровими системами, і регулярно підтримувати можливості, достатні для прогнозування та реагування на інциденти та надзвичайні ситуації на постійній основі.

2) Безперервність процесів передбачає планування та можливості для управління кризовими ситуаціями та відновлення, які практикуються для забезпечення того, щоб державні установи та бізнес-організації продовжували функціонувати навіть у несприятливих умовах. Безперервність залежить від наявності відповідних правил та стандартів, які дають бізнесу можливість для проведення фінансових операцій, забезпечуючи при цьому швидку адаптацію в рамках передбачуваного та загальноприйнятого набору правил та передової практики.

3) Захист персональних даних включає надійну екосистему даних, що складається з законів, установ і можливостей, які визначають і регулюють збір, зберігання та видалення даних. Функціонально це базується на визначенні прав доступу і використання, і тому, як дані, включаючи персональні дані, збираються і використовуються державою, підприємствами та іншими третіми сторонами. Приватність та захист даних важливі для запобігання збиткам, забезпечення цілісності державних та ділових операцій та захисту цифрового громадянства від потенційних зловживань, несправедливих рішень або помилок, а також для забезпечення економічної діяльності.

4) Цифрове громадянство означає готовність і здатність громадян безпечно користуватися перевагами цифрових систем та інфраструктури. Цифрове громадянство включає базову цифрову грамотність, практичне застосування цифрової гігієни та навичок, що забезпечують особисту безпеку в цифровому середовищі, а також поінформованість про цифрові права та обов'язки при використанні цифрових систем та даних.

Цілеспрямоване впровадження та використання вказаних компонентів цифрової стійкості на рівні організації шляхом впровадження «правильних» цифрових інструментів дозволяє досягти вже стійкості рівня організації (рівень 3). На цьому рівні також передбачається вжиття заходів, спрямованих на посилення відмовостійкості та запобігання загрозам технологічної залежності від іноземних виробників і постачальників продукції, технологій та послуг, що забезпечують функціонування цифрової екосистеми організації/підприємства/установи.

Стійке підприємство/організація/установа є фундаментальним елементом побудови стійкої економіки (рівень 4). На цьому рівні вживаються комплекси цілеспрямованих дій, методів та механізмів взаємодії «правильних» органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації. Фактично досягається стан національної стійкості.

Останній крок – трансформація стійкої держави у Смарт-Державу. Для забезпечення такого роду трансформації потрібно досягти стану стабільності даних, який передбачає впровадження на всіх рівнях та у всіх сферах діяльності держави національної системи управління майстер-даними (НСУМД) та національного репозиторію майстер-даних (НРМД).

Майстер-дані – вичерпний перелік сутностей організації/підприємства/установи та їх атрибутів, необхідний для надання інформації та цифрових послуг громадянам. Наприклад, до майстер даних можуть відноситися: реєстрова інформація, програмне забезпечення, класифікатори, стандарти, нормативна база тощо.

НСУМД являє собою сукупність процесів та інструментів для постійного визначення та централізованого управління основними даними держави (майстер-даними) та забезпечить:

– створення єдиного інформаційного простору;
– зв'язування інформації про одні і ті ж же майстер-дані з різних систем;
– збільшення ефективності бізнес-процесів та ділових процесів, пов'язаних з майстер-даними;
– зменшення часу обробки майстер-даних та мінімізацію державних витрат;
– оптимізацію зусиль щодо відповідності бізнесу регуляторним вимогам;
– швидке повернення інвестицій у розрізі роботи з майстер-даними;
– зниження загальної вартості володіння.

Впровадження НРМД дозволить державі постійно мати у використанні «правильне» представлення даних з інформаційних джерел завдяки:

– дослідженню даних – аналіз, профілювання та оцінка майстер-даних у інформаційних джерелах;
– стандартизації даних – приведення майстер-даних до єдиного формату;
– зіставленню даних – підрахунок схожості, виявлення дублів, кандидатів для злиття;
– видаленню дублікатів даних – створення "золотого" запису та збагачення;

ISSN 2786-9024

Т1. №1(33)’2023 https://doi.org/10.31474/2786-9024/v1i1(33).296433

– інтеграції даних – online/offline інтеграція з існуючими бізнес-застосунками, платформою «Дія» та іншими державними застосунками;

– безпеці даних – централізований контроль та безпека майстер-даних.

Інтеграція НСУМД та НРМД у повсякденну діяльність держави дозволить досягти стану глобальної стійкості – фінального стану цифрової трансформації держави, при якому досягається її здатність забезпечувати належний рівень надання послуг громадянам в будь-який момент часу та в будь-якій точці незалежно від типу, виду та масштабу загроз, які на неї впливають, а самій державі легко влитися у міжнародний інформаційний простір.

Побудована за таким принципом держава і є Смарт-Державою, яка характеризується станом глобальної стійкості і здатна виходити з будь-якої кризи з зиском для себе.

Проблема, яка потребує розв’язання, обмумовлена тим, що глобальні тенденції розвитку цифрової економіки в умовах мінливого ландшафту загроз вимагають переосмислення традиційних підходів до безпеки. Кібербезпека та захист інформації самі по собі не можуть забезпечити сталість цифрового розвитку. Вони стали частиною більш широкої концепції «цифрова стійкість», яка орієнтована на запобігання та адаптивність, та включає питання управління ризиками цифрового розвитку.

Ризик-інформований підхід, покладений в основу цифрової стійкості, забезпечує систематичне виявлення потенційних вразливостей інформаційних ресурсів, систем, мереж та загроз для них, імовірнісного оцінювання виникнення негативних подій, детерміністичного оцінювання потенційних негативних наслідків цих подій та розроблення рекомендацій щодо реалізації контрзаходів з метою мінімізації вразливостей, імовірностей виникнення негативних подій та їхніх наслідків.

Викладене дозволяє нам запропонувати наступне визначення цифрова стійкість - підхід, спрямований на забезпечення здатності держави, бізнесу і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу, але не обмежуючись ними, постійно адаптуватися та трансформуватися шляхом впровадження цифрових технологій в усі процеси та на всіх рівнях діяльності держави та суспільства.

Цифрова стійкість є елементом більш комплексного підходу «глобальної стійкості», який вимагає активної участі всіх зацікавлених сторін, включаючи державу, бізнес та громадянське суспільство.

Фактично, глобальна стійкість – це набір можливостей, методів та сприятливих умов, які забезпечують безперервність діяльності держави, бізнесу та суспільства в умовах постійних змін. Виникає необхідність концептуалізувати глобальну стійкість як набір стратегій, практик, можливостей та інструментів, які допомагають передбачати, запобігати та реагувати на неминучі економічні і геополітичні кризи, природні та техногенні катастрофи, і як результат - виходити з них з зиском для держави.

Запровадження на основі національних інтересів України та з урахуванням міжнародного досвіду багаторівневої комплексної системи глобальної стійкості сприятиме формуванню на державному, регіональному та місцевому рівнях необхідних спроможностей для запобігання та належного реагування держави, бізнесу і суспільства на широкий спектр загроз та швидкого відновлення після кризових ситуацій шляхом постійного адаптування та трансформування ділових та бізнес-процесів через впровадження нових цифрових технологій та інструментів в усі процеси діяльності та на всіх рівнях «Смарт-Держави».

Комплексне бачення мети, процедур, детальний перелік завдань та заходів, якісних і кількісних показників, очікуваних результатів реалізації завдань з розбудови цифрової стійкості на прикладі держави Україна, пропонуємо визначити через розроблення відповідної Концепції глобальної стійкості Смарт-держави. Метою реалізації Концепції є визначення основних принципів, напрямів, механізмів і строків запровадження та функціонування системи цифрової стійкості, спрямованої на забезпечення здатності держави, бізнесу і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу, але не обмежуючись ними, постійно адаптуватися та трансформуватися шляхом впровадження цифрових технологій в усі процеси та на всіх рівнях діяльності держави та суспільства.

Іншими словами, метою держави є створення сприятливого (у тому числі нормативно-правового) середовища та можливостей цифрового розвитку для всіх сторін (самої держави, бізнесу, громадянського суспільства) з повною інтеграцією у світовий простір.

Результатом має стати власне досягнення стану глобальної стійкості в усіх сферах життя, а сама держава має трансформуватися у «Смарт-Державу». Концепцію, що передбачає такі масштабні перетворення в державі, доцільно розробляти на період біля 10 років.

Реалізацію завдань з побудови цифрової стійкості будь якої державного утворення, на наш погляд, доцільно реалізувати через нижченаведені організаційні та практичні заходи, отже наведемо нашу позицію на прикладі побудови цифрової стійкості держави Україна.

Для досягнення вказаної мети на державному рівні необхідно:

– визначити принципи та політику цифрової стійкості та безпеки,

– здійснити аудит чинного законодавства та законодавчих бар’єрів, закласти основу створення комплексного нормативно-правового підходу до зазначеної сфери переглянути, і відповідно модернізувати законодавство, розробити відповідні національні стандарти;

– гармонізувати чинне законодавство відповідно до міжнародних стандартів

– розробити дорожню карту реалізації проекту «Цифрова стійкість України», орієнтовно на період від 3 до 5 років;

– розробити та впровадити дорожні карти розвитку цифрової стійкості для найбільш актуальних галузей економіки та сфер життєдіяльності (освіта, медицина, транспорт, енергетика тощо)

– впровадити алгоритм «Цифровий фільтр» у повсякденну діяльність, який передбачає обов’язкової процедури аналізу на наявність цифрових варіантів реалізації тих чи інших проектів при прийнятті будь-яких рішень, ініціатив національного, регіонального, галузевого рівнів та їх відповідності критеріям та показникам цифрової стійкості;

– створити та впровадити національну системи управління майстер-даними (НСУМД), національний репозиторій майстер-даних (НРМД) та національний резервний центр обробки даних (НРЦОД);

– наділити функціями формування політики центральний орган виконавчої влади, що відповідає за державну політику у сфері цифрових трансформацій, та який стане відповідальним за глобальну стійкість;

– забезпечити стійкість національних мереж та цифрових активів, у тому числі критичної інформаційної інфраструктури;

– розробити та впровадити нові програми підготовки та навчання фахівців, які працюють у критичних секторах економіки та державного управління;

– стимулювати державні програми щодо впровадження доступу до широкосмугового Інтернету по всій державі;

– створити, модернізувати та надати доступ до національних хмарних ресурсів для бізнесу;

– продовжити активне переведення державних послуг в онлайн формат (насамперед важливих для бізнесу – оподаткування, ліцензування та реєстрація тощо);

– підтримати цифрову освіту, забезпечити надійний доступ до централізованих онлайнових освітніх ресурсів для вчителів та учнів, забезпечити доступ до обладнання та відповідного програмного забезпечення, а також до високоякісного широкосмугового зв'язку;

– на системній основі проводити інформування та навчання (усіх) у галузі цифрової гігієни;

– діджіталізувати та розширити доступ до медичних послуг;

– розробити державні програми та прискорити доступ до цифрових транзакцій (фінансово-технічної, «пісочниці», електронна торгівля тощо).

Результатом реалізації Концепції повинна стати побудова сучасної та ефективної системи цифрової стійкості для забезпечення підтримки і подальшого цифрового розвитку ефективної та прозорої системи управління державою в цілому.

ВИСНОВКИ

Цифрова стійкість є ключовим фактором забезпечення безпеки та стабільності держави в умовах сучасного світу. Запропонована Концепція глобальної стійкості Смарт-Держави є всебічною та продуманою програмою, яка спрямована на підвищення рівня цифрової стійкості держави у всіх сферах її діяльності. Реалізація Концепції потребуватиме значних ресурсів та зусиль, але вона дозволить побудувати стійку та успішну державу в цифрову епоху.

ЛІТЕРАТУРА

[1] J.Dupont. The Smart State. Redesigning government in the era of intelligent services. London: Policy Exchange 8 – 10 Great George Street, 2018. 45 p. [Онлайн]. URL: http://surl.li/rlcqa. Дата звернення: 06.01.2024.

[2] І.В.Васильєва, О.Ю.Губенко, “Кібербезпека як складова глобальної стійкості смарт-держави”, *Наукові праці Національного університету «Львівська політехніка». Серія «Інформаційні технології та засоби обчислювальної техніки»*, 293, 121-132, 2022.

[3] Ю.О.Губенко, І.В.Васильєва, “Етичні аспекти використання технологій у формуванні смарт-держави”, *Наукові праці Національного університету «Львівська*

політехніка». Серія «Інформаційні технології та засоби обчислювальної техніки», 287, 123-134, 2021.

[4] A.Gupta, S.Sharma, "Smart governance for sustainable development: A review of the literature", *International Journal of Sustainable Development & World Ecology*, vol. 29, iss. 2, 173-182, 2022.

[5] Z.Pang, Y.Wang, Y.Zhang, "Smart city governance for sustainability: A review of the literature", *Sustainability*, vol. 14, iss. 15, 6970, 2022.

[6] Індекс цифрової економіки та суспільства: прогрес ЄС. [Онлайн]. URL: http://surl.li/rlcqv. Дата звернення: 06.01.2024.

[7] Програма діяльності Кабінету Міністрів України: Постанова Кабінету Міністрів України від 12.06.2020 р. № 471. [Онлайн]. URL: http://surl.li/rlcrp. Дата звернення: 06.01.2024.

[8] Національна стратегія із створення безбар'єрного простору в Україні на період до 2030 року: Розпорядження Кабінету Міністрів України від 14.04.2021 р. № 366-р. [Онлайн]. URL: http://surl.li/dhqql. Дата звернення: 06.01.2024.

[9] Державна стратегія регіонального розвитку на 2021-2027 роки : постанова від 05.08.2020 р. № 695. [Онлайн]. URL: http://surl.li/cczhd. Дата звернення: 06.01.2024.

[10] Стратегія реформування державного управління на 2022-2025 роки: Розпорядження Кабінету Міністрів України від 21.07.2021 р. № 831-р. [Онлайн]. URL: http://surl.li/rlcvv. Дата звернення: 06.01.2024.

[11] План дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2021-2022 роках: Розпорядження Кабінету Міністрів України від 21.02.2021 р. № 149-р. [Онлайн]. URL: http://surl.li/rlcwi. Дата звернення: 06.01.2024.

[12] Деякі питання цифрової трансформації: Розпорядження Кабінету Міністрів України від 17.02.2021 р. № 365-р. [Онлайн]. URL: http://surl.li/rlcxw. Дата звернення: 06.01.2024.

[13] Концепція розвитку системи електронних послуг в Україні: Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. [Онлайн]. URL: http://surl.li/rlcyv. Дата звернення: 06.01.2024.

[14] Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. [Онлайн]. URL: http://surl.li/qmhdv. Дата звернення: 06.01.2024.

[15] Стратегія розвитку сфери інноваційної діяльності на період до 2030 року: Розпорядження Кабінету Міністрів України від 10.07.2019 р. № 526-р. [Онлайн]. URL: http://surl.li/rldae. Дата звернення: 06.01.2024.

[16] Дорожня карта реформування ІТ-освіти: наказ Міністерства освіти і науки України, Міністерства цифрової трансформації України від 23 грудня 2021 р. № 1418/181.

[17] План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки: Розпорядження Кабінету Міністрів України від 21.05.2021 р. № 438-р. [Онлайн]. URL: http://surl.li/rlday. Дата звернення: 06.01.2024.

[18] Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 р. № 447/2021. [Онлайн]. URL: http://surl.li/bnpdr. Дата звернення: 06.01.2024.

[19] Концепція забезпечення національної системи стійкості: Указ Президента України від 27 вересня 2021 р. № 479/2021. [Онлайн]. URL: http://surl.li/kmjwd. Дата звернення: 06.01.2024.

CONCEPTUAL FOUNDATIONS OF GLOBAL RESILIENCE OF A SMART STATE

Iaroslav Dorohyi, Iryna Berdychenko

This article is dedicated to the examination of the conceptual foundations of the global resilience of a smart state. The authors explore the contemporary dimension of Ukraine's development in the context of the integration of technologies and innovations into all aspects of life. In particular, the article investigates the impact of information technologies, artificial intelligence, and other modern technologies on the efficiency of governance, socio-economic development, and ecological resilience.

The article provides a detailed analysis of key aspects of the creation and functioning of smart states, including the role of digital infrastructures, open data, and e-government. The authors analyze the principles of interaction between a smart state and citizens, businesses, and other members of society to achieve a high level of resilience and development.

The article also examines challenges and risks associated with the implementation of modern technologies in the state system and proposes strategies for ensuring cybersecurity and privacy protection in the digital environment. Special attention is given to the ideas of resilience development and ethical aspects of technology use to achieve global resilience of a smart state, understanding such definitions as digital resilience and global resilience, and accordingly, determining their structure and patterns of use

Keywords: *global resilience, smart state, resilience, digital infrastructure, sustainability, conceptual foundations*

REFERENCES

[1] J.Dupont. The Smart State. Redesigning government in the era of intelligent services. London: Policy Exchange 8 – 10 Great George Street, 2018. 45 p. [Online]. URL: http://surl.li/rlcqa. Accessed: 06.01.2024.

[2] I.V.Vasylieva, O.Iu.Hubenko, "Kiberbezpeka yak skladova hlobalnoi stiikosti smart-derzhavy", *Naukovi pratsi Natsionalnoho universytetu «Lvivska politekhnika». Seriia «Informatsiini tekhnolohii ta zasoby obchysliuvalnoi tekhniky»*, 293, 121-132, 2022.

[3] Yu.O.Hubenko, I.V.Vasylieva, "Etychni aspekty vykorystannia tekhnolohii u formuvanni smart-derzhavy", *Naukovi pratsi Natsionalnoho universytetu «Lvivska politekhnika». Seriia «Informatsiini tekhnolohii ta zasoby obchysliuvalnoi tekhniky»*, 287, 123-134, 2021.

[4] A.Gupta, S.Sharma, "Smart governance for sustainable development: A review of the literature", *International*

Journal of Sustainable Development & World Ecology, vol. 29, iss. 2, 173-182, 2022.

[5] Z.Pang, Y.Wang, Y.Zhang, “Smart city governance for sustainability: A review of the literature”, *Sustainability*, vol. 14, iss. 15, 6970, 2022.

[6] Indeks tsyfrovoi ekonomiky ta suspilstva: prohres YeS. [Online]. URL: http://surl.li/rlcqv. Accessed: 06.01.2024. (In Ukranian).

[7] Prohrama diialnosti Kabinetu Ministriv Ukrainy: Postanova Kabinetu Ministriv Ukrainy vid 12.06.2020 r. № 471. [Online]. URL: http://surl.li/rlcrp. Accessed: 06.01.2024. (In Ukranian).

[8] Natsionalna stratehiia iz stvorennia bezbariernoho prostoru v Ukraini na period do 2030 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 14.04.2021 p. № 366-p. [Online]. URL: http://surl.li/dhqql. Accessed: 06.01.2024. (In Ukranian).

[9] Derzhavna stratehiia rehionalnoho rozvytku na 2021-2027 roky : postanova vid 05.08.2020 r. № 695. [Online]. URL: http://surl.li/cczhd. Accessed: 06.01.2024. (In Ukranian).

[10] Stratehiia reformuvannia derzhavnoho upravlinnia na 2022-2025 roky: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 21.07.2021 r. № 831-p. [Online]. URL: http://surl.li/rlcvv. Accessed: 06.01.2024. (In Ukranian).

[11] Plan dii iz vprovadzhennia Initsiatyvy «Partnerstvo «Vidkrytyi Uriad» u 2021-2022 rokakh: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 21.02.2021 p. № 149-p. [Online]. URL: http://surl.li/rlcwi. Accessed: 06.01.2024. (In Ukranian).

[12] Deiaki pytannia tsyfrovoi transformatsii: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 17.02.2021 r. № 365-p. [Online]. URL: http://surl.li/rlcxw. Accessed: 06.01.2024. (In Ukranian).

[13] Kontseptsiia rozvytku systemy elektronnykh posluh v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 16.11.2016 r. № 918-p. [Online]. URL: http://surl.li/rlcyv. Accessed: 06.01.2024. (In Ukranian).

[14] Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 r. № 1556-p. [Online]. URL: http://surl.li/qmhdv. Accessed: 06.01.2024. (In Ukranian).

[15] Stratehiia rozvytku sfery innovatsiinoi diialnosti na period do 2030 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 10.07.2019 r. № 526-p. [Online]. URL: http://surl.li/rldae. Accessed: 06.01.2024. (In Ukranian).

[16] Dorozhnia karta reformuvannia IT-osvity: nakaz Ministerstva osvity i nauky Ukrainy, Ministerstva tsyfrovoi transformatsii Ukrainy vid 23 hrudnia 2021 r. № 1418/181.

[17] Plan zakhodiv z realizatsii Kontseptsii rozvytku shtuchnoho intelektu v Ukraini na 2021-2024 roky: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 21.05.2021 r. № 438-p. Accessed: 06.01.2024. [Online]. URL: http://surl.li/rlday. (In Ukranian).

[18] Stratehiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. Accessed: 06.01.2024. [Online]. URL: http://surl.li/bnpdr. (In Ukranian).

[19] Kontseptsiia zabezpechennia natsionalnoi systemy stiikosti: Ukaz Prezydenta Ukrainy vid 27 veresnia 2021 r. № 479/2021. [Online]. URL: http://surl.li/kmjwd. Accessed: 06.01.2024. (In Ukranian).

ISSN 2786-9024