ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351:338.2:005.6
DOI https://doi.org/10.32782/TNU-2663-6468/2026.5/27

Логвиненко С. В.
https://orcid.org/0009-0000-9186-4944
Київський національний університет імені Тараса Шевченка

СИСТЕМНИЙ ПІДХІД ДО ВИМІРЮВАННЯ ЕФЕКТИВНОСТІ БЕЗПЕКОВОГО УПРАВЛІННЯ: ЧОТИРИ ТИПИ МОНІТОРИНГУ ТА КОНЦЕПТУАЛЬНА РАМКА ДЛЯ УКРАЇНИ

Стаття присвячена системному підходу до моніторингу ефективності механізмів державного реагування на глобальні загрози в економічній сфері. Запропоновано концептуальне розмежування чотирьох типів моніторингу, що нерідко плутаються в управлінській практиці: моніторинг загрозового середовища (предмет: зовнішнє і внутрішнє середовище держави з точки зору наявності і характеру загроз); моніторинг функціонування системи реагування (предмет: інституційна архітектура, регуляторні процеси, оперативні дії); моніторинг результативності реагування (предмет: зв'язок між діями системи реагування і динамікою загрозового середовища); моніторинг системних ризиків (предмет: потенційні майбутні стани системи реагування і загрозового середовища). Систематизовано шість структурних обмежень чинної практики моніторингу в Україні: звітний характер, фрагментарність між органами влади, переважання ретроспективного підходу, недостатня формалізація методології, відрив від процесів прийняття рішень, недостатня цифровізація. Запропоновано шість принципів шестипринципової рамки вдосконалення моніторингу: постійність, інтеграція показників, вбудована прогностичність, формалізована методологічна основа, інтеграція в цикл прийняття рішень, цифровізована інфраструктура. На основі порівняльного аналізу трьох міжнародних моніторингових платформ (естонська X-Road, система Cooperation Group Директиви мережевої та інформаційної безпеки (Network and Information Security, NIS2) ЄС, сінгапурська платформа ризик-оцінювання і горизонтального сканування (Risk Assessment and Horizon Scanning, RAHS)) розроблено трирівневу архітектуру Інтегрованої системи моніторингу безпекового стану (ІСМБС) і визначено функціональні компоненти дашборду безпекового стану. Обґрунтовано п'ятиетапний імплементаційний план ІСМБС і визначено п'ять критичних умов функціональності системи. Обґрунтовано принцип інтегрованості: чотири типи моніторингу утворюють систему, де перший надає інформаційну основу для всіх інших, другий пояснює причини рівня результативності, третій вимірює вплив на загрозове середовище, четвертий формує превентивний потенціал системи. Запропонована концептуальна рамка завершує рекомендаційну логіку Розділу 4 і містить операційний вимір відповіді на центральне запитання: як системно виміряти ефективність механізмів державного реагування в умовах трансформації глобального загрозового середовища і одночасного євроінтеграційного курсу держави.

Ключові слова: *моніторинг ефективності, механізми державного реагування, глобальні загрози в економічній сфері, чотири типи моніторингу, шестипринципова рамка, ІСМБС, дашборд безпекового стану, X-Road, RAHS, NIS2 Cooperation Group.*

Постановка проблеми. Вимірювання ефективності механізмів державного реагування на глобальні загрози в економічній сфері є системно недооціненим виміром управлінської реформи. У типовій логіці реформування безпекового управління левова частка уваги концентрується на про-

© Логвиненко С. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

ектуванні нових структур, нормативних актів і процедур, тоді як питання їх вимірювання залишається другорядним. Наслідок є передбачуваним: через кілька років після реформи стає неможливим визначити, чи досягнула вона задекларованих цілей, оскільки система відліку не була закладена до початку реформи [5; 6]. Завершальний підрозділ Розділу 4 спрямований на усунення цієї прогалини через розроблення концептуальної рамки системи моніторингу ефективності.

Аналіз останніх досліджень і публікацій. Теоретичні засади моніторингу ефективності в публічному управлінні систематизовано у роботах Л. Лодж і К. Вегрих [5], Б. Петерса [6], А. Бойна зі співавторами [7]. Методологічний вимір оцінювання ефективності систем безпекового управління відображено у Методичних рекомендаціях Мінекономрозвитку України [1]. М. Рінард [19] аналізує ефект «крізіфікації» процесів формування політики і вплив цього ефекту на системи звітності. Методологія регуляторних пісочниць у контексті безпекових систем досліджується в роботі Т. Буоца і співавторів [23]. Цифровий вимір моніторингових систем представлений досвідом естонської X-Road [20], звітом Міжнародної організації вищих органів аудиту (International Organization of Supreme Audit Institutions, INTOSAI) [21] і дослідженням ООН [22]. Власна публікація автора у співавторстві [24] окреслює цифровий вимір управлінських рішень у сфері економічної безпеки. Попри значний масив публікацій, системна типологія моніторингу з концептуальною архітектурою для безпекової сфери залишається малодослідженою.

Постановка завдання. Мета статті полягає у системному аналізі типів моніторингу ефективності механізмів державного реагування на глобальні загрози в економічній сфері, критиці чинної практики і розробленні концептуальної рамки Інтегрованої системи моніторингу безпекового стану (ІСМБС) для України.

Виклад основного матеріалу. Чотири типи моніторингу: концептуальне розмежування. Поняття моніторингу в науці державного управління охоплює принципово відмінні управлінські функції, що нерідко плутаються [4]. Перший тип: моніторинг загрозового середовища. Його предметом є зовнішнє і внутрішнє середовище держави з точки зору наявності, інтенсивності і характеру загроз. Інструментарієм є систематичний збір інформації про геоекономічну динаміку, технологічні зміни, фінансові потоки і кіберактивність. Результатом є актуальний ситуаційний образ загрозового простору. Цей тип моніторингу в Україні є відносно найбільш розвиненим завдяки роботі розвідувальних структур і аналітичних підрозділів Ради національної безпеки і оборони України (РНБО) [2; 5].

Другий тип: моніторинг функціонування системи реагування. Його предметом є сама система: її інституційна архітектура, регуляторні процеси, оперативні дії, аналітичні продукти. Інструментарієм є збір інформації про швидкість прийняття рішень, повноту виконання процедур, якість координації між органами, дотримання визначених протоколів. Результатом є діагностична картина якості управлінських процесів незалежно від характеру загроз у конкретний момент [6; 7]. Третій тип: моніторинг результативності реагування. Його предметом є зв'язок між діями системи реагування і динамікою загрозового середовища: чи призводять конкретні регуляторні рішення до зниження безпекових ризиків. Цей тип є методологічно найскладнішим: встановлення причинно-наслідкового зв'язку між регуляторними заходами і станом безпеки вимагає контрфактичного аналізу [1; 14]. Четвертий тип: моніторинг системних ризиків. Його предметом є потенційні майбутні стани системи реагування і загрозового середовища. Інструментарієм є сценарне моделювання, аналіз слабких сигналів, форсайт-дослідження. Результатом є заздалегідь ідентифіковані уразливості, що стають підставою для превентивних заходів [11; 19].

Чотири типи утворюють інтегровану систему, де перший надає вхідні дані для третього і четвертого; другий дає зрозуміти, чому результативність є такою, якою вона є; четвертий визначає, де слід посилити другий і третій. В Україні між чотирма типами існує значна асиметрія: перший тип відносно розвинений, другий і третій реалізуються фрагментарно, четвертий практично відсутній як системна практика [3; 8].

Шість структурних обмежень чинної практики. Перше: звітний характер моніторингу. Чинна практика спирається на періодичні звіти, які формуються окремими державними органами і агрегуються у звичайних адміністративних процесах. Така модель структурно нездатна забезпечити постійний моніторинг між звітними циклами. Друге: фрагментарність між органами влади. Національний банк України (НБУ) відстежує фінансову стабільність, Міністерство економіки відстежує макропоказники, Держфінмоніторинг відстежує підозрілі транзакції, Кіберцентр фіксує інциденти у кіберпросторі. Методологічно інтегрованого продукту з усіх цих потоків не існує [1; 6]. Третє:

переважання ретроспективного підходу над прогностичним. Четверте: недостатня формалізація методології: відсутні єдині стандарти збору даних і узгоджені методики розрахунку показників. П'яте: відрив моніторингу від циклу прийняття рішень. Шосте: недостатня цифровізація моніторингових процесів, що уповільнює оновлення показників і обмежує можливості автоматизованого аналізу [14; 22; 24].

Шість принципів вдосконалення системи моніторингу. Перший принцип: постійність моніторингу: перехід від звітної моделі до безперервного оновлення показників. Інструментальною основою є цифрові платформи з автоматизованим збором даних. Другий принцип: інтеграція показників різних рівнів і галузей: об'єднання моніторингових даних різних органів в єдину аналітичну платформу з методологічно узгодженими показниками. Третій принцип: вбудована прогностичність: інтеграція прогностичних методологій у структуру моніторингу: сценарне моделювання, аналіз слабких сигналів, форсайт-дослідження [11; 19]. Четвертий принцип: формалізована методологічна основа: єдині стандарти збору, обробки і агрегування даних для всіх структур безпекової моніторингової системи [1; 17]. П'ятий принцип: інтеграція моніторингу в цикл прийняття рішень: формалізовані процедури використання результатів моніторингу при ухваленні стратегічних, регуляторних і оперативних рішень. Шостий принцип: цифровізована інфраструктура: системне використання цифрових технологій для всіх компонентів: автоматизованого збору даних, інтегрованої обробки і штучного інтелекту (ШІ)-асистованої аналітики [15; 16; 24].

Шість принципів прямо адресують шість обмежень: постійність усуває звітний характер; інтеграція показників усуває фрагментарність; вбудована прогностичність усуває ретроспективність; формалізована методологія усуває стихійність; інтеграція в цикл рішень усуває відрив від практики; цифровізована інфраструктура усуває технологічну відсталість [5; 7; 22].

Три міжнародних кейси. Естонська платформа X-Road є фундаментальною інфраструктурою цифрового урядування Естонії і технологічною основою для більшості державних моніторингових систем. Принциповою архітектурною характеристикою є децентралізована архітектура зберігання даних при централізованій методологічній координації: кожен орган влади зберігає власні дані, але через X-Road надає до них контрольований доступ іншим органам і агрегованим платформам. Для ІСМБС цей принцип є ключовим: він дозволяє вирішити проблему фрагментарності без створення централізованої бази даних з відповідними ризиками безпеки і концентрації влади [20; 22].

Система моніторингу критичної інфраструктури ЄС у межах Cooperation Group (NIS2) [10] становить взірцевий приклад наднаціональної моніторингової системи: кожна держава-член звітує за спільними показниками, що дозволяє виявляти транскордонні вразливості і порівнювати ефективність у порівняльній перспективі. Сінгапурська платформа ризик-оцінювання і горизонтального сканування (Risk Assessment and Horizon Scanning, RAHS) поєднує ретроспективний моніторинг поточного стану з систематизованим форсайт-аналізом майбутніх загроз. Принциповою рисою RAHS є інституційна інтеграція: її результати є обов'язковим елементом процесів стратегічного планування в урядовому секторі Сінгапуру [11; 19].

Методологічні уроки для ІСМБС. Перший: децентралізована архітектура зберігання з централізованою методологічною координацією забезпечує баланс між захистом даних і аналітичною цінністю. Другий: обов'язковість використання результатів моніторингу в управлінських рішеннях є необхідною умовою, а не опцією. Третій: орієнтація на міжнародні стандарти даних і таксономій є ключовою для подальшої євроінтеграції. Четвертий: довгостроковий горизонт інвестицій: X-Road розвивалась з 2001 р., RAHS з 2004 р. П'ятий: відкритість окремих компонентів системи для публічного аналізу підвищує легітимність і залучає ресурси громадянського суспільства [20; 21; 23].

Трирівнева архітектура ІСМБС. На основі шести принципів і міжнародного досвіду пропонується трирівнева архітектура Інтегрованої системи моніторингу безпекового стану (ІСМБС). Перший рівень: джерела даних. Охоплює внутрішні бази даних державних органів (реєстри Міністерства фінансів, банківська звітність НБУ, дані Держфінмоніторингу, відомості РНБО) і зовнішні потоки (ринкові індикатори, міжнародні індекси, відкриті джерела кіберзагроз від Агентства ЄС з кібербезпеки (European Union Agency for Cybersecurity, ENISA) і CERT-UA [12]). Другий рівень: обробка і агрегування. Охоплює системи нормалізації, очищення і методологічного агрегування даних за визначеними алгоритмами. Третій рівень: інтерфейс і прийняття рішень. Надає диференційований доступ для різних категорій користувачів: стратегічного (Президент, члени РНБО, Прем'єр-міністр), тактичного (профільні міністри, регулятори) і оперативного рівнів [18; 24].

Дашборд безпекового стану структурований за принципом ієрархічної декомпозиції. На верхньому рівні представлений інтегральний показник стану системи реагування. На другому рівні представлена декомпозиція за п'ятьма блоками критеріїв: інституційно-організаційним, нормативно-правовим, ресурсно-функціональним, комунікативно-координаційним і адаптивно-інноваційним. Чотири функціональні компоненти дашборду: ієрархічна декомпозиція показників; інструмент сценарного моделювання («що, якщо»); модуль раннього попередження (автоматичні сигнали при відхиленнях показників від порогових критеріїв); модуль міжнародних бенчмарків (порівняння з країнами-референтами і міжнародними індексами) [1; 14; 17].

П'ятиетапний імплементаційний план. Перший етап (місяці 1–6): концептуальне і нормативне оформлення: розробка концепції ІСМБС і ухвалення нормативного акта. Другий етап (місяці 4–12): інвентаризація і стандартизація джерел даних. Третій етап (місяці 9–21): розгортання технологічної платформи: розробка алгоритмічних модулів і дашбордів. Четвертий етап (місяці 18–30): пілотне впровадження в одному-двох секторах (фінансовому і кібербезпековому). П'ятий етап (місяці 27–36): повномасштабне впровадження і інтеграція в управлінський цикл [3; 9; 23].

П'ять критичних умов функціональності ІСМБС. Перша: якість і повнота джерел даних: ІСМБС функціонує настільки якісно, наскільки якісні вхідні дані. Друга: захист системи від кіберзагроз: ІСМБС є привабливою мішенню через концентрацію чутливих безпекових даних, що потребує проектування з урахуванням принципу «безпека як базова вимога» [8; 15]. Третя: наявність кваліфікованого персоналу трьох рівнів: технічних фахівців, методологів і аналітиків-інтерпретаторів. Четверта: реальна інтеграція результатів моніторингу в управлінські рішення, а не формальна звітність [5; 13]. П'ята: суспільна легітимність через прозорість методології і відкриті компоненти системи [22; 24].

Зв'язок ІСМБС з архітектурною моделлю п'яти контурів. Запропонована система моніторингу є функціонально інтегрованою з інтегральною архітектурною моделлю з п'яти контурів, розробленою у підрозділі 4.4. Аналітичний контур з моделі 4.4 є організаційним носієм другого рівня ІСМБС: він агрегує, обробляє і готує аналітичні продукти з даних першого рівня. Стратегічний контур є основним споживачем третього рівня ІСМБС: саме стратегічне керівництво використовує дашборд безпекового стану для прийняття рішень. Контур адаптивного навчання є організаційним носієм аналізу після дій (after-action review, AAR), що є одним з основних механізмів зворотного зв'язку ІСМБС. Отже, ІСМБС не є окремою системою поруч з архітектурою п'яти контурів, а є її вбудованим вимірювальним контуром: без ІСМБС архітектурна модель залишається конструкцією без зворотного зв'язку, без адаптивного характеру [5; 7; 13].

Методологія розрахунку інтегрального показника безпекового стану. Дашборд безпекового стану містить інтегральний показник стану системи реагування, що потребує визначеної методології розрахунку. Пропонується п'ятирівнева шкала (критичний: 1,0–1,9; незадовільний: 2,0–2,9; задовільний: 3,0–3,9; достатній: 4,0–4,9; відмінний: 5,0), аналогічна шкалі оцінювання Методичних рекомендацій Мінекономрозвитку [1]. Розрахунок ґрунтується на зваженому агрегуванні п'яти блоків критеріїв: інституційно-організаційного, нормативно-правового, ресурсно-функціонального, комунікативно-координаційного та адаптивно-інноваційного. Ваги блоків диференційовані залежно від операційного режиму системи: у режимі планомірного функціонування більша вага надається інституційному і нормативному блокам; у кризовому режимі більша вага надається ресурсно-функціональному і комунікативно-координаційному. Методологічна основа зваженого агрегування спирається на процес аналітичної ієрархії [17], верифікований методологічними настановами ОЕСР і Всесвітнього банку [6; 14; 17].

Відкриті компоненти ІСМБС і стратегія публічної комунікації. Принцип суспільної легітимності, визначений як п'ята критична умова функціональності ІСМБС, вимагає не лише декларативної відкритості, а й конкретних механізмів публічного доступу до результатів моніторингу. Пропонується трирівнева стратегія відкритості. Перший рівень: повністю відкриті компоненти ІСМБС: агреговані показники безпекового стану без деталізації секретних джерел, методологія розрахунку показників, міжнародні бенчмарки. Другий рівень: умовно відкриті компоненти, тобто інформація, що є відкритою для парламентських комітетів і незалежних аудиторів, але не для широкої публіки (детальні джерела даних, методологія сценарного моделювання). Третій рівень: закриті компоненти: розвідувальні оцінки, алгоритмічні деталі. Трирівнева стратегія відкритості дозволяє максимізувати суспільну легітимність при збереженні необхідного рівня інформаційної безпеки [20; 21; 22].

Порівняльна оцінка ІСМБС відносно наявних систем в Україні. Для коректного позиціонування ІСМБС важливо зрозуміти, як вона співвідноситься з наявними моніторинговими елементами українського безпекового апарату. Рахункова палата України здійснює аудит ефективності використання бюджетних коштів, але не охоплює безпекову результативність у динамічному вимірі. Система показників оцінювання Міністерства економіки фіксує агреговані макропоказники, але не диференціює між чотирма типами моніторингу. Стратегічний аудит РНБО охоплює оцінку реалізації стратегічних рішень, але не містить автоматизованого моніторингу у реальному часі. ІСМБС є не альтернативою, а інтеграційним шаром над усіма наявними системами: вона агрегує і синтезує їх дані, формуючи цілісний образ безпекового стану [1; 2; 3; 17]. Ця логіка запозичена з естонської X-Road: платформа не замінює відомчі бази даних, а надає уніфікований інтерфейс доступу до них.

Поетапна деталізація впровадження і ресурсні потреби. Реалізм імплементаційного плану ІСМБС визначається відповідністю між амбіціями і ресурсними потребами. Перший і другий етапи (концептуальне оформлення і стандартизація) є переважно організаційно-методологічними і не потребують значних фінансових ресурсів: їх реалізація можлива в межах наявного бюджету апарату РНБО і профільних міністерств за умови відповідного мандату [2; 3]. Третій етап (розгортання платформи) є найбільш ресурсоємним. Досвід аналогічних проектів в Естонії і Польщі свідчить: вартість системи такого класу варіюється від 5 до 15 млн євро залежно від рівня автоматизації і охоплення джерел даних. Значна частина цих інвестицій може бути покрита через євроінтеграційні фонди і двосторонню технічну допомогу від держав-партнерів, що вже реалізували аналогічні системи [20; 21; 22]. Четвертий і п'ятий етапи (пілот і повне впровадження) є переважно організаційними і залежать передусім від якості інституційного мандату і готовності персоналу [18; 23].

Висновки. Запропонована концептуальна рамка системи моніторингу завершує рекомендаційну логіку Розділу 4, надаючи їй операційного виміру. По-перше, розмежування чотирьох типів моніторингу усуває концептуальну плутанину між інструментами різного призначення і дозволяє адресно усувати специфічні дефіцити. По-друге, шість принципів вдосконалення разом формують цілісну рамку, де кожен принцип адресує конкретне обмеження чинної практики. По-третє, трирівнева архітектура ІСМБС і дашборд безпекового стану є конкретними операційними конструкціями, доступними для практичного проектування. Перспективи подальших досліджень включають розробку детальних технічних специфікацій для кожного рівня ІСМБС і пілотне тестування методології ієрархічної декомпозиції показників на матеріалі конкретного сектора безпекової сфери.

Список літератури:

1. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України: наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13

2. Про рішення Ради національної безпеки і оборони України «Про Стратегію економічної безпеки України»: Указ Президента України від 11.08.2021 № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021

3. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19

4. Ситник Г. П. Державне управління у сфері національної безпеки: підручник. Київ: НАДУ, 2012. 544 с.

5. Lodge G., Wegrich K. The Problem-Solving Capacity of the Modern State: Governance Challenges and Administrative Capacities. Oxford: Oxford University Press, 2014. 290 p.

6. Peters B. G. The Politics of Bureaucracy: An Introduction to Comparative Public Administration. 7th ed. New York: Routledge, 2018. 344 p.

7. Boin A., Hart P., Stern E., Sundelius B. The Politics of Crisis Management: Public Leadership Under Pressure. 2nd ed. Cambridge: Cambridge University Press, 2017. 228 p.

8. Farrell H., Newman A. L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*. 2019. Vol. 44. No. 1. P. 42–79.

9. Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*. 2022. L 333. P. 164–198.

10. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union.* 2022. L 333. P. 80–152.

11. European Commission. 2024 Strategic Foresight Report: Sustainability and People's Wellbeing at the Heart of Europe's Open Strategic Autonomy. COM (2024) 530 final. Brussels: European Commission, 2024. 36 p.
12. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Athens: ENISA, 2024. 156 p.
13. World Economic Forum. The Global Risks Report 2025. 20th Edition. Geneva: World Economic Forum, 2025. 124 p.
14. Center for Strategic and International Studies (CSIS). Assessing the Economic Security Landscape: Benchmarks and Gaps. Washington, D.C.: CSIS, 2023. 64 p.
15. Brundage M., Avin S., Clark J., Toner H., Eckersley P. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, Oxford, 2018. 100 p.
16. Acharya P. Artificial Intelligence in National Security: Strategic Approaches. *Journal of Strategic Security*. 2023. Vol. 16. No. 2. P. 89–112.
17. World Bank. Worldwide Governance Indicators: Methodology and Analytical Issues. Policy Research Working Paper. Washington, D.C.: World Bank, 2021. 68 p.
18. Financial Action Task Force (FATF). Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems. Paris: FATF, 2022. 244 p.
19. Rhinard M. The Crisisification of Policy-making in the European Union. *Journal of Common Market Studies*. 2019. Vol. 57. No. 3. P. 256–272.
20. e-Estonia Briefing Centre. X-Road: A Decentralized Data Exchange Layer. Tallinn: e-Estonia Briefing Centre, 2024. 60 p.
21. International Organization of Supreme Audit Institutions (INTOSAI). Auditing Public Sector Digital Infrastructure: Methodological Guidelines. Vienna: INTOSAI, 2023. 48 p.
22. United Nations. E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: UN DESA, 2024. 312 p.
23. Buocz T., Pfotenhauer S., Eisenberger I. Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety. *Law, Innovation and Technology*. 2023. Vol. 15. No. 2. P. 357–389.
24. Logvynenko S., Krivonosov L., Zhurba O., Kukin I., Pynda Yu. Digital Technologies in the System of State Economic Security Management. *Periodicals of Engineering and Natural Sciences*. 2026. Vol. 14. No. 1. P. 141–166. DOI: 10.21533/pen.v14.i1.1527

Logvynenko S. V. A SYSTEMIC APPROACH TO MEASURING SECURITY GOVERNANCE EFFECTIVENESS: FOUR MONITORING TYPES AND A CONCEPTUAL FRAMEWORK FOR UKRAINE

This article is devoted to a systemic approach to monitoring the effectiveness of state response mechanisms to global threats in the economic sphere. A conceptual distinction is proposed among four monitoring types that are frequently conflated in management practice: monitoring of the threat environment (subject: the state's external and internal environment from the perspective of the presence and nature of threats); monitoring of response system functioning (subject: institutional architecture, regulatory processes, operational actions); monitoring of response effectiveness (subject: the link between the response system's actions and the dynamics of the threat environment); and monitoring of systemic risks (subject: potential future states of the response system and threat environment). Six structural limitations of current monitoring practice in Ukraine are systematized: its reporting character; fragmentation among government bodies; predominance of the retrospective approach; inadequate methodological formalization; disconnection from decision-making processes; and insufficient digitalization. Six principles of an improvement framework are proposed: continuity, indicator integration, embedded foresight, formalized methodological basis, integration into the decision-making cycle, and digitalized infrastructure. Based on a comparative analysis of three international monitoring platforms (Estonian X-Road, the EU NIS2 Cooperation Group system, and Singapore's RAHS), a three-tier architecture of an Integrated Security Status Monitoring System (ISSMS) is developed and the functional components of a security status dashboard are identified. A five-stage implementation plan for ISSMS is substantiated, and five critical conditions for system functionality are identified. The proposed framework completes the recommendation logic of Chapter 4 and provides the operational dimension for systematically measuring the effectiveness of response mechanisms.

Keywords: *effectiveness monitoring; state response mechanisms; global threats in the economic sphere; four monitoring types; six-principle framework; ISSMS; security status dashboard; X-Road; RAHS; NIS2 Cooperation Group.*

Дата першого надходження статті до видання: 03.09.2026
Дата прийняття статті до друку після рецензування: 21.09.2026
Дата публікації (оприлюднення) статті: 16.11.2026