УДК 004.738.5:330.322
DOI https://doi.org/10.32782/pdu.2024.4.75

Б. В. Богдан
кандидат юридичних наук, доцент,
професор кафедри публічного та міжнародного права
Київського національного економічного університету імені Вадима Гетьмана,

ВПЛИВ ЦИФРОВІЗАЦІЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ЕКОНОМІЧНУ СТІЙКІСТЬ ДЕРЖАВИ: ВИКЛИКИ ТА МОЖЛИВОСТІ

Визначено, що цифровізація критичної інфраструктури набуває ключового значення для забезпечення економічної стійкості держави в умовах глобальних викликів. Перехід від традиційних (аналогових) систем управління до інформаційно-комунікаційних технологій (ІКТ) дозволяє підвищити оперативність прийняття рішень, ефективність використання ресурсів та прогнозування ризиків. Поєднання інтернету речей (IoT), хмарних рішень, автоматизованих систем диспетчеризації та великих даних (Big Data) сприяє оптимізації енергоресурсів, зменшенню експлуатаційних витрат, скороченню простоїв у роботі енергетичних мереж, транспортних та комунальних систем. Надійний цифровий моніторинг дозволяє оперативно виявляти аварійні ситуації та запобігати масштабним збоям, що забезпечує стабільне функціонування ключових галузей економіки.

Проте процес цифровізації критичної інфраструктури супроводжується низкою викликів. По-перше, це вразливість до кіберзагроз: будь-яке підключення об'єктів до мережі Інтернет розширює поверхню атаки, а наявність застарілого обладнання ускладнює оновлення програмного забезпечення й впровадження сучасних протоколів шифрування. По-друге, високі початкові інвестиції та необхідність забезпечити належну кваліфікацію персоналу є суттєвими економічними бар'єрами для держави і приватних операторів. Крім того, стандартизація та сумісність різноманітних технологічних рішень часто перебувають на низькому рівні, що ускладнює інтеграцію компонентів із різних галузей та від різних виробників. Водночас відсутність єдиних нормативно-правових актів, які чітко регулювали б етапи цифрової трансформації, створює додаткові ризики для інвесторів і операторів.

Серед можливостей, що відкриває цифровізація, – підвищення інвестиційного клімату через прозорість і передбачуваність роботи об'єктів критичної інфраструктури, поліпшення якості послуг для населення (наприклад, інтегровані системи розумного міста), а також зростання експорту технологічних рішень у суміжні країни. Крім того, використання аналітики великих даних сприяє більш точному прогнозуванню попиту й пропозиції в енергетиці чи транспорті, що позитивно позначається на макроекономічних показниках, зокрема ВВП та бюджетних надходженнях. Комплексне втілення проєктів цифровізації за участю державних, приватних та міжнародних партнерів дає змогу сформувати стійкі моделі фінансування та мінімізувати ризики. У результаті державна економіка отримує неабиякі можливості для сталого розвитку, інноваційного зростання та підвищення конкурентоспроможності на світовому ринку.

Ключові слова: *держава, функції держави, адміністративно-правове регулювання, цифровізація, цифрові технології, державна політика, правове регулювання, кібербезпека, кіберпростір, критична інфраструктура.*

Постановка проблеми. Цифровізація критичної інфраструктури – інтеграція інформаційно-комунікаційних технологій (ІКТ), Інтернету речей (IoT) та автоматизованих систем управління в енергетичні мережі, транспорт, водопостачання й інші ключові галузі – стає невід'ємною складовою сучасного державного розвитку. Однак цей процес породжує одночасно як нові можливості (підвищення операційної ефективності, оптимізація ресурсой енергоспоживання, оперативне вияв-

лення й ліквідацію аварій), так і низку суттєвих викликів. Насамперед, використання застарілого обладнання та відсутність уніфікованих стандартів сумісності призводять до технологічних розривів при інтеграції нових компонентів, що збільшує ризики простоїв та неефективного розподілу інвестицій. Підключення об'єктів до відкритих мереж створює значну кіберризику: поширені вразливості SCADA/ICS, дефіцит кваліфікованих кадрів і обмеженість ресурсів не дозволяють гарантувати належний рівень інформаційного захисту. Водночас високі початкові витрати на модернізацію й навчання персоналу, невизначеність щодо окупності інвестицій та брак прозорості нормативно-правового середовища гальмують масштабне впровадження цифрових рішень. Таким чином, проблема полягає у розробці збалансованої стратегії цифровізації критичної інфраструктури, що враховує технічні, кібербезпекові та економічні аспекти у формуванні адекватних інструментів оцінки ризиків і ефективного розподілу інвестицій для забезпечення економічної стійкості та надійності держави.

Метою статті є розкриття впливу цифровізації критичної інфраструктури на економічну стійкість держави.

Стан дослідження. Окремі питання діджиталізації в сфері критичної інфраструктури були предметом дослідження як українських, так і зарубіжних вчених: А. П. Гаврись, В. В. Філіппова, Н. Ю. Тур здійснили комплексний аналіз сучасних загроз, зокрема воєнних, техногенних, природних та кібернетичних [10]; Брюс Шнейєр фокусується на глобальних аспектах збору, обробки та захисту персональних і промислових даних [2]; у статті Деніел Гір «Економіка кібербезпеки: виклики для критичної інфраструктури» розглядає, як економічні мотивації визначають рівень захищеності елементів критичної інфраструктури [5]; робота Рікардо Балдоні «Захист критичної інфраструктури в цифрову епоху» ґрунтується на детальному аналізі сучасного стану кіберзахисту інфраструктури у різних країнах Європи [6].

Виклад основного матеріалу. Цифровізація критичної інфраструктури вимагає інтеграції сучасних інформаційно-комунікаційних технологій із застарілими промисловими системами, що створює численні технічні виклики. По-перше, безперервний цикл роботи об'єктів (енергетики, транспорту, водопостачання) унеможливлює тривалі простої для оновлення "legacy" контролерів і впровадження патчів, а відсутність уніфікованих протоколів шифрування та автентифікації ускладнює централізований моніторинг і своєчасне виявлення кіберзагроз. По-друге, обмежені обчислювальні ресурси промислових ПЛК й SCADA-систем не завжди дозволяють використовувати сучасні агенти виявлення атак або машинне навчання для аналізу аномального трафіку, що підвищує залежність від ручного аудиту й збільшує ймовірність пропуску критичних інцидентів. По-третє, відсутність зональної сегментації між IT- та OT-мережами часто призводить до "розмивання" кордонів безпеки, коли компрометація однієї компоненти ланцюга може швидко поширюватися на інші елементи інфраструктури.

Поряд із технічними перешкодами цифровізація КІ ставить перед операторами суттєві економічні виклики. Високі початкові інвестиції (CAPEX) на модернізацію обладнання, впровадження IDS/IPS, SIEM-систем і квантово-стійке шифрування значно перевищують бюджети багатьох держпідприємств, у той час як точну окупність (ROI) важко спрогнозувати через невизначеність щодо масштабу потенційних кіберзбитків і тривалості перехідного періоду. До того ж нестабільність курсу валют і зростання цін на імпортні рішення підвищують собівартість проєктів, а брак кваліфікованих фахівців із кібербезпеки змушує виділяти великі кошти на навчання та залучення зовнішніх консультантів. Додатково конкуренція між різними напрямами інвестицій (оновлення виробничих активів, капітальний ремонт, соціальні проєкти) створює ризик недофінансування кіберзахисних заходів, що може підірвати загальну економічну стійкість держави в разі масштабних інцидентів.

Серед технічних викликів забезпечення кібербезпеки критичної інфраструктури в умовах діджиталізації особливо можна виділити такі, як:

1) інтеграція старих і нових систем. Багато об'єктів критичної інфраструктури працюють на застарілих ПЛК (програмованих логічних контролерах) та мережевому обладнанні, які не підтримують сучасних криптографічних методів аутентифікації і шифрування. Поєднання таких «legacy» систем із новими хмарними або edge-рішеннями створює розрив у безпеці, адже оновити програмне забезпечення старих контролерів часто неможливо без повної заміни обладнання [1];

2) відсутність єдиних стандартів і протоколів. Різні виробники пристроїв можуть використовувати унікальні чи незахищені протоколи зв'язку (Modbus, DNP3, OPC UA без захисту). Наявність кастомізованих реалізацій ускладнює уніфіковане застосування інструментів моніторингу й виявлення аномалій, а також реалізацію корпоративних політик безпеки;

3) ріст складності атак. Сучасні загрози – від «зрошення» мережі (watering hole) до атак типу Advanced Persistent Threat (APT) – потребують інтегрованого підходу: поєднання IDS/IPS (систем виявлення та запобігання вторгнень), SIEM (систем збору й аналізу подій), EDR (endpoint detection and response), а також регулярного проведення пентестів і аудиту конфігурацій. Брак власних фахівців із досвідом роботи у промислових мережах підсилює ризики, бо типові IT-рішення не завжди адаптовані для OT-сегменту [3; 4];

4) потреба в постійному оновленні та моніторингу. Кожне оновлення програмного забезпечення чи прошивки пристроїв може створити нові уразливості. Системи SCADA та HMI (human-machine interface) потребують 24/7 моніторингу мережевого трафіку й швидкого реагування на аномальну поведінку, що вимагає розгортання спеціалізованих SOC (security operations center) або віддалених MSSP (managed security service provider) із глибоким розумінням як IT-, так і OT-середовища.

Отже, технічні виклики забезпечення кібербезпеки критичної інфраструктури в умовах діджиталізації - це сукупність проблем і обмежень, пов'язаних із інтеграцією застарілих промислових систем (OT) із новими інформаційно-комунікаційними технологіями (IT), які ускладнюють реалізацію ефективного захисту. До них належать: необхідність сумісності «legacy» контролерів із сучасними протоколами шифрування; відсутність стандартизованих інтерфейсів для централізованого моніторингу інцидентів; обмежені апаратні ресурси промислових пристроїв для впровадження агентів безпеки; складність патч-менеджменту та оновлення прошивок без зупинки виробничих процесів; висока уразливість мережевих з'єднань через використання незахищених протоколів; а також потреба у безперервному (24/7) моніторингу й оперативному реагуванні на загрози в реальному часі.

Серед економічних викликів ключовими, на нашу думку, є:

1) високі початкові інвестиції. Закупівля захищеного обладнання (виробничі ПЛК із вбудованими засобами аутентифікації), ліцензійних рішень для шифрування, оборудка з IDS/IPS та SIEM-системами, облаштування сегментованих DMZ-зон для критичних вузлів потребують значних капітальних витрат. Для держави або приватного оператора це часто означає перегляд бюджету та пріоритетів: вкладення у кібербезпеку може на перший погляд видаватися менш пріоритетним, ніж, скажімо, будівництво нових ліній електропередач або прокачка газу [7-9];

2) окупність інвестицій (ROI). На відміну від прямих капіталовкладень у виробництво чи будівництво, вигода від інвестицій у кібербезпеку частково невидима: запобігти нападу легше, ніж відновлювати втрачені об'єкти й репутацію. Потрібно розрахувати економічні втрати від припинення роботи критичної інфраструктури (вартість простоїв, штрафи, компенсації споживачам, зниження довіри партнерів) й порівняти їх із витратами на сучасний SOC, навчання персоналу та оновлення обладнання;

3) підготовка кадрів. Запровадження «закритих» сезонних програм перекваліфікації та підтримка сертифікацій (наприклад, CISSP, CISM, SANS-курси для інженерів OT) вимагають системних вкладень у розвиток людського капіталу. Водночас ринок праці стимулює «відтік» досвідчених аналітиків безпеки до міжнародних проєктів чи банківського сектора із вищою

оплатою, що призводить до нестачі кваліфікованих фахівців у держпідприємствах критичного призначення;

4) моделювання загроз і збитків. Щоб доцільно інвестувати в кіберзахист, необхідно розробити економічно обґрунтовану модель оцінки ризиків (технічна й фінансова ймовірність інциденту), а також методику обчислення очікуваних збитків. Наприклад, орієнтуватись на стандарт NIST SP 800-30 (Risk Management Guide for Information Technology Systems), але адаптувати його до локального регуляторного середовища та галузевих специфік. Це потребує бюджетної статті на проведення аудитів, пентестів, моделювання атак із залученням зовнішніх експертів і страхування кіберризиків;

5) використання економічних методів захисту. На об'єктовому рівні: оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об'єктах критичної інфраструктури [11].

Отже, економічні виклики забезпечення кібербезпеки критичної інфраструктури в умовах діджиталізації - це комплекс проблем, пов'язаних із доцільним розподілом обмежених фінансових і людських ресурсів для впровадження та підтримки захисних заходів у цифрових системах. Вони включають високі початкові інвестиції (CAPEX) у закупівлю сертифікованого обладнання, ліцензійного програмного забезпечення та створення SOC із цілодобовим моніторингом; значні операційні витрати (OPEX) на оновлення й обслуговування засобів безпеки, патч-менеджмент і навчання персоналу; невизначеність розрахунку окупності (ROI), бо вигоди від запобігання кібератакам є складно кількісно виражати; а також конкуренцію таких витрат з іншими пріоритетами бюджетування (модернізація виробництва, оновлення обладнання). Додаткові виклики – нестача кваліфікованих фахівців із високими зарплатними очікуваннями, коливання валютного курсу й інфляції, що підвищує вартість імпортних рішень, а також необхідність створення систем страхування кіберризиків за адекватними ставками, яка здешевила б інвестиційні проєкти – усе це ускладнює обґрунтування й планування кошторисів для сталого захисту критичної інфраструктури.

Можемо констатувати, що цифровізація критичної інфраструктури стикається з низкою технічних викликів, пов'язаних із інтеграцією нових IT-рішень у застарілі OT-системи. Багато об'єктів КІ використовують «legacy» контролери та мережеве обладнання, які не підтримують сучасних алгоритмів шифрування й аутентифікації. Через це оновлення прошивок чи встановлення патчів найчастіше потребує зупинки виробничих процесів, що неприпустимо для енергетики, транспорту або водопостачання. Відсутність єдиних стандартів і сегментації мережі призводить до «розмивання» зон безпеки: компрометація одного вузла може швидко поширюватися на інші елементи системи. До того ж обмежена обчислювальна потужність промислових ПЛК та SCADA-систем ускладнює впровадження агентів виявлення вторгнень та алгоритмів машинного навчання для аналізу аномального трафіку, що підвищує ризик пропуску критичних інцидентів.

Наявні економічні виклики цифровізації критичної інфраструктури теж є суттєвими. По-перше, високі початкові інвестиції (CAPEX) на закупівлю захищеного обладнання, впровадження SIEM-/IDS/IPS-систем, створення SOC та модернізації мережі часто перевищують доступні бюджети державних і приватних операторів. По-друге, розрахунок окупності (ROI) цих інвестицій ускладнений невизначеністю щодо масштабу потенційних кіберзбитків: неможливо точно спрогнозувати ймовірність та наслідки масштабної атаки, що змушує ухвалювати рішення в умовах високого ризику. По-третє, нестабільність курсу валют і зростання цін на імпортне обладнання додатково підвищують вартість проєктів цифровізації, а дефіцит кваліфікованих фахівців із кібербезпеки зму-

шує витрачати значні кошти на навчання персоналу та залучення консультантів.

Водночас цифровізація створює величезні можливості для підвищення економічної стійкості держави. По-перше, впровадження інструментів реального часу (IoT, Big Data, хмарні платформи) дозволяє оптимізувати споживання ресурсів, скоротити експлуатаційні витрати та зменшити кількість аварій. Завдяки прогнозному моніторингу можна оперативно виявляти потенційні неполадки в енергетичних мережах або транспортних системах, що знижує ризик масштабних перебоїв і підтримує стабільність національної економіки. По-друге, цифрові рішення сприяють підвищенню прозорості процесів і є основою для впровадження механізмів діджитал-урядування, що покращує управління державними ресурсами й підвищує довіру інвесторів.

Крім того, цифровізація критичної інфраструктури стимулює диверсифікацію економічної діяльності й розвиток нових сервісів. Завдяки впровадженню «розумних» лічильників, інтегрованих платформ розподілу енергії та автоматизованих диспетчерських з'являються можливості для створення інноваційних продуктів: платформи для динамічного ціноутворення, електронних ринків енергії, дистанційного керування інфраструктурою. Це сприяє зростанню інвестиційної привабливості сектору, залученню приватного капіталу та розвитку стартап-екосистеми. Крім того, підвищення кіберстійкості підсилює стійкість економіки до зовнішніх шоків, формує більш конкурентоспроможні галузі й зміцнює загальну безпеку держави у цифровому середовищі.

Список використаних джерел:

1. Ross, Anderson. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems). John Wiley and Sons Ltd. 450 p.
2. Schneier, Bruce. (2016). The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 448 p.
3. NIST. (2015). *Довідник NIST SP 800-82 Rev. 2: Захист систем промислового керування (ICS)* (Guide to Industrial Control Systems (ICS) Security, SP 800-82 Rev. 2). National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
4. ENISA. (2018). *Ландшафт загроз для кіберфізичних і SCADA-систем (Threat Landscape for CPS/SCADA)*. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-cyber-physical-systems-and-scada
5. Geer, D. (2013). *Економіка кібербезпеки: виклики для критичної інфраструктури* (The Economics of Cybersecurity: Challenges for Critical Infrastructure). IEEE Security & Privacy, 11(3), P. 10–17.
6. Baldoni, P. (2017). Critical Infrastructure Protection in the Digital Age. Springer. 250 p.
7. Jones, A. (2019). Economic Aspects of Securing the Smart Grid. Energy Policy. P. 1021–1030.
8. Kharchenko, B. (2021). Economic Challenges of Cybersecurity for Ukraine's Critical Infrastructure. *Кібернетика і Безпека*. № 2. С. 45–52.
9. Golod, C., & Petrenko, O. (2020). Risk Assessment Models for Cybersecurity in Power Supply. *Енергетика та інформаційні технології*. №8 (1). С. 33–41.
10. Гаврись А. П., Філіппова В. В., Тур Н. Ю. (2024). Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану. *Вісник ЛДУБЖД*. № 30. С. 173-187.
11. Bohdan, B., Kuzmenko, O., & Chorna, V. (2023). Economic measures for managing critical infrastructure facilities in Ukraine. *Baltic Journal of Economic Studies*, 9 (3), P. 22-32. https://doi.org/10.30525/2256-0742/2023-9-3-22-32

Bohdan B. V. The impact of digitalization of critical infrastructure on the economic sustainability of the state: challenges and opportunities

It has been determined that the digitalization of critical infrastructure is becoming key to ensuring the economic sustainability of the state in the face of global challenges. The transition from traditional (analog) management systems to information and communication technologies (ICT) allows for increased decision-making efficiency, resource efficiency, and risk forecasting. The combination of the Internet of Things (IoT), cloud solutions, automated

dispatching systems, and big data (Big Data) contributes to the optimization of energy resources, reduction of operating costs, and reduction of downtime in the operation of energy networks, transport, and utility systems. Reliable digital monitoring allows for the prompt detection of emergencies and the prevention of large-scale failures, which ensures the stable functioning of key sectors of the economy.

However, the process of digitalization of critical infrastructure is accompanied by a number of challenges. Firstly, it is vulnerability to cyber threats: any connection of objects to the Internet expands the attack surface, and the presence of outdated equipment makes it difficult to update software and implement modern encryption protocols. Secondly, high initial investments and the need to ensure proper personnel qualifications are significant economic barriers for the state and private operators. In addition, standardization and compatibility of various technological solutions are often at a low level, which complicates the integration of components from different industries and from different manufacturers. At the same time, the lack of unified regulatory and legal acts that would clearly regulate the stages of digital transformation creates additional risks for investors and operators. Among the opportunities opened up by digitalization are an increase in the investment climate through transparency and predictability of the operation of critical infrastructure facilities, improved quality of services for the population (for example, integrated smart city systems), as well as increased exports of technological solutions to neighboring countries. In addition, the use of big data analytics contributes to more accurate forecasting of supply and demand in energy or transport, which has a positive impact on macroeconomic indicators, in particular GDP and budget revenues. The comprehensive implementation of digitalization projects with the participation of public, private and international partners allows for the formation of sustainable financing models and minimize risks. As a result, the state economy receives significant opportunities for sustainable development, innovative growth and increased competitiveness in the global market.

Key words: *state, state functions, administrative and legal regulation, digitalization, digital technologies, state policy, legal regulation, cybersecurity, cyberspace, critical infrastructure.*