

<https://doi.org/10.31891/2307-5740-2026-358-53>

УДК 351.746.1:004.8:35.073.515

JEL classification H56, H83, O33, O38, K24

ГАВРИЛЕЧКО Юрій

ЗВО «Університет трансформації майбутнього»

<https://orcid.org/0000-0003-1930-7638>

ШЛЯХИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ІНСТИТУЦІЙНІ, НОРМАТИВНІ ТА ТЕХНОЛОГІЧНІ РІШЕННЯ

Статтю присвячено проблемі розриву між змістом державних стратегій у сфері інформаційної безпеки та станом їх фактичної реалізації. Показано, що цей розрив є не випадковим наслідком ресурсних обмежень, а структурним: стратегія формулює цілі в категоріях бажаного стану, тоді як виконання фіксується в категоріях проведених заходів, і між цими двома мовами опису немає переходу. На матеріалі офіційних даних про стан виконання Стратегії кібербезпеки України, за якими загальний показник зріс із 32 % у 2022 році до 86 % у 2025-му за одночасного збереження напрямів із виконанням на рівні 23 %, обґрунтовано, що високий агрегований показник приховує нерівномірність, яка й визначає реальну захищеність. Запропоновано розглядати шляхи реалізації стратегії у трьох взаємопов'язаних зрізах: інституційному, нормативному та технологічному. Для кожного зрізу визначено характерний тип розриву між задумом і виконанням, а також інструмент його усунення. Обґрунтовано, що ключовою умовою результативності є перехід від звітування про заходи до вимірювання спроможностей, для чого запропоновано використати конструкцію щорічних операційних планів із індикаторами стану. Систематизовано зарубіжний досвід оцінювання реалізації національних стратегій, зокрема висновки щодо відсутності вартісних оцінок і показників результативності, та визначено, які його елементи придатні для вітчизняних умов. Запропоновано модель трирівневого зчеплення документів, за якої стратегічна ціль, операційний захід і технологічна спроможність пов'язані спільним індикатором.

Ключові слова: інформаційна безпека, державна стратегія, реалізація стратегії, інституційна спроможність, нормативне забезпечення, індикатори результативності, кіберстійкість, державне управління.

GAVRILECHKO Yuriy

Higher Educational Institution "University of Future Transformation"

PATHWAYS FOR IMPLEMENTING THE STATE INFORMATION SECURITY STRATEGY: INSTITUTIONAL, REGULATORY AND TECHNOLOGICAL SOLUTIONS

The article addresses the gap between the content of state strategies in the field of information security and the state of their actual implementation. It is shown that this gap is not an incidental consequence of resource constraints but a structural one: a strategy formulates goals in terms of a desired state, whereas implementation is recorded in terms of measures carried out, and there is no transition between these two descriptive languages. Drawing on official data concerning the implementation of Ukraine's Cybersecurity Strategy, according to which the aggregate indicator rose from 32 per cent in 2022 to 86 per cent in 2025 while individual directions remained at 23 per cent, it is substantiated that a high aggregate figure conceals the unevenness that actually determines the level of protection. It is proposed to consider the pathways of strategy implementation in three interrelated dimensions: institutional, regulatory and technological. For each dimension, a characteristic type of gap between intent and execution is identified, together with the instrument capable of closing it. It is argued that the key condition for effectiveness is the transition from reporting on measures to measuring capabilities, for which the construction of operational plans with indicators, embedded in the draft of the new Information Security Strategy, can be used. Foreign experience in evaluating the implementation of national strategies is systematised, in particular the findings concerning the absence of cost estimates and outcome-oriented performance measures, and those of its elements suitable for domestic conditions are identified. A model of three-tier linkage between documents is proposed, in which a strategic goal, an operational measure and a technological capability are connected by a shared indicator.

Key words: information security, state strategy, strategy implementation, institutional capacity, regulatory framework, performance indicators, cyber resilience, public administration.

Стаття надійшла до редакції / Received 04.09.2026

Прийнята до друку / Accepted 25.10.2026

Опубліковано / Published 29.10.2026



This is an Open Access article distributed under the terms of the [Creative Commons CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)

© ГАВРИЛЕЧКО Юрій

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Україна має розгорнуту систему стратегічних документів у сфері інформаційної безпеки. Стратегію інформаційної безпеки затверджено Указом Президента України від 28 грудня 2021 року № 685/2021 [14], Стратегію кібербезпеки України – Указом Президента України від 26 серпня 2021 року № 447/2021 [13], план заходів з реалізації першої з них – розпорядженням Кабінету Міністрів України від 30 березня 2023 року № 272-р [9]. Формально конструкція є повною: визначено цілі, виконавців, строки та механізм звітування.

Проте наявність документів і наявність результату – різні речі, і саме відстань між ними становить предмет цього дослідження. Питання полягає не в тому, чи правильно сформульовано цілі, а в тому, що відбувається між їх формулюванням і моментом, коли вони мають бути досягнуті.

Офіційні дані дають підстави для точнішої постановки проблеми. За результатами огляду національної системи кібербезпеки загальний стан виконання Стратегії кібербезпеки України зріс із 32 % у 2022 році до 86 % у 2025-му: «Радикально зменшується кількість кіберінцидентів критичного та високого рівня, і одночасно з цим загальний показник реалізації Стратегії кібербезпеки зріс від 32% у 2022 році до 86% у 2025-му» [8, с. 4]. Показник високий, і сам собою він свідчить про суттєве просування. Водночас у тому самому огляді за окремими напрямками зафіксовано виконання на рівні 76 %, 88 % і 97 %, а щодо одного з показників 2025 року – лише 23 % [8, с. 38–42]. Тобто агрегований результат приховує розкид, за якого окремі напрями фактично не рухаються, і саме вони, а не середнє значення, визначають реальний рівень захищеності: система стійка настільки, наскільки стійка її найслабша ланка.

Друга обставина, що загострює проблему, – це зміна самого предмета захисту протягом строку дії стратегії. Обидві чинні стратегії ухвалювалися до масового поширення генеративних моделей штучного інтелекту (ШІ). За чотири роки, що минули, змінився не лише інструментарій нападу, а й структура вразливостей, а також склад суб'єктів, здатних здійснювати складні операції. Стратегічний цикл, розрахований на відносно стабільне середовище, у таких умовах стикається з тим, що частина запланованих заходів втрачає актуальність ще до моменту їх виконання. Це стосується і класифікацій загроз, покладених в основу планування: наявні вітчизняні класифікації формувалися з урахуванням реалій воєнного часу, причому дослідники фіксують, що «на сьогоднішній день відсутній єдиний підхід до класифікації та оцінки таких загроз» [7, с. 257], проте чинник ШІ в них представлений фрагментарно.

Третя обставина має суто управлінський характер. Реалізація стратегії фіксується у звітності про виконання плану заходів, тобто в категоріях дії: розроблено, затверджено, проведено, забезпечено. Сама ж стратегія формує цілі в категоріях стану: підвищення рівня захищеності, зміцнення стійкості, формування спроможності. Між цими двома мовами опису немає автоматичного переходу. Виконання всіх заходів плану не є доказом досягнення цілі, а невиконання окремого заходу не є доказом її недосягнення. Унаслідок цього звітність перестає бути інструментом управління й перетворюється на самостійну процедуру, що описує власний перебіг.

Практичне значення проблеми посилюється тим, що Україна перебуває на етапі зміни стратегічного циклу: строк дії чинних документів завершується, а наступний цикл планування лише формується. Момент переходу до нового циклу є саме тією точкою, у якій можливо врахувати досвід попереднього, і саме тому систематизація шляхів реалізації стратегії має не ретроспективний, а прикладний характер.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика реалізації стратегій у сфері інформаційної безпеки опрацьована нерівномірно: оцінювання змісту стратегій представлено значно ширше, ніж оцінювання їх виконання.

Серед вітчизняних джерел найбільшу вагу для цього дослідження має огляд національної системи кібербезпеки, що містить систематизовані дані про стан виконання Стратегії кібербезпеки України за 2022–2025 роки з розподілом за напрямками та фіксацією системних викликів, які унеможливили повноцінне виконання [8]. Окреме значення має підготовлена експертним середовищем оцінка реалізації Стратегії інформаційної безпеки 2021–2025 років, автори якої – П. Бурдяк, О. Спесивцева, В. Онищенко та В. Митрофанова – проаналізували текст Стратегії, план заходів та офіційні звіти за 2023–2025 роки й зіставили вітчизняний підхід із досвідом Європейського Союзу, Естонії, Латвії та Молдови [2]. Первинним матеріалом для такого оцінювання слугують щорічні аналітичні звіти профільного міністерства про стан виконання плану заходів [15]. Їхній висновок про те, що система звітності поступово стала аналітично орієнтованою й почала містити не лише перелік заходів, а й виявлені проблеми та рекомендації, є важливим свідченням еволюції самого інструмента звітування.

Інституційний зріз проблеми розглянуто в дослідженнях інституційного забезпечення стійкості критичної інфраструктури, де «зазначені рівні та органи управління національною системою захисту критичної інфраструктури України» у зіставленні з практикою Європейського Союзу та НАТО [16, с. 46], а також у працях щодо формування та реалізації державної політики у відповідній сфері, де наголошено, що успішність розв'язання відповідних питань «здебільшого залежить від ефективності формування та реалізації державної політики у сфері захисту критичної інфраструктури та забезпечення національної системи стійкості України, належної організації державного управління у цій сфері» [1, с. 138].

Зарубіжний доробок дає матеріал іншого типу – методичний. Висновки Урядового бюро підзвітності США щодо реалізації національної кіберстратегії є в цьому сенсі показовими: за наявності повноцінного плану реалізації в ньому бракувало оцінки вартості заходів і орієнтованих на результат показників ефективності, без яких неможливо встановити, чи рухається система до мети [17]. Порівняльне оцінювання стратегій провідних держав, здійснене за єдиною шкалою, демонструє, що стратегічне документування у цій сфері залишається молодого дисципліною: майже половина зі 132 держав, що мають національну кіберстратегію, станом на 2024 рік ухвалили лише один такий документ [18].

Методологічну основу вимірювання спроможностей опрацьовано в межах моделей зрілості. Систематизація обмежень таких моделей, здійснена на основі огляду наявних підходів, фіксує характерну ваду: моделі добре описують наявний стан, але слабко пов'язують його з конкретними управлінськими

рішеннями, потрібними для переходу на вищий рівень [19]. Функціональна рамка кібербезпеки другої версії, що вперше виокремила врядування як самостійну функцію поряд із ідентифікацією, захистом, виявленням, реагуванням і відновленням, дає конструкцію, придатну для зчеплення стратегічного й операційного рівнів [20].

Нарешті, безпосереднім підґрунтям дослідження є попередні праці автора. У межах того самого завдання дисертаційного дослідження обґрунтовано концептуальну модель системи державного управління інформаційною безпекою в умовах поширення ІІІ, визначальною рисою якої є контур адаптації, що «передбачає періодичний перегляд правил, оскільки технології ІІІ змінюються швидше за нормативні акти» [3, с. 314]; порівняльний аналіз інституційних моделей державного управління у цій сфері викладено окремо, де проблему визначено як брак «систематизованого порівняльного аналізу цих моделей, що охоплював би інституційну архітектуру, регуляторний підхід до ІІІ та механізм їх інтеграції» [5, с. 23]; трансформацію моделей публічного управління під впливом інформаційних технологій розглянуто в попередній публікації у цьому виданні, де серед напрямів інституційної адаптації визначено «перехід від реактивної до антиципаційної моделі держави» [4, с. 141].

Отже, зміст стратегій оцінено, інституційна конструкція описана, методичний інструментарій вимірювання зрілості розроблено. Водночас бракує праць, які пов'язували б ці три складові в єдину конструкцію шляхів реалізації й давали відповідь на питання, за рахунок чого саме стратегічна ціль перетворюється на зміну фактичного стану захищеності. Саме на цьому питанні й зосереджено подальший виклад.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті – обґрунтувати шляхи реалізації державної стратегії інформаційної безпеки в інституційному, нормативному та технологічному зрізах і запропонувати конструкцію, що пов'язує стратегічні цілі з вимірюваними змінами стану захищеності.

Завдання дослідження. Для досягнення зазначеної мети визначено наступні дослідницькі завдання:

- 1) Визначити природу розриву між змістом стратегії та станом її реалізації й показати, чому цей розрив є структурним, а не ресурсним.
- 2) Систематизувати шляхи реалізації стратегії за трьома зрізами, визначивши для кожного характерний тип розриву та інструмент його усунення.
- 3) Обґрунтувати модель зчеплення стратегічного, операційного й технологічного рівнів через спільний індикатор та визначити умови й обмеження її впровадження.

Реалізація стратегії розглядається тут як сукупність пов'язаних між собою рішень різного рівня, а не як перелік відокремлених заходів, що й зумовило застосування системного підходу у поєднанні з порівнянням, класифікацією та узагальненням. Матеріалом слугували чинні нормативно-правові акти України, офіційні звітні документи про стан виконання стратегій, зарубіжні оцінювальні висновки щодо реалізації національних стратегій, а також наукові публікації переважно 2024–2026 років.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Природа розриву між стратегією та її реалізацією

Розрив між стратегічним задумом і фактичним результатом прийнято пояснювати браком ресурсів. Таке пояснення є частково слушним, однак недостатнім: воно не пояснює, чому за високих агрегованих показників виконання окремі напрями залишаються нерухомими, і чому виконання заходу не завжди змінює стан, заради якого його запроваджували.

Точніше пояснення полягає в різниці мов опису. Стратегія оперує станами: захищеність, стійкість, спроможність. План заходів оперує діями: розробити, затвердити, провести. Звіт фіксує виконання дій. Між виконаною дією і зміненим станом лежить припущення, яке в жодному документі не перевіряється: що саме ця дія призводить саме до цієї зміни. Доки припущення не перевірено, система звітує про рух, не маючи змоги встановити його напрям. Показово, що цю невідповідність фіксує й сам огляд національної системи кібербезпеки, зазначаючи, що «значна частина підзаконних актів набула чинності лише наприкінці року, а їх практична реалізація відстає від нормотворчих темпів» [8, с. 4].

Із цього випливає перший практичний висновок. Агрегований показник виконання, навіть високий, не є показником захищеності. Зростання з 32 % до 86 % [8] фіксує, що план виконується, а не що держава стала захищенішою у відповідній пропорції. Водночас напрям із показником 23 % [8] є інформативнішим за середнє значення саме тому, що вказує місце, де рух відсутній.

Другий висновок стосується асиметрії уваги. Заходи, що легко піддаються фіксації – ухвалення акта, проведення навчання, створення підрозділу, – мають вищу ймовірність бути виконаними й відображеними у звіті, ніж заходи, результат яких проявляється поступово й не має дати завершення. Відповідно, звітність систематично зміщена на користь дискретних дій, а завдання, що потребують тривалого накопичення спроможності, опиняються в зоні структурної недооцінки. Наслідок цього названо в огляді прямо: наявний дефіцит кваліфікованих кадрів «створює ризики формального виконання вимог без досягнення реального підвищення рівня кіберстійкості» [8, с. 11].

Саме ці дві властивості – відсутність перевіреного зв'язку між дією та станом і зміщення на користь дискретних заходів – роблять розрив структурним. Він відтворюється незалежно від обсягу виділених ресурсів, і тому збільшення фінансування саме собою його не усуває.

Інституційні рішення

Інституційний зріз реалізації стратегії охоплює розподіл відповідальності, координацію виконавців і механізм, за яким ухвалюється рішення про коригування.

Характерним розривом цього зрізу є невідповідність між кількістю виконавців і спроможністю узгоджувати їхні дії. План заходів із реалізації стратегії за своєю природою є міжвідомчим документом: той самий захід часто потребує участі кількох органів, жоден з яких не має повноважень щодо інших. За відсутності суб'єкта, уповноваженого не лише збирати звітність, а й ухвалювати рішення про перерозподіл зусиль, координація зводиться до узагальнення поданих відомостей.

Інструментом усунення цього розриву є перехід від координації як збирання до координації як функції. Практично це означає закріплення за визначеним суб'єктом трьох повноважень: встановлювати єдині вимоги до змісту звітних відомостей, ініціювати перегляд заходів за результатами моніторингу й виносити питання невиконання на рівень, здатний ухвалити рішення. Перші два елементи у вітчизняній практиці вже частково реалізовані: офіційні звіти останніх років містять не лише перелік заходів, а й опис виявлених проблем та рекомендації [2], що свідчить про рух саме в цьому напрямі.

Другим інституційним рішенням є розмежування ролей замовника й виконавця в межах самої системи. Коли орган, відповідальний за напрям, одночасно є головним виконавцем заходів і джерелом звітності про їх виконання, оцінка результату неминуче зміщується. Міжнародна практика розв'язує це через зовнішнє оцінювання: висновки щодо реалізації національної кіберстратегії США готувалися органом, не причетним до її виконання, що й дозволило зафіксувати відсутність вартісних оцінок і показників результативності [17]. Для вітчизняних умов аналогом може бути залучення до оцінювання наукових установ і експертного середовища, що вже відбувається у форматі підготовки незалежних оцінок реалізації [2].

Третім рішенням є кадрове забезпечення. Воно зазвичай розглядається як ресурсне питання, однак має й інституційний вимір: без фахівців, здатних співвіднести технічний стан систем із формулюваннями стратегічних цілей, переклад між мовами опису, про який йшлося вище, не може бути здійснений у принципі.

Нормативні рішення

Нормативний зріз охоплює акти, якими стратегічні положення перетворюються на обов'язкові вимоги.

Характерний розрив тут полягає у відмінності юридичної природи документів. Стратегія є документом політики: вона визначає напрями, але не встановлює обов'язків, невиконання яких має наслідки. План заходів є актом організаційного характеру: він покладає завдання на органи, але не створює вимог до суб'єктів поза системою органів влади. Відповідно, між стратегічною ціллю й реальною поведінкою суб'єктів, чия захищеність і становить предмет стратегії, лежить ланка, яка має бути створена окремо.

Першим нормативним рішенням є послідовне доведення стратегічних положень до рівня приписових вимог. Йдеться не про ухвалення нових законів для кожної цілі, а про використання вже наявних повноважень: значна частина вимог у сфері інформаційної безпеки встановлюється підзаконними актами в межах компетенції, визначеної Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [12].

Другим рішенням є синхронізація строків. Нормативний акт, що запроваджує вимогу, і захід плану, що передбачає її запровадження, мають бути узгоджені не лише за змістом, а й у часі з циклом бюджетного планування. Практика щорічних планів заходів із реалізації Стратегії кібербезпеки, затверджуваних розпорядженнями Кабінету Міністрів України [10; 11], створює для цього придатну рамку: річний горизонт дозволяє співвіднести захід із бюджетним роком, тоді як багаторічний план такої прив'язки не має.

Третім рішенням є запровадження індикаторів безпосередньо в тексті планових документів. Чинна практика щорічного планування вже містить придатну для цього форму, оскільки річний план за своєю будовою передбачає визначення очікуваного результату кожного заходу [10; 11]. Принципово, що індикатор має фіксувати не факт дії, а стан: не «розроблено методу», а «частка суб'єктів, які застосовують методику». Лише за такої побудови звітність перестає описувати власний перебіг і починає вимірювати предмет.

Технологічні рішення

Технологічний зріз охоплює державні рішення, що забезпечують виявлення, обмін відомостями й реагування: національні платформи виявлення, центри реагування, канали обміну даними про інциденти та вимоги до засобів захисту.

Характерний розрив цього зрізу полягає в тому, що спроможність описується через наявність засобу, а не через результат його застосування. Створення центру, запровадження платформи чи придбання системи фіксуються як виконаний захід, тоді як питання про те, чи скоротився завдяки цьому час виявлення й реагування, у звітності зазвичай не ставиться.

Першим технологічним рішенням є запровадження показників, що вимірюють результат, а не наявність. Для цього зрізу придатними є часові показники: проміжок між появою ознаки інциденту та його виявленням, між виявленням і початком реагування, між реагуванням і відновленням. Їх перевага полягає в

тому, що вони зберігають визначеність навіть тоді, коли конкретний тип загрози спостерігається вперше, а отже, статистики щодо нього немає. Це властивість, істотна саме в умовах поширення ІІІ, коли кваліфікаційний поріг здійснення складних операцій знижується стрибкоподібно, а історична частота втрачає прогностичну силу. Потреба в механізмі, придатному для середовища, «у якому швидкість технологічних змін перевищує швидкість перегляду нормативних актів» [3, с. 321], обґрунтована автором раніше. Схожа закономірність простежується і в наданні публічних послуг: як зазначено в попередньому дослідженні автора, «нинішня практика публічного управління випереджає нормативно-правове регулювання» [6, с. 22].

Другим рішенням є побудова обміну відомостями про інциденти як технологічного, а не лише організаційного процесу. Цінність таких відомостей швидко спадає, і за скорочення циклу підготовки атаки це спадання прискорюється; відповідно, обмін, що здійснюється через узгодження документів, втрачає сенс незалежно від якості самих документів.

Третім рішенням є забезпечення зіставності. Якщо різні суб'єкти описують однакові події в різних термінах, зведення відомостей не дає картини: воно дає суму описів. Функціональна рамка, що виокремлює врядування як самостійну функцію поряд із ідентифікацією, захистом, виявленням, реагуванням і відновленням [20], придатна тут як спільна мова опису, у якій може бути виражений стан різних систем.

Водночас слід назвати обмеження технологічного зрізу. Моделі зрілості, що є основним інструментом вимірювання спроможностей, мають характерну ваду: вони добре описують наявний стан, але слабо пов'язують його з конкретними управлінськими рішеннями, потрібними для переходу на вищий рівень [19]. Тобто вимірювання саме собою не вказує на пряму дію, і без інституційного та нормативного зрізів технологічний залишається діагностичним інструментом без продовження.

Зіставлення трьох зрізів за типом розриву та інструментом його усунення наведено в табл. 1.

Таблиця 1.

Зрізи реалізації стратегії інформаційної безпеки: типи розривів та інструменти їх усунення

Зріз	Характерний розрив	Інструмент усунення	Суб'єкт, у чий компетенції рішення
Інституційний	Кількість виконавців перевищує спроможність узгодження їхніх дій	Координація як функція: єдині вимоги до звітності, ініціювання перегляду, винесення невиконання на рівень рішення	Кабінет Міністрів України; апарат Ради національної безпеки і оборони України
Нормативний	Стратегія не створює обов'язків, план не поширюється на суб'єктів поза системою органів влади	Доведення положень до приписових вимог підзаконними актами; синхронізація з бюджетним циклом	Кабінет Міністрів України; Адміністрація Держспецзв'язку; секторальні органи
Технологічний	Спроможність описується через наявність засобів, а не через вимірюваний результат їх застосування	Перехід від обліку засобів до вимірювання спроможностей через показники стану	Адміністрація Держспецзв'язку; оператори систем

Джерело: складено автором

Зчеплення трьох рівнів через спільний індикатор

Викладене дозволяє сформулювати конструкцію, що пов'язує три зрізи. Її зміст полягає в тому, що стратегічна ціль, операційний захід і технологічна спроможність мають бути зчеплені спільним індикатором, який вимірює стан, а не дію.

Практично це означає таку послідовність. Стратегічна ціль формулюється як бажаний стан із визначеним показником. Операційний план визначає заходи, кожен з яких прив'язаний до цього самого показника, а не до власного показника виконання. Технологічний рівень забезпечує фактичне вимірювання показника. Звітвання відбувається за показником стану, а відомості про виконані заходи є допоміжними й пояснюють динаміку показника, а не замінюють її.

Перевага конструкції полягає в тому, що вона робить видимою ситуацію, за якої заходи виконано, а стан не змінився. У чинній побудові така ситуація не виявляється взагалі, оскільки звітність не містить величини, яка могла б її відобразити. Зіставлення чинної та запропонованої побудов наведено в табл. 2.

Таблиця 2.

Зіставлення чинної та запропонованої побудови звітування про реалізацію стратегії

Елемент	Чинна побудова	Запропонована побудова
Одиниця звітування	Захід плану	Показник стану, до якого прив'язано заходи
Відповідь на питання «чи виконано»	Так, якщо дію вчинено	Так, якщо показник досяг визначеного значення
Виявлення ситуації «заходи виконано, стан не змінився»	Неможливе: величини для відображення немає	Можливе: фіксується розбіжність між виконанням і показником
Підстава для коригування плану	Невиконання заходу	Відсутність руху показника за виконаних заходів
Роль технологічного рівня	Об'єкт заходів (створити, запровадити)	Джерело вимірювання показника

Джерело: складено автором

Ми вбачаємо такі можливі обмеження запропонованої конструкції з огляду на наявний стан системи. Вона потребує показників, яких наразі немає, і їх розроблення є самостійним завданням, що не зводиться до вибору з наявних переліків. Вона також зміщує навантаження на той рівень, що має найменшу спроможність: фактичне вимірювання здійснюють оператори систем, і без методичної підтримки з боку держави вимога вимірювати перетвориться на вимогу звітувати про вимірювання. Нарешті, конструкція не усуває політичної природи вибору цілей: вона робить видимим результат, але не визначає, який результат є достатнім.

З огляду на це доцільно розглянути два можливі варіанти дій і пов'язані з кожним ризики.

Перший варіант полягає у збереженні наявної побудови звітування за заходами. Його перевагою в умовах воєнного стану є простота: він дозволяє швидко фіксувати виконану роботу й не потребує вимірювального апарату, а ресурси спрямовуються на невідкладні завдання. Ризик цього варіанта полягає в тому, що система не отримує сигналу про напрями, де заходи виконуються, а стан не змінюється. Опосередкованим свідченням реалізації такого ризику є зафіксований в огляді розрив «між встановленими законодавчими обов'язками щодо повідомлення про інциденти та наявними практичними інструментами їх реалізації» [8, с. 11], що співіснує з високими показниками виконання за більшістю напрямів.

Другий варіант передбачає поетапне запровадження показників стану, починаючи з напрямів, де вимірювання є технічно найпростішим, зокрема з часових показників виявлення та реагування. Його ризиком є додаткове навантаження на операторів систем у період, коли їхні ресурси обмежені, а також імовірність того, що на початковому етапі показники вимірюватимуться нерівномірно й даватимуть неповну картину.

Зіставлення двох варіантів показує, що вибір між ними не зводиться до переваг одного з них: перший є дешевшим у впровадженні, другий – інформативнішим в управлінні. Проміжним рішенням, що зменшує ризики обох, є збереження чинної звітності за заходами з паралельним запровадженням обмеженого переліку показників стану на окремих напрямках, що дозволяє накопичити вимірювальний досвід без одномоментної перебудови всієї системи.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ **I ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ**

Реалізація державної стратегії інформаційної безпеки залежить не лише від обсягу спрямованих ресурсів, а передусім від того, чи існує перехід між мовою цілей і мовою виконання. Проведений аналіз дає підстави для таких висновків.

Розрив між стратегічним задумом і фактичним результатом має структурну, а не ресурсну природу. Стратегія формулює цілі в категоріях стану, звітність фіксує виконання в категоріях дії, а припущення про зв'язок між дією та зміною стану в жодному документі не перевіряється. Наслідком є те, що агрегований показник виконання не є показником захищеності: зростання з 32 % до 86 % фіксує рух плану, а не пропорційне зростання рівня захищеності, тоді як напрям із показником 23 % є інформативнішим, оскільки вказує місце, де руху немає.

Шляхи реалізації стратегії доцільно розглядати у трьох зрізах, кожен з яких має власний тип розриву: інституційний, де кількість виконавців перевищує спроможність узгодження; нормативний, де стратегія не створює обов'язків, а план не поширюється на суб'єктів поза системою органів влади; технологічний, де спроможність описується через наявність засобу, а не через результат його застосування. Для кожного визначено інструмент усунення та суб'єкта, у чий компетенції перебуває рішення.

Ключовою умовою результативності є перехід від звітування про заходи до вимірювання спроможностей через зчеплення стратегічної цілі, операційного заходу й технологічної спроможності спільним показником стану. Придатною рамкою для такого переходу є щорічні операційні плани, за умови, що визначені в них індикатори фіксуватимуть стан, а не факт дії.

Наукова новизна полягає в обґрунтуванні структурної природи розриву між стратегією та її реалізацією й у розробленні трирівневої конструкції зчеплення документів через спільний показник стану, що дозволяє виявляти ситуацію, за якої заходи виконано, а стан не змінився, – ситуацію, яку чинна побудова звітності не фіксує в принципі.

Одержані результати можуть бути застосовані безпосередньо в роботі над операційними планами з реалізації стратегічних документів у сфері інформаційної безпеки – передусім на тій стадії, коли визначаються індикатори, а також при формуванні вимог до змісту звітних відомостей.

Перспективи подальших досліджень пов'язані з розробленням переліку показників стану для окремих напрямів інформаційної безпеки, із визначенням джерел їх вимірювання та періодичності, а також з емпіричною перевіркою запропонованої конструкції на матеріалі річної звітності про виконання планів заходів.

Література

1. Бойко О. Державна політика та державне управління у сфері захисту критичної інфраструктури. Науковий вісник: Державне управління. 2024. № 2(16). С. 137–156. DOI: [https://doi.org/10.32689/2618-0065-2024-2\(16\)-137-156](https://doi.org/10.32689/2618-0065-2024-2(16)-137-156)

2. Бурдяк П., Спесивцева О., Онищенко В., Митрофанова В. Стратегія інформаційної безпеки 2021–2025 років: оцінка реалізації. Київ : Центр демократії та верховенства права, 2026. URL: <https://cedem.org.ua/library/strategy-infobezpeky-otsinka/>
3. Гавриленко Ю. Концептуальна модель системи державного управління інформаційною безпекою в умовах поширення штучного інтелекту. Аспекти публічного управління. 2026. Т. 14, № 3. С. 314–323. DOI: <https://doi.org/10.15421/152643>
4. Гавриленко Ю. Трансформація сучасної війни: як інформаційні технології змінюють моделі публічного управління. Herald of Khmelnytskyi National University. Economic Sciences. 2026. Т. 356, № 4. С. 139–145. DOI: <https://doi.org/10.31891/2307-5740-2026-356-20>
5. Гавриленко Ю. В. Моделі державного управління у сфері інформаційної безпеки та регулювання штучного інтелекту: порівняльний аналіз. Публічне урядування. 2026. № 2(47). С. 23–31. DOI: [https://doi.org/10.32689/3083-774X-2026-2\(47\)-3](https://doi.org/10.32689/3083-774X-2026-2(47)-3)
6. Гавриленко Ю. В. Ризики та перспективи використання штучного інтелекту у системі надання публічних послуг в Україні під час воєнного стану. Сучасний науковий журнал. 2025. № 10(4). С. 20–27. DOI: <https://doi.org/10.36994/2786-9008-2025-10-2>
7. Герасименко О. М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 84, ч. 3. С. 257–263. DOI: <https://doi.org/10.24144/2307-3322.2024.84.3.39>
8. Огляд національної системи кібербезпеки України 2025 : аналітичне дослідження / Національний координаційний центр кібербезпеки при РНБО України. Київ, 2026. URL: https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf
9. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р. URL: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80>
10. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80>
11. Про затвердження плану заходів на 2026 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 24.06.2026 № 631-р. URL: <https://zakon.rada.gov.ua/laws/show/631-2026-%D1%80>
12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021>
14. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021>
15. Річний аналітичний звіт щодо реалізації Стратегії інформаційної безпеки за 2024 рік. Київ : Міністерство культури України, 2025. URL: <https://mincult.gov.ua/wp-content/uploads/2025/11/zvit-uzagalnenyj-2.pdf>
16. Шкуропадська Д., Лебедева Л., Гонсалвес Ж. Інституційне забезпечення стійкості критичної інфраструктури ЄС, НАТО та України. Scientia fructuosa. 2025. Т. 159, № 1. С. 45–60. DOI: [https://doi.org/10.31617/1.2025\(159\)03](https://doi.org/10.31617/1.2025(159)03)
17. Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy : Report GAO-24-106916. Washington, DC : U.S. Government Accountability Office, 2024. URL: <https://www.gao.gov/products/gao-24-106916>
18. Heiding F., O'Neill A., Price L. Cybersecurity Strategy Scorecard. Cambridge, MA : Belfer Center for Science and International Affairs, Harvard Kennedy School, 2025. URL: <https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard>
19. Liyanage L., Gamagedara Arachchilage N. A., Russello G. SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv preprint. 2024. arXiv:2408.16140. DOI: <https://doi.org/10.48550/arXiv.2408.16140>
20. The NIST Cybersecurity Framework (CSF) 2.0 : NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: <https://doi.org/10.6028/NIST.CSWP.29> URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

References

1. Boiko, O. (2024), “State policy and public administration in the field of critical infrastructure protection”, Naukovyi visnyk: Derzhavne upravlinnia, No. 2(16), pp. 137–156, DOI: [https://doi.org/10.32689/2618-0065-2024-2\(16\)-137-156](https://doi.org/10.32689/2618-0065-2024-2(16)-137-156) [in Ukrainian].

2. Burdiak, P., Spesyvtseva, O., Onyshchenko, V. and Mytrofanova, V. (2026), Stratehiia informatsiinoi bezpeky 2021–2025 rokiv: otsinka realizatsii [Information Security Strategy 2021–2025: assessment of implementation], Centre for Democracy and Rule of Law, Kyiv, available at: <https://cedem.org.ua/library/strategiya-infobezpeky-otsinka/> [in Ukrainian].
3. Havrylecho, Yu. (2026), “Conceptual model of the system of public administration of information security under the proliferation of artificial intelligence”, *Aspekty publichnogo upravlinnia*, Vol. 14, No. 3, pp. 314–323, DOI: <https://doi.org/10.15421/152643> [in Ukrainian].
4. Havrylecho, Yu. (2026), “Transforming modern warfare: how information technology is changing public administration models”, *Herald of Khmelnytskyi National University. Economic Sciences*, Vol. 356, No. 4, pp. 139–145, DOI: <https://doi.org/10.31891/2307-5740-2026-356-20> [in Ukrainian].
5. Havrylecho, Yu. V. (2026), “Models of public administration in the field of information security and artificial intelligence regulation: a comparative analysis”, *Publichne uriaduvannia*, No. 2(47), pp. 23–31, DOI: [https://doi.org/10.32689/3083-774X-2026-2\(47\)-3](https://doi.org/10.32689/3083-774X-2026-2(47)-3) [in Ukrainian].
6. Havrylecho, Yu. V. (2025), “Risks and prospects of using artificial intelligence in the public services delivery system in Ukraine during martial law”, *Suchasnyi naukovi zhurnal*, No. 10(4), pp. 20–27, DOI: <https://doi.org/10.36994/2786-9008-2025-10-2> [in Ukrainian].
7. Herasymenko, O. M. (2024), “Threats to critical infrastructure facilities of Ukraine under martial law”, *Naukovi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya: Pravo*, Issue 84, part 3, pp. 257–263, DOI: <https://doi.org/10.24144/2307-3322.2024.84.3.39> [in Ukrainian].
8. National Cybersecurity Coordination Center under the National Security and Defence Council of Ukraine (2026), *Ohiad natsionalnoi systemy kiberbezpeky Ukrainy 2025: analitichne doslidzhennia* [Review of the national cybersecurity system of Ukraine 2025: analytical study], Kyiv, available at: https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf [in Ukrainian].
9. Cabinet of Ministers of Ukraine (2023), *Pro zatverdzhennia planu zakhodiv z realizatsii Stratehii informatsiinoi bezpeky na period do 2025 roku* [On approval of the action plan for implementing the Information Security Strategy for the period up to 2025], Order No. 272-r of 30.03.2023, available at: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80> [in Ukrainian].
10. Cabinet of Ministers of Ukraine (2025), *Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy* [On approval of the 2025 action plan for implementing the Cybersecurity Strategy of Ukraine], Order No. 204-r of 07.03.2025, available at: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80> [in Ukrainian].
11. Cabinet of Ministers of Ukraine (2026), *Pro zatverdzhennia planu zakhodiv na 2026 rik z realizatsii Stratehii kiberbezpeky Ukrainy* [On approval of the 2026 action plan for implementing the Cybersecurity Strategy of Ukraine], Order No. 631-r of 24.06.2026, available at: <https://zakon.rada.gov.ua/laws/show/631-2026-%D1%80> [in Ukrainian].
12. Verkhovna Rada of Ukraine (2017), *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* [On the basic principles of ensuring cybersecurity of Ukraine], Law No. 2163-VIII of 05.10.2017, available at: <https://zakon.rada.gov.ua/laws/show/2163-19> [in Ukrainian].
13. President of Ukraine (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku “Pro Stratehiu kiberbezpeky Ukrainy”* [On the decision of the National Security and Defence Council of Ukraine of 14 May 2021 “On the Cybersecurity Strategy of Ukraine”], Decree No. 447/2021 of 26.08.2021, available at: <https://zakon.rada.gov.ua/laws/show/447/2021> [in Ukrainian].
14. President of Ukraine (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku “Pro Stratehiu informatsiinoi bezpeky”* [On the decision of the National Security and Defence Council of Ukraine of 15 October 2021 “On the Information Security Strategy”], Decree No. 685/2021 of 28.12.2021, available at: <https://zakon.rada.gov.ua/laws/show/685/2021> [in Ukrainian].
15. Ministry of Culture of Ukraine (2025), *Richnyi analitichnyi zvit shchodo realizatsii Stratehii informatsiinoi bezpeky za 2024 rik* [Annual analytical report on the implementation of the Information Security Strategy for 2024], Kyiv, available at: <https://mincult.gov.ua/wp-content/uploads/2025/11/zvit-uzagalnenvi-2.pdf> [in Ukrainian].
16. Shkuropadska, D., Lebedeva, L. and Gonçalves, J. (2025), “Institutional provision of critical infrastructure resilience of the EU, NATO and Ukraine”, *Scientia fructuosa*, Vol. 159, No. 1, pp. 45–60, DOI: [https://doi.org/10.31617/1.2025\(159\)03](https://doi.org/10.31617/1.2025(159)03) [in Ukrainian].
17. U.S. Government Accountability Office (2024), *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*, Report GAO-24-106916, Washington, DC, available at: <https://www.gao.gov/products/gao-24-106916>
18. Heiding, F., O'Neill, A. and Price, L. (2025), *Cybersecurity Strategy Scorecard*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, available at: <https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard>
19. Liyanage, L., Gamagedara Arachchilage, N. A. and Russello, G. (2024), “SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)”, arXiv preprint, arXiv:2408.16140, DOI: <https://doi.org/10.48550/arXiv.2408.16140>
20. National Institute of Standards and Technology (2024), *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Gaithersburg, MD, DOI: <https://doi.org/10.6028/NIST.CSWP.29> available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>