ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA

DOI (Issue): https://doi.org/10.36486/np.2024.1(63) **Issue 1(63) 2024**

КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ. КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 004.056

Демедюк Сергій Васильович,
кандидат юридичних наук,
заступник Секретаря Ради національної безпеки і
оборони України, м. Київ, Україна,
ORCID ID 0009-0008-1359-5265

РЕАЛІЗАЦІЯ СПРОМОЖНОСТІ СУБ'ЄКТІВ СИСТЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Статтю присвячено аналізу проблемних питань щодо розбудови кіберстійкості як здатності протистояти кіберзагрозам, відновлюватися та адаптуватися до них. Незважаючи на національну та міжнародну важливість, показники стійкості для прийняття управлінських рішень все ще перебувають на ранніх стадіях розвитку. Зазначено, що показники стійкості повинні пов'язувати цілі національної політики з конкретними системними заходами таким чином, що рішення про розподіл ресурсів можуть бути переведені в конкретні заходи та інвестиції.

Запропоновано загальний підхід на основі формування матриці кіберстійкості, яка інтегрує фактичні дані, технічний стан та інші показники для оцінки стійкості системи у фізичній, інформаційній, когнітивній і соціальній сферах.

Ключові слова: *стійкість, кібербезпека, кіберстійкість, показники, кіберризик, оцінка ризиків.*

Зростаюча залежність громадян, бізнесу та суспільства від кіберінфраструктури поставила національну безпеку під значний ризик непередбачуваних і невідомих загроз. Високий рівень взаємозв'язку в сучасному суспільстві відкрив багато шляхів для кібератак, у тому числі внутрішні та зовнішні загрози і вразливості в мережах ланцюгів постачання [1]. Як наслідок, маломасштабні шкідливі програми, доступні на чорному ринку, завдають шкоди, неспівмірної з їхньою вартістю та складністю. Більше того, швидке розгортання провідних технологій для розподілу критично важливих послуг (наприклад, електроенергії) свідчить про те, що в майбутньому атаки на інфраструктуру можуть мати руйнівні наслідки для громадянського суспільства [2]. Незважаючи на постійний прогрес в управлінні ризиками в кіберпросторі, очевидно, що передбачення і запобігання всім можливим атакам і збоям у роботі неможливе для нинішніх або майбутніх інфраструктурних кіберсистем. За визначенням (Merriam-Webster) [3], стійкість – це здатність відновлюватися після нещастя або легко пристосовуватися до змін. У системах, що надають критично важливі послуги, стійкість характеризується чотирма можливостями: планувати/готуватися, поглинати,

DOI (Article): https://doi.org/10.36486/np.2024.1(63).13
Issue 1(63) 2024 **https://naukaipravoohorona.com/**

відновлюватися та адаптуватися до відомих і невідомих загроз [4; 5]. Впровадження комплексного плану забезпечення стійкості кіберінфраструктури систем має на меті зменшити потенційні збитки та сприяти швидкому відновленню після атаки. Однак, сучасні концепції та методи, що обговорюються як способи підвищення стійкості, часто об'єднують стійкість (тобто здатність протистояти і швидко відновлюватися після невідомих і відомих загроз) і ризик (тобто добуток ймовірності настання несприятливої події та величини спричиненої нею шкоди [6]). Зокрема, регуляторні органи закликають до розробки та впровадження стандартів, заснованих на оцінці ризиків, для захисту критичної інфраструктури від кіберзагроз, проте підходи, що базуються на оцінці ризиків, не обов'язково створюють стійкість [7]. Натомість стійкі системи повинні використовувати узагальнюючі концепції, що відрізняються від оцінки ризиків, але доповнюють її, для інформування і підтримки співпраці між різними федеральними відомствами, відповідальними за критично важливі об'єкти інфраструктури. До того ж додаткова плутанина виникає через змішування надійності і стійкості, пов'язаних між собою але різних властивостей систем. Надійність означає ступінь, до якого система здатна протистояти неочікуваним внутрішнім чи зовнішнім подіям або змінам без погіршення продуктивності системи [8]. Стійкість, з іншого боку, належить до здатності системи відновлювати або регенерувати свою продуктивність після неочікуваного впливу, що призводить до погіршення її роботи. З цієї причини необхідно вжити заходів для використання більш узагальнених концепцій стійкості та їх інтеграції з підходами до управління, що базуються на ризик-орієнтованому підході.

До того ж обговорення стійкості, що зустрічаються в літературі, часто зосереджені на одній операційній області (наприклад, фізичній, інформаційній, когнітивній або соціальній) і не відображають взаємозв'язки між компонентами системи для інформування в цих сферах. В інженерній літературі методи оцінки стійкості часто зосереджуються на мережах, що складаються з однорідних елементів (наприклад, мережа комунікаційних пристроїв або мережі соціальних істот). Реальні мережі складаються з технологічних, соціологічних, екологічних та економічних компонентів таким чином, що комбінація взаємопов'язаних фізичних елементів, пристроїв зв'язку, людей і сил навколишнього середовища утворюють єдине ціле [9]. Стійкість є властивістю всієї системи і має оцінюватися відповідно. Наприклад, у разі атаки система може повідомити про стан і дії окремих комп'ютерів і серверів (фізичний домен). Інформація повинна ефективно та оперативно передаватися відповідним особам, які приймають рішення, що використовують цю інформацію для оцінки шкоди і визначення відповідної реакції на атаку (когнітивна сфера). Визначивши осіб, які приймають рішення, і делегуючи системні ресурси конкретним особам, можна чітко визначити, хто повинен діяти на основі інформації, що надходить із фізичного домену. Стійкість системи значною мірою залежить від ефективності міждоменної комунікації та координації на кожному етапі циклу управління.

Метою цієї статті є дослідження проблематики показників, які можуть інформувати про ступінь стійкості кіберсистем, а також підходів щодо їх розроблення та застосування.

Для планування та оперативних рішень показники кіберстійкості мають важливе значення і забезпечують засоби для визначення пріоритетності потреб, моніторингу прогресу і розподілу ресурсів [4]. Проте спроби експертів зібрати показники кіберстійкості не дають такої інформації. Наприклад, огляд, проведений Науковою радою з питань оборони (Defense Science Board – DSB) [2], не знайшов у літературі жодних показників, які були б корисними оборонним системам для управління кіберризиками. Крім того, показники, розроблені DSB [2], були визначені як неповні, оскільки вони ігнорують процеси управління стійкістю [10]. Незадовільний стан розуміння та визначення показників стійкості не викликає здивування, особливо у сфері кібербезпеки. Дійсно, навіть показники кіберризику є недостатньо зрозумілими і прийнятими, хоча ризик, можливо, є більш вивченим поняттям, ніж стійкість. Наявні на сьогодні алгоритми оцінки кіберризиків покладаються здебільшого на простих евристиках, таких як суми вразливостей у балах або кількість таких речей, як відсутні патчі, відкриті порти тощо. Такі показники широко розглядаються як слабкі та потенційно оманливі [11; 12]. Наприклад, індивідуальні оцінки вразливостей, як правило, є суб'єктивними та потенційно неточними; прості суми не враховують, як вразливості розподілені між хостами або у часі; вони також не враховують топологію мережі, роль і динаміку міжхостової взаємодії, ні нелінійну взаємодію між вразливостями, ні наміри зловмисника та потенційно неточну інформацію, ні наявність чи відсутність відповідних механізмів мережевого захисту, ні те, як компроміс може вплинути на місію організації [13]. Загалом, сувора теорія або моделі того, як різні фактори можуть поєднуватися в кількісну характеристику справжніх кіберризиків, бракує так само, як і суворої емпіричної перевірки показників кіберризиків. Подібні, а можливо, й більші недоліки та обмеження впливають на показники кіберстійкості. Запропонований у літературі підхід на основі матриці стійкості інтегрує чотири системні здібності планувати/готуватися, поглинати, відновлюватися і адаптуватися до відомих і невідомих загроз [4] з чотирма операційними доменами (фізичний, інформаційний, когнітивний та соціальний), що пропонує ефективний метод для класифікації показників стійкості.

Нещодавні досягнення у сфері стійкості визначили кілька важливих атрибутів ефективних показників для кіберсистем, призначених для оборони та критичної інфраструктури. У звіті 2013 року про «Стійкі військові системи і сучасні кіберзагрози» (Resilient Military Systems and the Advanced Cyber Threat) Наукової Ради з питань оборони (DSB) [2] рекомендується, щоб показники були:

- *достатньо широкими*, щоб їх можна було використовувати в різноманітному діапазоні систем;

- *достатньо точними* для вимірювання конкретних системних процесів і компонентів.

Важливо зазначити, що DSB слова «показники» і «вимірники» визначаються по-різному. Вимірник – це кількісний або якісний засіб фіксації атрибуту певної системи або компонента системи [14]. Показник – це засіб для порівняння якості двох або більше систем чи компонентів системи через застосування вимірника [14]. Наприклад, продуктивність системи в умовах кіберзбою буде показником, де швидкість передачі

даних через неї буде вимірником, пов'язаним із цим показником. Лінков та інші [10] стверджують, що поєднання доктрини мережецентричної війни (Network-Centric Warfare – NCW) [15] і визначення Національної академії наук [4] стійкості до катастроф може бути використане для розробки показників, які відповідають цим критеріям. Національна Академія наук (National Academy of Sciences – NAS) визначає чотири етапи циклу управління подіями, які система повинна підтримувати для того, щоб бути стійкою:

- *планування/підготовка:* закладення основи для забезпечення доступності послуг та функціонування активів під час руйнівної події (несправності або атаки);
- *поглинання:* підтримка найбільш важливих функцій активів та доступність послуг під час відбиття або ізоляції збоїв у роботі;
- *відновлення:* відновлення всіх функцій активів та доступність сервісів та їх функціональність як до події;
- *адаптація:* використовуючи знання, отримані під час події, зміна протоколу, конфігурації системи, навчання персоналу або інші аспекти для досягнення більшої стійкості.

Доктрина мережецентричної війни (NCW) визначає чотири сфери, які створюють загальну обізнаність про ситуацію і забезпечують децентралізоване прийняття рішень, а саме:

- *фізична:* фізичні ресурси, можливості і структура цих ресурсів;
- *інформаційна:* інформація та розвиток інформації про фізичну сферу;
- *когнітивна:* використання інформаційного та фізичного доменів для ухвалення рішень;
- *соціальна:* організаційна структура та комунікація для ухвалення когнітивних рішень.

Лінков та інші [10; 16] об'єднали визначення чотирьох функцій системи NAS і чотирьох доменів NCW, щоб створити загальну матрицю показників стійкості та адаптувати до кіберсистем (табл. 1). Ними запозичено багато показників із літератури [17; 18]. Показники доповнюються оцінкою їхніх наслідків на різних етапах і в різних сферах, так що відомі показники на одному з етапів циклу управління подіями або в межах однієї операційної сфери мають прямий вплив на показники в інших сферах.

Окремі сегменти матриці містять показники, які вимірюють здатність системи управляти несприятливими подіями та представляють конкретні показники для оцінки стійкості кіберсистеми. При інтерпретації матриці кожен сегмент відповідає на питання: «Як реалізується спроможність (планувати/готуватися, поглинати, відновлюватися, адаптуватися) системи до кіберподії у (фізичній, інформаційній, когнітивній, соціальній) сфері?». При цьому сегменти в колонках (поглинати, відновлюватися, адаптуватися) відображають спроможності, які система має продемонструвати, щоб бути стійкою до збоїв, тоді як колонка (планувати/готуватися) зосереджується на розумінні та документуванні структури та функцій системи.

Таблиця 1

Матриця кіберстійкості [10]

	планувати/готуватися	поглинати	відновлюватися	адаптуватися
фізична				
інформаційна				
когнітивна				
соціальна				

Показники, розроблені на основі матриці стійкості, не обов'язково можуть бути виміряні прямими методами, їх слід генерувати за допомогою спеціальних заходів, розроблених для кожної системи окремо. Це можуть бути як кількісні дані, так і якісні показники, які потім оцінюються технічними експертами та зацікавленими сторонами, пов'язаними з конкретною системою. Наприклад, показники, визначені для здатності кіберсистеми поглинати збої в інформаційній сфері, включають у себе здатність передавати дані відповідальним зацікавленим сторонам і особам, що приймають рішення. Цей показник може бути найкраще представлений комбінацією кількісних даних і якісних вимірників, таких як кількість зацікавлених сторін, типи залучених стейкхолдерів, ієрархія управління, кількість резервів у системах передачі інформації та частота обміну інформацією.

Зростаюча складність кіберсистем та кіберзагроз вимагає інтеграції процесів управління ризиками та процесу управління стійкістю. Часто загроза не розпізнається доти, доки вона не проявиться у кіберсистемі, а отже, може бути пропущена в сценаріях загроз, які розглядаються у межах оцінки ризиків. Кіберстійкість, гнучка за своєю природою, може забезпечити основу для боротьби з кіберзагрозами і життєздатність критично важливих кіберактивів і послуг. Управління стійкою кіберсистемою з використанням цієї концепції визнає і підкреслює взаємодію між кожним доменом організації на кожному етапі управлінського циклу – фактор, який не враховується в інших підходах до забезпечення стійкості.

Стійкість кіберсистеми залежить від ефективного функціонування всіх аспектів організації протягом усього циклу управління подіями в чотирьох визначених сферах. Ключовою перевагою використання матриці стійкості і є прозорий зв'язок між сферами впродовж усього циклу управління заходами. Як результат, системне застосування визначення NAS об'єднує всі компоненти організації в гетерогенну систему кіберінфраструктури, бізнес-функцій та зовнішніх суб'єктів. Однак аналіз цієї системи сам по собі не дає інформації про те, як стійкість виникає з системних взаємодій. Натомість організація та вимірювання цих компонентів як підсистем дозволяє визначити, як ці різнорідні компоненти взаємодіють, щоб стати стійкими.

Протягом усього процесу заповнення матриці взаємозалежність показників, етапів і доменів є критично важливою. Додаючи показник, слід враховувати, як він впливає на інші в матриці. Матриця стійкості не є вичерпним посібником, але натомість може бути використана для визначення та прив'язки системних заходів до проєктування та

експлуатації складних систем. По-перше, розроблені показники можна узагальнити для багатьох систем, таким чином, їх можна використовувати для порівняльної оцінки стійкості системи. Крім того, постійний моніторинг і звітність можуть інформувати керівництво про зміни, що вносяться як особами, що приймають рішення, так і системними операторами. Найважливіше те, що цей підхід може бути використаний для розподілу ресурсів щодо підвищення стійкості.

Незважаючи на те, що запропонований підхід інтегрує кілька сфер стійкості та реагування системи на загрози за допомогою інтегрованих показників стійкості, подальша робота має зосереджуватися на визначенні стійкості як мережевої властивості системи. Однак, незважаючи на критичну важливість міждоменних явищ, дослідження систем як багатодоменних мереж є відносно рідкісним явищем; натомість у науковій літературі прийнято зосереджуватися на мережах, що складаються з однорідних елементів (наприклад, мережа комунікаційних пристроїв або мережа соціальних істот). Проте більшість, якщо не всі мережі реального світу, є багатодоменними – важко знайти будь-яку реальну систему значної складності, яка б не включала комбінацію взаємопов'язаних фізичних елементів, комунікаційних пристроїв і каналів зв'язку, колекцій даних і людей-користувачів, що утворюють інтегроване, взаємозалежне ціле. Зв'язки між доменами, особливо зв'язки гетерогенної природи, можуть впливати на стійкість мережі і повинні оцінюватися за допомогою інструментів мережевої науки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Department of Defense (2011). Department of defense strategy for operating in cyberspace. URL: http://www.defense.gov/news/d20110714cyber.pdf (дата звернення: 12.11.2023).

2. Defense Science Board (2013). Task force report: resilient military systems and the advanced cyber threat. URL: http://www.acq.osd.mil/ dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

3. Resilience. URL: http://www.merriam-webster.com/dictionary/resilience (дата звернення: 12.11.2023).

4. National Academy of Sciences (2012). Disaster resilience: a national imperative. Washington DC, United States. URL: http://www.nap.edu/ catalog.php?record_id=13457 (дата звернення: 12.11.2023).

5. *Hollnagel, E., Paries, J., Woods, D. & Wreathall, J.* (2011). Resilience engineering in practice: a guidebook. Ashgate, United Kingdom.

6. *Kaplan. S. & Garrick, J.* (1981). On the quantitative definition of risk. Risk Analysis, 1 (1), 11–27.

7. *Park, J., Seager, T.P., Rao, P.S., Convertino, M. & Linkov, I.* (2012). Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Analysis, 33(3), 356–367.

8. *Chandrasekharan, P.C.* (1996). Robust control of linear dynamical systems. Academic Press, Missouri.

9. *Halvin, S., Kenett, D.Y., Ben-Jacob, E., Bunde, A., Choen, R., Hermann, H., Kantelhardt, J.W., Kertesz, J., Kirkpatrick, S., Kurths, J., Portugali, J. & Solomon, S.* (2012). Challenges in network science: applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics,* 214, 273–293.

10. *Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. & Seager, T.* (2013). Measurable resilience for actionable policy. *Environmental Science & Technology*, 47, 10108–10110.

11. *Jansen, W.* (2009). Directions in security metrics research. The National Institute of Standards and Technology (NISTIR), 7564. URL: http://csrc. nist.gov/publications/nistir/ir7564/nistir-7564_ metrics-research.pdf (дата звернення: 12.11.2023).

12. *Bartol, N., Bates, B., Goertzel, K. & Winograd, T.* (2009). Measuring cyber security and information assurance: a state of the art report. URL: https://www.thecsiac.com/sites/default/files/ cybersecurity.pdf (дата звернення: 12.11.2023).

13. *Kott, A. & Arnold, C.* (2013). The promises and challenges of continuous monitoring and risk scoring. IEEE Security & Privacy, 11 (1), 90–93.

14. *Alberts, D. & Hayes, R.* (2005). Code of best practice for experimentation. CCRP Publication Series, Washington.

15. *Alberts, D.* (2002). Information age transformation, getting to a 21st century military. DOD Command and Control Research Program. URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904 (дата звернення: 12.11.2023).

16. *Linkov, Igor, Eisenberg, Daniel A., Plourde, Kenton, Seager, Thomas P., Allen, Julia & Kott, Alex* (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33, 471–476. DOI: 10.1007/s10669-013-9485-y

17. *Allen, J. & Curtis, P.* (2011). Measures for managing operational resilience. CMU/SEI-2011-TR-019. URL: http://www.sei.cmu.edu/ reports/11tr019.pdf (дата звернення: 12.11.2023).

18. *Bodeau, D. & Graubart, R.* (2011). Cyber resiliency engineering framework. MTR110237. URL: http://www.mitre.org/sites/default/files/pdf/ 11_4436.pdf3 (дата звернення: 12.11.2023).

REFERENCES

1. Department of Defense (2011). Department of defense strategy for operating in cyberspace. URL: http://www.defense.gov/news/d20110714cyber.pdf. (Date of Application: 12.11.2023) [in English].

2. Defense Science Board (2013). Task force report: resilient military systems and the advanced cyber threat. URL: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (Date of Application: 12.11.2023) [in English].

3. Resilience. URL: http://www.merriam-webster.com/dictionary/resilience (Date of Application: 12.11.2023) [in English].

4. National Academy of Sciences (2012). Disaster resilience: a national imperative. Washington DC, United States. URL: http://www.nap.edu/ catalog.php?record_id=13457 (Date of Application: 12.11.2023) [in English].

5. *Hollnagel, E., Paries, J., Woods, D. & Wreathall, J.* (2011). Resilience engineering in practice: a guidebook. Ashgate, United Kingdom [in English].

6. *Kaplan. S. & Garrick, J*. (1981). On the quantitative definition of risk. *Risk Analysis,* 1 (1), 11–27 [in English].

7. *Park, J., Seager, T.P., Rao, P.S., Convertino, M. & Linkov, I.* (2012). Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Analysis, 33(3), 356–367 [in English].

8. *Chandrasekharan, P.C.* (1996). Robust control of linear dynamical systems. Academic Press, Missouri [in English].

9. *Halvin, S., Kenett, D.Y., Ben-Jacob, E., Bunde, A., Choen, R., Hermann, H., Kantelhardt,* J.W., *Kertesz, J., Kirkpatrick, S., Kurths, J., Portugali, J. & Solomon, S.* (2012). Challenges in network science: applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics,* 214, 273–293 [in English].

10. *Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. & Seager, T.* (2013). Measurable resilience for actionable policy. *Environmental Science & Technology,* 47, 10108–10110 [in English].

11. *Jansen, W.* (2009). Directions in security metrics research. The National Institute of Standards and Technology (NISTIR), 7564. URL: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf (Date of Application: 12.11.2023) [in English].

12. *Bartol, N., Bates, B., Goertzel, K. & Winograd, T.* (2009). Measuring cyber security and information assurance: a state of the art report. URL: https://www.thecsiac.com/sites/default/files/cybersecurity.pdf (Date of Application: 12.11.2023) [in English].

13. *Kott, A. & Arnold, C.* (2013). The promises and challenges of continuous monitoring and risk scoring. IEEE Security & Privacy, 11 (1), 90–93 [in English].

14. *Alberts, D. & Hayes, R.* (2005). Code of best practice for experimentation. CCRP Publication Series, Washington [in English].

15. *Alberts, D.* (2002). Information age transformation, getting to a 21st century military. DOD Command and Control Research Program. URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904 (Date of Application: 12.11.2023) [in English].

16. *Linkov, Igor, Eisenberg, Daniel A., Plourde, Kenton, Seager, Thomas P., Allen, Julia & Kott, Alex* (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions,* 33, 471–476. DOI: https://doi.org/10.1007/s10669-013-9485-y [in English].

17. *Allen, J. & Curtis, P.* (2011). Measures for managing operational resilience. CMU/SEI-2011-TR-019. URL: http://www.sei.cmu.edu/ reports/11tr019.pdf (Date of Application: 12.11.2023) [in English].

18. *Bodeau, D. & Graubart, R.* (2011). Cyber resiliency engineering framework. MTR110237. URL: http://www.mitre.org/sites/default/files/pdf/ 11_4436.pdf3 (Date of Application: 12.11.2023) [in English].

UDC 004.056

Demediuk Serhii,
Candidate of Juridical Sciences (Ph.D),
Deputy Secretary of the National Security and Defense Council of Ukraine,
Kyiv, Ukraine,
ORCID ID 0009-0008-1359-5265

REALIZATION OF THE ABILITY OF CYBERCRIME COUNTERMEASURES SYSTEM SUBJECTS

The article is devoted to the analysis of problematic issues related to the development of cyber resilience as the ability to withstand cyber threats, to update and adapt to them. Despite its national and international importance, resilience indicators for management decision-making are still in the early stages of development. These indicators establish a link between national policy goals and specific systemic measures, thereby enabling decisions regarding resource allocation to be translated into concrete actions and investments.

Attention is focused on determining the indicators of infrastructure sustainability, using quantitative and qualitative indicators popularized in the scientific literature. The proposed general matrix-based approach based on the integration of evidence, technical judgment and other opinions on the assessment of system resilience in the physical, information, cognitive and social spheres is considered. The individual segments of the matrix contain indicators

that measure the system's ability to manage adverse events and provide specific metrics for assessing cyber system resilience. The indicators developed from the resilience matrix cannot necessarily be measured by direct methods, but should be generated through specific measures developed for each system separately. These can be both quantitative data and qualitative indicators, which are then evaluated by technical experts and stakeholders related to the specific system. A key advantage of using a sustainability matrix is the transparent linkage between areas throughout the entire management cycle of the measures. Throughout the process of completing the matrix, the interdependence of indicators, stages and domains is critical. When adding an indicator, one should consider how it affects the others in the matrix.

It is emphasized that the growing complexity of cyber systems and cyber threats requires the integration of risk management and resilience management processes. Cyber resilience, which is flexible in nature, can provide a basis for combating cyber threats and the viability of critical cyber assets and services.

Keywords: sustainability, cyber security, cyber resilience, indicators, cyber risk, risk assessment.

Отримано 27.03.2024