УДК 004.056:351.862.4(477)
DOI: 10.31673/2409-7292.2025.032375

Шульга В.П., Корченко О.Г., Іванченко Є.В., Казмірчук С.В., Кондратюк С.В.

КРИТЕРІЇ СТРАТЕГІЧНОГО ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ: КІБЕРДИПЛОМАТИЧНИЙ АСПЕКТ

Для України, яка перебуває у стані збройної агресії та системного тиску у кіберпросторі, питання кіберзахисту набуває критичного значення, особливо у контексті інтеграції до європейського та євроатлантичного безпекового простору. Це вимагає не лише технологічної готовності до відбиття атак, а й створення стійкої, комплексної системи кіберзахисту, здатної ефективно взаємодіяти з міжнародними партнерами та інтегруватися у глобальний безпековий простір. У цьому контексті важливим забарвленням цієї системи стає кібердипломатичний аспект. Реалізація ефективної кібердипломатії потребує чітких інструментів моніторингу та оцінювання стану кіберзахисту країни, щоб: визначати сильні та слабкі сторони національної кібербезпеки; коригувати політики та програми розвитку; забезпечувати прозорість і підзвітність перед суспільством та міжнародними партнерами тощо. З огляду на це виникає потреба у розробці адаптованих до українських реалій відповідних критеріїв оцінювання складових кібердипломатії, що поєднують найкращі світові практики з урахуванням сучасних унікальних викликів державі. Метою даного дослідження є формування критеріїв для оцінюван-ня кібербезпеки країни в рамках складових стратегії кібердипломатії з використанням найкращих світових рактик. Для формування таких критеріїв на початковому етапі дослідження проведемо аналіз міжнародних визнаних підходів, розроблених урядами, міждержавними організаціями та галузевими експертами. Сформована множина з 11 критеріїв, за якими можна здійснити оцінювання рівня кібербезпеки України у межах реалізації стратегії кібердипломатії мають достатній рівень деталізації, який дозволяє: комплексно оцінювати стан кіберзахисту за широким спектром напрямів; ефективно планувати розвиток інституційних, технологічних та правових механізмів; зміцнювати позиції України у кіберпросторі.

Ключові слова: кібердипломатія, кібербезпека, критерії стратегічного оцінювання кібербезпеки держави, кіберзахист держави, кіберзагрози.

Вступ

У сучасних умовах глобальної цифровізації, швидкого розвитку інформаційно-комунікаційних технологій та зростання масштабності кіберзагроз, кібербезпека стала одним із ключових елементів національної безпеки. За даними міжнародних аналітичних центрів, кібератаки все частіше використовуються не лише як інструмент економічного чи політичного тиску, але й як невід'ємна складова гібридних війн та засіб впливу на внутрішню стабільність держав. Для України, яка перебуває у стані збройної агресії та системного кібертиску, питання кіберзахисту набуває критичного значення, особливо у контексті інтеграції до європейського та євроатлантичного безпекового простору. Український досвід останніх років засвідчив, що атаки на цифрову інфраструктуру, державні інформаційні ресурси та приватний сектор відбуваються систематично та в координації з інформаційними і психологічними впливами. Це вимагає не лише технологічної готовності до відбиття атак, а й створення стійкої, комплексної системи кіберзахисту, здатної ефективно взаємодіяти з міжнародними партнерами та інтегруватися у глобальний безпековий простір.

Важливою складовою цієї системи є кібердипломатія – цілеспрямована діяльність держави у міжнародному цифровому просторі, спрямована на захист національних інтересів, просування власних ініціатив у сфері кібербезпеки та формування коаліцій для протидії кіберзагрозам. Реалізація ефективної кібердипломатії потребує чітких інструментів моніторингу та оцінювання стану кіберзахисту країни, щоб: визначати сильні та слабкі сторони національної кібербезпеки; коригувати політики та програми розвитку; забезпечувати прозорість і підзвітність перед суспільством та міжнародними партнерами тощо.

Аналіз останніх досліджень і публікацій

Міжнародна практика пропонує низку підходів до оцінювання рівня кібербезпеки держав, серед яких Global Cybersecurity Index (GCI) [1], Network and Information Security Directive 2 (NIS2 Directive) [2], EU Cybersecurity Strategy [3], OECD Digital Security Risk Management Framework [4] тощо. Ці підходи включають від п'яти до восьми ключових

напрямів, охоплюючи правові, організаційні, технічні, кадрові та міжнародні аспекти. Проте їхня структура є орієнтованою на країни зі стабільною безпековою ситуацією та не завжди враховує специфіку держав, які перебувають у стані гібридної війни. Україна є унікальним прикладом держави, яка водночас: перебуває під постійними масштабними кібератаками; змушена вибудовувати кіберзахист у тісній координації з міжнародними партнерами; потребує активної кібердипломатії для зміцнення власних позицій на міжнародній арені; має розвивати кадровий, технологічний та інституційний та інший потенціал в умовах обмежених ресурсів. Їх ефективний розподіл для забезпечення активної кібердипломатії безпосередньо пов'язаний з оцінюванням її стану за певними складовими. З огляду на це виникає потреба у розробці адаптованих до українських реалій відповідних критеріїв оцінювання складових кібердипломатії, що поєднують найкращі світові практики з урахуванням сучасних унікальних викликів державі.

Мета та завдання дослідження

Отже, метою даного дослідження є формування критеріїв для оцінювання кібербезпеки країни в рамках складових стратегії кібердипломатії з використанням найкращих світових практик.

Основна частина

Для формування таких критеріїв на початковому етапі дослідження проведемо аналіз міжнародних визнаних підходів, розроблених урядами, міждержавними організаціями та галузевими експертами. Їх головна мета – надати універсальний інструмент для порівняння стану кібербезпеки між країнами, визначення пріоритетів політики та підвищення рівня безпеки у цифровому довкіллі.

1. GCI глобальний індекс кібербезпеки [1]. Розробник Міжнародний союз електрозв’язку (International Telecommunication Union, ITU). Перший випуск – 2014 року, оновлення версій – 2017, 2020, 2024. GCI надійним орієнтиром, який вимірює рівень зобов’язань країн щодо кібербезпеки на глобальному рівні з метою підвищення обізнаності про важливість та різні виміри цієї проблематики.

Таблиця 1

Напрямки оцінювання GCI

Напрям	Опис	Приклади індикаторів
1. Правова база.	Оцінка законів та нормативних актів щодо кіберзлочинності та кібербезпеки.	У країнах існував принаймні один чинний або розглядуваний нормативний акт щодо захисту персональних даних, захисту конфіденційності або повідомлення про порушення. Країни з чинними правилами захисту даних. Країни з регулюванням критичної інфраструктури.
2. Технічні заходи.	Вимірювання реалізації технічних можливостей через національні та галузеві установи.	Країни з активними CIRT. Країни, що співпрацюють з регіональною асоціацією CIRT. Країни з системами для впровадження стандартів кібербезпеки.
3. Організаційні заходи.	Вимірювання національних стратегій та організацій, що впроваджують кібербезпеку.	Країни з національними стратегіями кібербезпеки. Країни з агентствами з кібербезпеки. Країни, за якими зареєстровано стратегії та ініціативи щодо захисту дітей в Інтернеті.
4. Потенціал нарощування.	Вимірювання інформаційно-просвітницьких кампаній, навчання, освіти та стимулів для розвитку потенціалу в галузі кібербезпеки.	Країни, що здійснюють ініціативи з підвищення обізнаності в галузі кібербезпеки. Країни, де кібербезпека знаходиться на певному рівні національних навчальних програм. Країни зі стимулами для розвитку потенціалу кібербезпеки.
5. Міжнародне співробітництво.	Вимірювання партнерських відносин між агентствами, фірмами та країнами.	Країни, що беруть участь або будуть брати участь у внутрішніх або міжнародних державно-приватних партнерствах у сфері кібербезпеки. Країни з міжнародними угодами про кібербезпеку. Країни, що повідомляють про міжвідомчу співпрацю.

Оскільки кібербезпека має широкий спектр застосувань, що охоплює багато галузей і секторів, рівень розвитку або залученості кожної країни оцінюється за п’ятьма напрямками (див. табл. 1), після чого результати агрегуються в загальний бал.

Використовується якісно-кількісне оцінювання на основі анкетування, аналізу документів і практик. Щоб відобразити результати, ефективність країн вимірюється за п'ятьма рівнями, де 1-й рівень є найвищим, а 5-й – найнижчим. Ці рівні формуються на основі балів, щоб допомогти країнам зрозуміти та визначити свої еталони для наслідування і подальшого покращення. Деталізуємо зазначені рівні.

1. Рівень (Tier) – Role-modelling (95–100 балів) – «Рольова модель». Найвищий рівень розвитку кібербезпеки. Країни-лідери, які демонструють найвищий рівень зрілості в усіх вимірах кібербезпеки. Вони формують глобальні стандарти, мають передові стратегії, високий рівень впровадження політик, інноваційні технології, тісну міжнародну співпрацю та є прикладом для інших.

2. Рівень – Advancing (85–95 балів) – «Просунутий рівень». Держави з дуже високим рівнем розвитку кібербезпеки, які впровадили більшість найкращих практик та стратегій. Країни, які вже мають сформовані базові законодавчі, організаційні та технічні інструменти, але вони ще не є комплексними або не повністю інтегрованими. Пріоритетом є розширення покриття заходів безпеки, підвищення ефективності координації та інвестицій у спроможності.

3. Рівень – Establishing (55–85 балів) – «Становлення». Середній рівень зрілості. Країни, які вже мають сформовані базові законодавчі, організаційні та технічні інструменти, але вони ще не є комплексними або не повністю інтегрованими. Пріоритетом є розширення покриття заходів безпеки, підвищення ефективності координації та інвестицій у спроможності. Україна знаходиться на цьому рівні за даними GCI звіт за 2024 рік [5] (рис. 1).

4. Рівень – Evolving (20–55 балів) – «Еволюція». Початковий етап розвитку системи кібербезпеки. Держави, що перебувають на початкових етапах розвитку кібербезпеки. У них є певні елементи політик або технічних заходів, але відсутня цілісна стратегія чи достатня координація між секторами. Розвиток часто фрагментарний і залежить від зовнішньої допомоги.

5. Рівень – Building (0–20 балів) – «Побудова». Стартовий рівень. Країни, які лише починають будувати систему кібербезпеки. Вони не мають повноцінних законів, організаційних структур та технічних рішень. Потребують значних інвестицій, міжнародної підтримки та створення базової інфраструктури безпеки [1, 5].

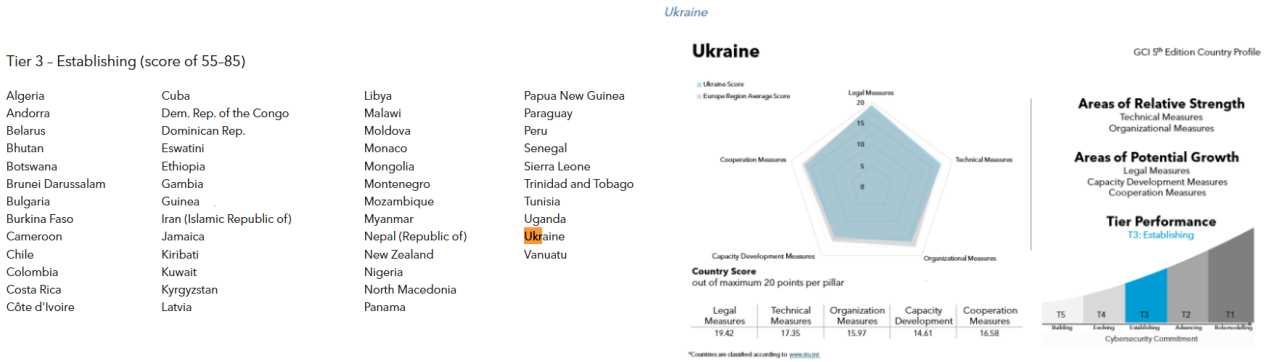

Рис. 1. Результати оцінювання України GCI за 2024 рік

До слабких сторін GCI можна віднести наступне: індикатори часто занадто загальні, не враховують контекст гібридної війни, інформаційних операцій і специфіки країн із високим рівнем зовнішніх загроз.

2. NIS2 Directive [2] та Європейська стратегія кібербезпеки (Cybersecurity Strategy) [3] (NIS2&EU). Розробник Європейський Союз. Офіційно ухвалена Європейським парламентом та Радою ЄС 14 грудня 2022 року, набрала чинності 16 січня 2023 року, з обов'язковим імплементаційним терміном до жовтня 2024 року. Директива NIS2 є ключовим нормативно-правовим актом ЄС, спрямованим на підвищення рівня кіберстійкості держав-членів. Вона розширює сферу дії першої директиви NIS, вводячи жорсткіші вимоги до безпеки мереж і інформаційних систем, а також встановлює чіткі обов'язки для операторів критичної інфраструктури та цифрових постачальників. Європейська стратегія кібербезпеки, вперше оприлюднена Європейською комісією у 2013 році, актуалізована новою редакцією 16 грудня 2020 року («EU Cybersecurity Strategy for the Digital Decade»), доповнює NIS2 на політичному рівні, визначаючи пріоритети, інвестиційні напрями та міжнародну співпрацю в кіберсфері. Структура основних напрямів:

1. Безпека мереж та інформаційних систем – стандарти захисту, резервування та моніторинг;
2. Управління інцидентами – обов'язкове повідомлення про інциденти, створення внутрішніх планів реагування;
3. Захист критичної інфраструктури – включення енергетики, транспорту, охорони здоров'я, фінансів та інших ключових секторів;
4. Обмін інформацією – між державами-членами та з органами ЄС (ENISA, CERT-EU);
5. Сертифікація продуктів і послуг – впровадження європейської схеми сертифікації кібербезпеки;
6. Кібергігієна та підготовка кадрів – навчальні програми, стандарти мінімальної безпеки для організацій.

Ці нормативні документ впроваджують уніфікацію підходів до кібербезпеки у всіх державах ЄС, є обов'язковими вимогами до держав та операторів критичної інфраструктури (передбачені штрафи за невиконання). Також вони регламентують централізований моніторинг виконання через національні компетентні органи та Європейську агенцію з кібербезпеки (ENISA) [2, 3].

Слабкими сторонами цих підходів є: орієнтація на внутрішній ринок ЄС (країни поза ЄС можуть запровадити аналогічні вимоги лише добровільно); вузьке охоплення деяких аспектів (цифрова дипломатія, міжнародний імідж та просування власних позицій у глобальному кіберпросторі прямо не входять до обов'язкових положень); можлива складність адаптації для країн з нижчим рівнем інституційної готовності.

3. National Cyber Security Index (NCSI) [6]. Рік запуску: 2016. Розробник e-Governance Academy (Естонія). Національний індекс кібербезпеки – це глобальний індекс режиму реального часу, який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами. NCSI також є базою даних із загальнодоступними доказовими матеріалами та інструментом для нарощування національного потенціалу у сфері кібербезпеки [6]. NCSI організовано за категоріями, спроможностями та індикаторами і має: 3 категорії ідентифікаторів; 12 ідентифікаторів. Рейтинги країн базуються на таких публічних даних, як правові акти, офіційна документація, веб сайти. Використовуються наступні категорії ідентифікаторів: 1. Стратегічні індикатори (Strategic Cybersecurity Indicators) – показують, наскільки в країні розвинені державна політика, міжнародна співпраця, освіта та наука у сфері кібербезпеки; 2. Превентивні індикатори (Preventive Cybersecurity Indicators) – оцінюють здатність країни попереджати кіберзагрози (захист критичної інфраструктури та цифрових технологій, збір і аналіз інформації про загрози, а також захист персональних даних); 3. Індикатори реагування (Responsive Cybersecurity Indicators) – вимірюють готовність країни виявляти, розслідувати та нейтралізувати кіберінциденти, управляти кризами, боротися з кіберзлочинністю та захищатися у військовій кіберсфері.

Безпосередньо кожна категорія характеризується низкою ідентифікаторів.

Категорія 1. Стратегічні індикатори кібербезпеки:

1. Політика кібербезпеки (Cybersecurity policy) – наявність та якість національної стратегії кібербезпеки, законодавства, нормативних документів та планів дій.

2. Глобальний внесок у кібербезпеку (Global cybersecurity contribution) – участь держави у міжнародних угодах, конвенціях та ініціативах з кібербезпеки.

3. Освіта та професійний розвиток (Education and professional development) – програми підготовки кадрів, курси, академічні програми та підвищення кваліфікації у сфері кібербезпеки.

4. Кібербезпекові дослідження та розробки (Cybersecurity research and development) – наукові дослідження, інноваційні проекти, підтримка R&D у галузі кібербезпеки.

Категорія 2. Превентивні індикатори кібербезпеки:

5. Кібербезпека критичної інформаційної інфраструктури (Cybersecurity of critical information infrastructure) – захист енергетичних систем, транспорту, зв'язку, фінансового сектору тощо від кіберзагроз.

6. Кібербезпека цифрових рушіїв (Cybersecurity of digital enablers) – безпека електронного уряду, електронних сервісів, хмарних технологій та IoT.

7. Аналіз кіберзагроз та підвищення обізнаності (Cyber threat analysis and awareness raising) – системи моніторингу загроз, кіберрозвідка, програми навчання населення та бізнесу.

8. Захист персональних даних (Protection of personal data) – законодавство та практична реалізація захисту даних громадян, регуляторні органи, контроль і санкції.

Категорія 3. Індикатори реагування на кіберінциденти:

9. Реагування на кіберінциденти (Cyber incident response) – наявність та ефективність CERT/CSIRT, процеси реагування, інструменти й ресурси.

10. Управління кіберкризами (Cyber crisis management) – координація під час масштабних кібератак, планування та взаємодія між структурами.

11. Боротьба з кіберзлочинністю (Cyber crisis management) – законодавство, кіберполіція, розслідування, міжнародна співпраця у сфері кіберзлочинів.

12. Військова кібероборона (Military cyber defence) – спроможності з кіберзахисту в збройних силах, кібероперації у воєнній сфері.

В зазначеному контексті ідентифікаторами є конкретні вимірювані параметри (наявність законів, робота CERT, міжнародні угоди тощо), які оцінюються як "ТАК/НІ" з підтвердженням офіційними джерелами [6].

Оцінка базується на формальній наявності документів, структур і механізмів, але не вимірюється ефективність у режимі реального часу. Кожен показник має певну кількість балів, які сумуються у загальний індекс (0–100) (див. рис.2).

Слабкі сторони такого підходу є:

– фокус на формальній наявності, а не на ефективності – індекс оцінює, чи існує закон, стратегія або орган, але не перевіряє, наскільки вони реально працюють або забезпечують результативність. Це може створювати завищену оцінку для країн, де документи формально ухвалені, але не виконуються;

– обмежене охоплення кібердипломатії та міжнародного іміджу – хоча враховується участь у міжнародних угодах, глибокий аналіз ролі держави в розробці глобальних норм або у формуванні політики кіберпростору відсутній;

– недостатня увага до інформаційної стійкості та протидії дезінформації – основний акцент зроблено на технічній і правовій базі, але не на соціально-комунікаційних аспектах, що є критичними у сучасних гібридних загрозах;

– відсутність детальної оцінки підготовки кадрів – питання освіти, сертифікації та розвитку людського капіталу в кіберсфері розглянуті лише загально, без чітких індикаторів рівня кваліфікації;

– не оцінюється інвестиційний та інноваційний потенціал – поза увагою залишаються державні та приватні програми фінансування нових технологій у сфері кіберзахисту;

– мала гнучкість у відображенні національної специфіки – усі країни оцінюються за єдиною схемою, без урахування особливостей геополітичних ризиків чи специфіки економіки.

– слабкий зв'язок із практичними показниками кіберінцидентів – індекс не інтегрує статистику атак, успішності відбиття загроз або швидкості реагування в реальних умовах.

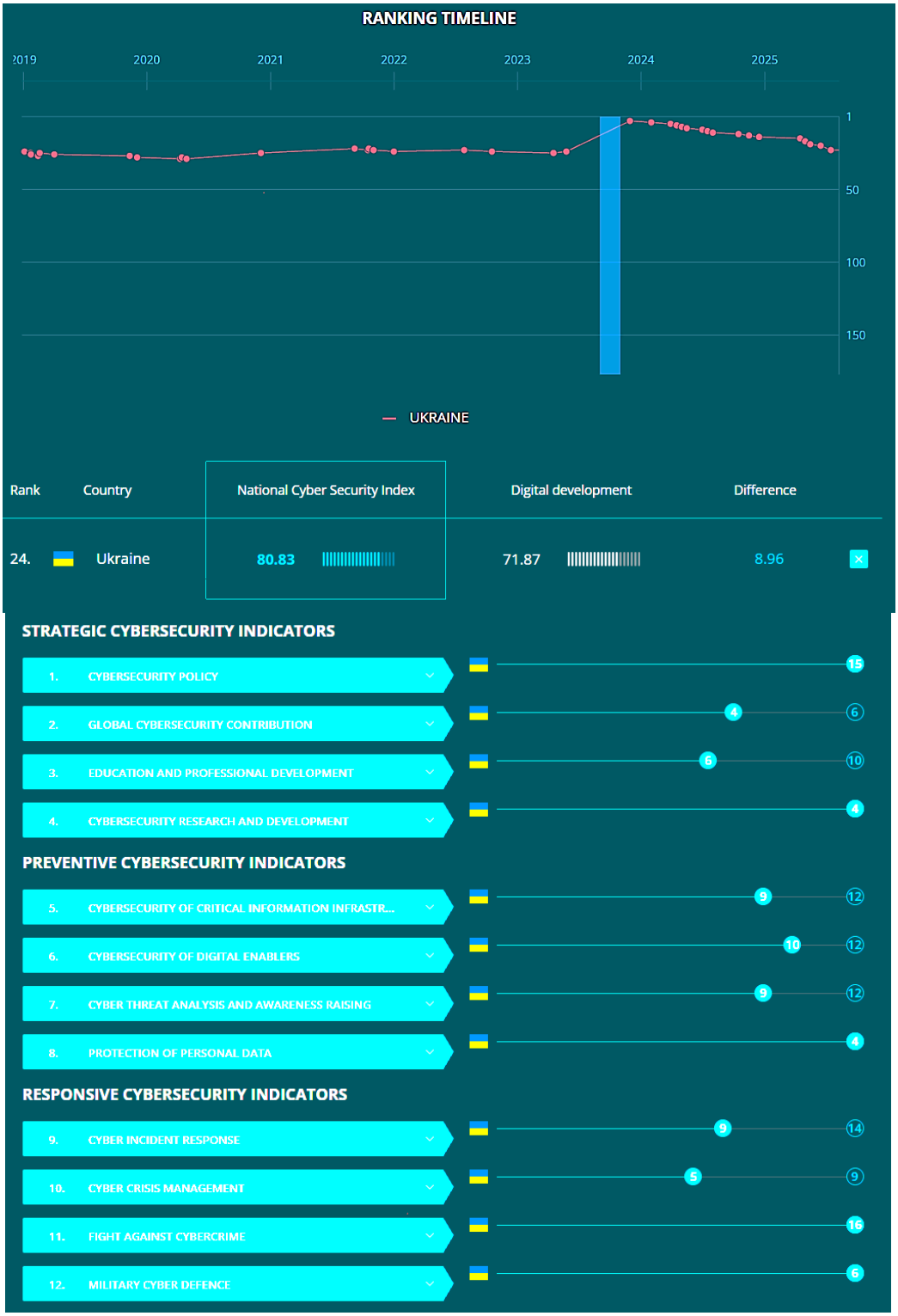

Рис. 2 Оцінка України NCSI за 2024 рік

4. OECD (Organisation for Economic Co-operation and Development) фреймворк управління ризиками цифрової безпеки (Digital Security Risk Management Framework) [4]. Рік розробки 2015, остання модернізація 2022р. Розробник Організація економічного співробітництва та розвитку (OECD). Це концептуальна основа, що пропонує високорівневі принципи для керування кіберризиками з урахуванням економічних і соціальних наслідків інцидентів. На відміну від суто технічного підходу, цей фреймворк наголошує, що цифрові інциденти впливають не лише на IT-системи, але й можуть мати суттєві бізнес- та суспільні наслідки (наприклад, атаки на лікарні створюють ризики для життя, витоки бізнес інформації шкодять конкурентоспроможності). Відповідно, кібербезпека розглядається як питання управління ризиками на рівні організації та держави, а не тільки як технічна проблема. OECD закликає організації запровадити управління цифровими ризиками як безперервний цикл: оцінювати ризики, визначати стратегії поводження з ними (прийняття, зменшення, уникнення чи передача ризику) та впроваджувати заходи безпеки, що забезпечують стійкість, але не гальмують розвиток.

Фреймворк містить набір із кількох ключових компонентів та рекомендацій. По-перше, він формулює принципи управління цифровою безпекою – загальні та операційні – які мають слугувати орієнтиром для всіх зацікавлених сторін. По-друге, на основі цих принципів надаються рекомендації щодо розроблення національної стратегії кібербезпеки та створення культури цифрової безпеки в суспільстві. Фреймворк організовано на 4-х рівнях: 1. Фундаментальний – описує базові принципи кібербезпеки для процвітання (включно з нижченаведеними принципами ризик-менеджменту); 2. Стратегічний – присвячений розбудові культури цифрової безпеки і національним стратегіям; 3. Ринковий – охоплює безпеку критичних активів та IT-продуктів; 4. Технічний – описує питання управління технічними уразливостями. Основою всієї конструкції є саме принципи управління цифровими ризиками, які далі деталізуються на стратегічному та інших рівнях.

OECD-фреймворк цифрової безпеки має переважно якісно-процесний характер. Він не задає конкретних числових метрик або суворих стандартів, натомість пропонує принципи та процеси для впровадження належного управління ризиками. Це принципово відрізняється від технічних стандартів (як-от, наприклад, стандартів ISO/IEC [7-10] чи фреймворків таких як NIST CSF[11]) – OECD-фреймворк орієнтований на політиків і управлінців, а не на технічних фахівців. Він описує структурну модель у вигляді набору принципів (критеріїв), дотримання яких свідчить про зрілість системи цифрової безпеки. Модель є процесною, оскільки акцентує цикл оцінки та обробки ризику і безперервне вдосконалення безпеки. Вона також є якісною, бо фокусує увагу на політиках, культурах та процедурах, а не на кількісних показниках. Таким чином, OECD-фреймворк можна розглядати як набір високорівневих критеріїв оцінки та орієнтирів, які кожна держава чи організація деталізує під свої потреби, потенційно доповнюючи власними метриками [4]. Опишемо основні недоліки фреймворку:

– високий рівень абстракції. Документ подає принципи у дуже загальних формулюваннях (наприклад, «забезпечувати баланс між безпекою та економічною вигодою») і не пропонує детальних показників чи метрик, за якими можна виміряти ефективність реалізації. Відсутні конкретні індикатори або стандартизовані ключові показники ефективності (Key Performance Indicators (KPI)) для оцінювання рівня цифрової безпеки;

– невизначеність у вимогах до реалізації. У фреймворку не прописано чітких процедур чи етапів впровадження політик. Рекомендації носять характер «найкращих практик», але не дають покрокових інструкцій, що ускладнює практичне застосування в державному чи корпоративному довкіллі;

– відсутність прив’язки до національних або міжнародних нормативів. Фреймворк описує принципи, підходи та етапи управління цифровими ризиками, але не містить чіткої «мапи відповідності» (mapping) до вимог конкретних міжнародних або національних стандартів і регуляцій. Він подає загальні принципи, але не показує, як ці принципи

© Шульга В.П., Корченко О.Г., Іванченко Є.В., Казмірчук С.В., Кондратюк С.В. (2025) Критерії стратегічного оцінювання кібербезпеки держави: кібердипломатичний аспект. Сучасний захист інформації, 3(63), 205–218. https://doi.org/10.31673/2409-7292.2025.032375

співвідносяться з ISO 27001 [7], NIST CSF [11], NIS2 [2] чи індексами на кшталт GCI [1] або NCSI [6]. Для урядів і організацій, які зобов'язані виконувати ці стандарти (наприклад, через законодавство чи галузеві вимоги), доведеться самостійно робити mapping. Це зменшує практичну придатність фреймворку для прямого використання у регульованих секторах або в міждержавних порівняннях;

– обмежена увага до специфічних загроз. Документ більше зосереджений на ризик-менеджменті як процесі, ніж на конкретних типах загроз (APT, кібершпигунство, дезінформаційні атаки, атак на ланцюг постачання та інше, мало надається уваги до нових викликів (IoT, AI-driven threats, квантові загрози та інше);

– відсутність чіткої системи оцінки зрілості. Фреймворк не пропонує рівнів зрілості (maturity levels) для організацій чи країн. Це ускладнює можливість провести порівняння стану цифрової безпеки між різними суб'єктами;

– мало приділяється уваги людському чиннику. Хоча згадується потреба у підвищенні обізнаності, відсутня деталізація щодо програм кібергігієни, навчальних планів чи сертифікацій для персоналу;

– відсутність механізмів моніторингу та зворотного зв'язку. Не передбачено конкретних інструментів чи підходів для постійного моніторингу ризиків і зворотного зв'язку, що особливо важливо для динамічного кібердовкілля.

5. Cybersecurity Capacity Maturity Model (CMM) Модель зрілості спроможностей у сфері кібербезпеки [12]. Модель розроблена Оксфордським університетом (Global Cyber Security Capacity Centre), перша версія якої була розроблена 2014 році, а остання в 2021 році. Модель містить наступних 5 вимірів (dimensions), кожен з яких розбитий на чинники та індикатори оцінювання.

Вимір 1. Політика та стратегія кібербезпеки (Dimension 1: Cybersecurity Policy and Strategy) – національна політика, стратегічні документи, програми розвитку. До цього виміру відноситься чинники: національна стратегія кібербезпеки (D 1.1: National Cybersecurity Strategy); реагування на інциденти та управління кризами (D 1.2: Incident Response and Crisis Management); захист критичної інфраструктури (KI) (D 1.3: Critical Infrastructure (CI) Protection); кібербезпека в обороні та національній безпеці (D 1.4: Cybersecurity in Defence and National Security).

Вимір 2. Культура та суспільні аспекти кібербезпеки (Dimension 2: Cyber Culture and Society) – обізнаність, освіта, залученість суспільства. До цього виміру відносяться чинники: мислення у сфері кібербезпеки (D 2.1: Cybersecurity Mindset); довіра та впевненість у використанні онлайн-сервісів (D 2.2: Trust and Confidence in Online Services); розуміння користувачами захисту персональної інформації в онлайн-довкілля (D 2.3: User Understanding of Personal Information Protection Online); механізми повідомлення про інциденти (D 2.4: Reporting Mechanisms); медіа та онлайн-платформи (D 2.5: Media and Online Platforms).

Вимір 3. Освіта, підготовка та навички у сфері кібербезпеки (Dimension 3: Cybersecurity Education, Training and Skills) – професійна підготовка та розвиток компетенцій. До цього виміру відносяться чинники: підвищення обізнаності (D 3.1: Awareness Raising); рамкова система професійної підготовки (D 3.2: Framework for Professional Training); національна освітня рамка (D 3.3: National Education Framework); попит і пропозиція на ринку праці (D 3.4: Labour Market Supply and Demand).

Вимір 4. Правова та нормативна база (Dimension 3: Legal and Regulatory Frameworks) – закони, норми, регуляторні вимоги у сфері кібербезпеки. Цей вимір містить такі чинники: правові рамки, що регулюють кіберпростір (D 4.1: Legal Frameworks Governing Cyberspace); законодавство у сфері кіберзлочинності (D 4.2: Cybercrime Legislation); законодавство щодо захисту даних (D 4.3: Data Protection Legislation); законодавство щодо приватності (D 4.4: Privacy); законодавство про захист прав споживачів (D 4.5: Consumer Protection Legislation);

законодавство щодо цифрових доказів (D 4.6: Digital Evidence Legislation); права інтелектуальної власності в кіберпросторі (D 4.7: Intellectual Property Rights in Cyberspace).

Вимір 5. Стандарти, організації та технології (Dimension 4: Standards, Organisations and Technologies) – технічні стандарти, сертифікація, інфраструктура. Цей вимір складається із таких чинників: впровадження міжнародних стандартів (D 5.1: International Standards Adoption); розробка національних стандартів (D 5.2: National Standards Development); галузеві стандарти (D 5.3: Sector-specific Standards); сертифікація та оцінка відповідності (D 5.4: Certification and Conformity Assessment); технічні засоби безпеки (D 5.5: Technical Security Controls); безпека за принципом "від проектування" (D 5.6: Security by Design); технології виявлення та реагування на інциденти (D 5.7: Incident Detection and Response Technologies).

У CMM кожен чинник у п'яти вимірах оцінюється за п'ятиступеневою шкалою зрілості:

1. Початковий рівень (Start-Up). Діяльність або підхід до кібербезпеки практично відсутні. Ініціативи носять випадковий характер, залежать від окремих людей, а не від системи. Немає формалізованої політики, процедур або інституційної підтримки. Фокус – на усвідомленні проблеми, а не на її вирішенні;

2. Формувальний рівень (Formative). Є початкові кроки до впровадження політик і процедур. Існують окремі програми чи ініціативи, але вони ще не системні. Обмежене охоплення і невеликий масштаб впровадження. Основна мета — закласти основу для розвитку;

3. Сформований рівень (Established). Кібербезпекові заходи є сталими, узгодженими і підтримуються інституційно. Існують формальні політики, стандарти та органи, що відповідають за їх виконання. Практики інтегровані в ключові процеси організації або країни. Регулярний моніторинг та удосконалення, але фокус ще на внутрішньому рівні;

4. Стратегічний рівень (Strategic). Кібербезпека є частиною національної або корпоративної стратегії. Існує чітка координація між різними органами, секторами та стейкхолдерами. Рішення приймаються на основі ризик-менеджменту та аналітики. Є міжнародна взаємодія та участь у глобальних ініціативах;

5. Динамічний рівень (Dynamic). Система кібербезпеки гнучка, адаптивна і швидко реагує на нові виклики. Постійне вдосконалення на основі досвіду, досліджень і технологічних інновацій. Високий рівень взаємодії на міжнародному рівні, обмін даними в режимі реального часу. Проактивний підхід до загроз – прогнозування та запобігання замість реагування.

Модель не тільки оцінює поточний рівень зрілості, але й описує 5 рівнів розвитку для кожного чинника (від початкового до стратегічно оптимізованого), що дозволяє будувати дорожні карти підвищення спроможностей [12].

На сьогодні офіційно опублікованих результатів оцінки України за CMM немає у відкритому доступі. Зазвичай CMM-оцінки, проведені Оксфордським Global Cyber Security Capacity Centre, часто зберігаються у внутрішніх звітах або публікуються лише за згодою країни. Деякі держави погоджуються на відкритий звіт (наприклад, Грузія, Кенія, Гана, Кіпр (див. рис. 3) [13] та інші [14]), але Україна поки не входить до цього списку. Є лише непрямі згадки, що Україна розглядала можливість участі в CMM, але офіційний звіт не публікувався.

Опишемо слабкі сторони CMM, до яких можемо віднести:

– відсутність чітких KPI – модель описує рівні зрілості, але не дає вимірюваних метрик;

– висока трудомісткість оцінки – потребує багато даних і опитувань різних стейкхолдерів;

– не враховує регіональні особливості – застосовується як універсальний підхід, але не адаптований під специфіку окремих країн;

– не інтегрує напряму міжнародні рейтинги (NCSI [6], GCI [5]) – тому складно порівнювати з ними результати;

– відсутність прямої прив'язки до кібердипломатії – акцент на внутрішніх спроможностях, а не зовнішньополітичних аспектах.

© Шульга В.П., Корченко О.Г., Іванченко Є.В., Казмірчук С.В., Кондратюк С.В. (2025) Критерії стратегічного оцінювання кібербезпеки держави: кібердипломатичний аспект. Сучасний захист інформації, 3(63), 205–218. https://doi.org/10.31673/2409-7292.2025.032375

Factors based on CMM 2017	Maturity Stage‡ 2017	Maturity Stage‡ 2021	Capacity Changes*
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Formative to Established	Established to Strategic	+ +
D1.2 Incident Response	Formative	Established to Strategic	+ +
D1.3 Critical Infrastructure Protection	Start-Up to Formative	Established	+ +
D1.4 Crisis Management	Formative	Established	+ +
D1.5 Cyber Defence	Formative	Established	+ +
D1.6 Communications Redundancy	Established	Established	o
D2 Cybersecurity Culture and Society			
D2.1 Cybersecurity Mind-Set	Formative	Formative	o
D2.2 Trust and Confidence on the Internet	Formative	Formative	o
D2.3 User Understanding of Personal Inf.	Formative	Formative	o
D2.4 Reporting Mechanisms	Formative	Establish	+ +
D2.5 Media and Social Media	Formative	Formative	o
D3 Cybersecurity Education, Training, and Skills			
D3.1 Awareness Raising	Formative to Established	Formative to Established	o
D3.2 Framework for Education	Established	Formative to Established	-
D3.3 Framework for Professional Training	Formative	Formative to Established	+
D4 Legal and Regulatory Frameworks			
D4.1 Legal Frameworks	Established	Established	o
D4.2 Criminal Justice System	Formative to Established	Established	+
D4.3 Formal and Informal Cooperation Fra.	Established	Established	o
D5 Standards, Organisations, and Technologies			
D5.1 Adherence to Standards	Start-Up to Formative	Formative to Established	+ +

Рис. 3. Загальне представництво потенціалу кібербезпеки на Кіпрі – Огляд CMM за 2017 та 2021 роки

Проведений аналіз провідних міжнародних моделей та фреймворків оцінювання кібербезпеки (див. табл. 2, де в колонці **Рік** наведено рік створення першої і останньої версії, а в **К** – кількість напрямків оцінки) продемонстрував, що жодна з існуючих систем не є універсальною для повного врахування як національних, так і міжнародних пріоритетів України у сфері кібердипломатії.

Виявлені ключові спостереження:

– різна кількість напрямків оцінювання (від 4 до 12) та відмінності у структурі індикаторів ускладнюють порівняння результатів між моделями;

– відсутність уніфікованих стандартизованих KPI у більшості фреймворків, що ускладнює практичне вимірювання прогресу;

– нерівномірна прив’язка до міжнародних стандартів (ISO/IEC 27001, NIST CSF, NIS2, GCI, NCSI) – частина моделей взагалі не містить таблиць відповідності з нормативами;

– спеціалізація моделей – окремі моделі орієнтовані на регуляторні вимоги (NIS2), інші на індексування для міжнародних рейтингів (GCI, NCSI), або на вимірювання зрілості (CMM);

– відсутність інтеграції кібердипломатичного виміру – жодна модель безпосередньо не враховує індикатори, пов'язані з міжнародним співробітництвом, довірою у кіберпросторі та виконанням міжнародних зобов'язань.

Таблиця 2

Зведені дані дослідження існуючих підходів до оцінки кібербезпеки в різних аспектах

Модель /Фрейм-ворк	Розробник	Рік	К	Мета	Приклади напрямків	Слабкі сторони	Можливість інтеграції
GCI	ITU	2014 2023	5	Глобальна оцінка кіберготовності країн.	Правові заходи, технічні заходи.	Орієнтований на статистику, без глибокої якості.	Так – для міжнародних порівнянь.
NIS2 & EU	ЄС	2016 2022	6	Єдині вимоги для кіберстійкості ЄС.	Управління ризиками, звітність.	Складно адаптувати поза ЄС.	Частково – для регуляторних вимог.
NCSI	EGA (Естонія)	2016 2023	12	Національні кіберспроможності.	Політика, освіта, кіберінциденти.	Не оцінює ефективність, лише наявність.	Так – для структуризації критеріїв.
OECD DSRMF	OECD	2015 2021	4	Управління цифровими ризиками.	Управління ризиками, культура.	Відсутні KPI, нормативна прив'язка.	Частково – для управлінських принципів.
CMM	University of Oxford	2015 2021	5	Зрілість національних кіберспроможностей.	Політика, культура, освіта.	Немає кількісних оцінок.	Так – для рівнів зрілості.

Висновки і рекомендації

Виходячи із отриманих результатів аналізу сформовано 11 основних критеріїв оцінювання кібербезпеки держави в рамках стратегії кібердипломатії, а також їх кількість та зміст було визначено на основі:

– синтезу кращих практик з п'яти визначених міжнародних моделей, із врахуванням ключових напрямків, релевантних для України (див. табл. 2);

– потреб національної стратегії кібердипломатії, де пріоритети виходять за рамки суто технічної кібербезпеки й включають політичні, правові, соціальні та міжнародні аспекти;

– урахування нормативної бази (ISO 27001, NIST CSF, NIS2, Будапештська конвенція, резолюції ООН з кібербезпеки) для забезпечення відповідності міжнародним стандартам;

– необхідності балансу між кількістю напрямків (щоб не розпорошувати увагу) та їх повнотою (щоб охопити всі критично важливі виміри);

– гнучкості інтеграції в міжнародні рейтинги (щоб мати можливість адаптувати оцінку під GCI, NCSI, CMM тощо).

Таким чином, за результатами аналізу запропоновано 11 критеріїв, які стали результатом компромісу між повнотою охоплення ключових аспектів кіберстійкості та кібердипломатії, зручністю практичного використання в оцінюванні та можливістю порівняння з міжнародними метриками.

Сформована множина з 11 критеріїв, за якими можна здійснити оцінювання рівня кібербезпеки України у межах реалізації стратегії кібердипломатії мають достатній рівень деталізації, який дозволяє:

– комплексно оцінювати стан кіберзахисту за широким спектром напрямів;
– ефективно планувати розвиток інституційних, технологічних та правових механізмів;
– зміцнювати позиції України у кіберпросторі.

Таблиця 3

Критерії оцінювання кібербезпеки в рамках реалізації Стратегії кібердипломатії України

№	Напрям	Критерії	Відповідні компоненти міжнародних моделей	Міжнародні стандарти / рекомендації	Коментар щодо інтеграції
1	Політика і законодавство.	Наявність актуального законодавства та стратегій кібербезпеки, відповідність міжнародним стандартам.	GCI – Legal Measures; NIS2 – Governance; CMM – Policy and Strategy; OECD – Governance.	ISO/IEC 27001, NIST CSF Identify.	Чітка стратегія, структура управління та відповідальність органів.
2	Міжнародне співробітництво та кібердипломатія.	Участь у форумах, ініціативах (ООН, ЄС, НАТО), міжнародні угоди, обмін досвідом.	GCI – Legal Measures; NIS2 – Compliance; NCSI – International Cooperation; CMM – Cybersecurity Policy.	Budapest Convention, ISO/IEC 27002, ITU-D X.1051.	Відповідність міжнародним договорам і рекомендаціям.
3	Інституційна спроможність і координація.	Система раннього виявлення кіберзагроз, обмін ІКТ-інформацією з партнерами.	CMM – Organizational Structures; NIS2 – Cooperation Mechanisms; NCSI – Capacity.	ISO 22301, NIST SP 800-37.	Міжвідомча та міждержавна координація, кризове управління.
4	Захист критичної інформаційної інфраструктури (КІІ).	Технічна захищеність КІІ, наявність протоколів реагування.	GCI – Technical Measures; NIS2 – Critical Entities; CMM – Critical Infrastructure Protection.	NIST SP 800-82, ISO 27019, ITU-T X.1056.	Ідентифікація та захист критичних секторів.
5	Технологічна спроможність і кіберінновації.	Фінансування кіберінновацій, наявність патентів, партнерство з НДІ.	GCI – Technical Measures; NCSI – Cybersecurity Capabilities; OECD – Risk Management Cycle.	ISO/IEC 27035, NIST SP 800-61, MITRE ATT&CK.	Реагування, виявлення та відновлення після інцидентів.
6	Освіта, підготовка кадрів і просвіта населення.	Навчальні програми для дипломатів, ІТ-спеціалістів, міжнародна сертифікація.	CMM – Education, Training, Skills; GCI – Capacity Building.	NICE Framework, ISO/IEC 27021.	Підготовка кадрів, тренінги, підвищення кваліфікації.
7	Оперативне реагування та управління кіберінцидентами.	Оперативність CERT-UA, наявність планів реагування, взаємодія з міжнародними CERT.	CMM – Cybersecurity Culture and Society; OECD – Awareness.	ISO/IEC 27002 Awareness clauses, ENISA guidelines.	Культура кібергігієни, довіра, громадська освіта.
8	Інформаційна стійкість та протидія дезінформації.	Освітні кампанії, цифрова гігієна, доступ до інструкцій, участь молоді.	GCI – Organisational Measures; NCSI – Industry Involvement.	ISO/IEC 20000, NIST SP 800-53 supply chain controls.	Розвиток національної кіберіндустрії та інновацій.
9	Інвестиції в нові технології.	Державна підтримка ШІ, розробки в кіберзахисті, проекти в ІКТ.	CMM – Research and Development; OECD – Innovation.	Horizon Europe R&D, ISO/IEC TR 27103.	Стимулювання досліджень і технологічних рішень.

10	Міжнародний імідж і вплив.	Роль у формуванні міжнародних норм, ініціативи в ООН/ЄС/НАТО.	NCSI – International Cooperation; GCI – Cooperation; CMM – International Engagement.	UN GGE/OEWG Reports, Budapest Convention.	Активна участь у міжнародних ініціативах.
11	Політика приватності, права людини і законність у кіберпросторі	Цифрові права, етика і законність.	OECD – Metrics & Monitoring; CMM – Performance Measurement.	ISO/IEC 27004, NIST SP 800-55.	Використання KPI та регулярних аудитів.

Вибір таких критеріїв обґрунтований наступними причинами.

1. Повнота охоплення кіберсистеми. Сформована множина критеріїв дозволяє врахувати як стратегічні (політика, міжнародне співробітництво, імідж), так і операційні аспекти (захист критичних інфраструктур, реагування, технологічні інновації) не залишаючи «сліпих зон».

2. Баланс між глобальними підходами та національною специфікою. Кожен критерій був адаптований з урахуванням міжнародного досвіду, але з фокусом на актуальні виклики України – кібератаки у воєнних умовах, протидія дезінформації, участь у міжнародних альянсах.

3. Відповідність міжнародним стандартам. Критерії безпосередньо співвіднесені з ISO/IEC, NIST, ENISA, рекомендаціями ООН та ЄС, що забезпечує узгодженість із загальноприйнятими підходами і підвищує легітимність оцінки.

4. Можливість кількісного та якісного вимірювання. Для кожного критерію можна визначити індикатори ефективності (KPI), що дає змогу проводити як кількісну, так і якісну оцінку прогресу.

5. Гнучкість та масштабованість. Визначена множина критеріїв дозволяє деталізувати оцінку залежно від контексту (наприклад, для регіонального, секторального або міжнародного аналізу), а також доповнювати систему без її руйнування.

6. Інтеграція з кібердипломатичними цілями. Критерії враховують не лише технічну безпеку, а й роль держави у формуванні глобальної політики кіберпростору, що є ключовим для дипломатичного виміру.

Такий підхід дозволяє не лише відстежувати загальний рівень зрілості державної політики, комплексно оцінювати стан кіберзахисту держави, визначати пріоритетні напрями розвитку та забезпечувати прозорість у формуванні й реалізації Стратегії кібердипломатії України, а й виявляти слабкі місця у таких напрямках, як протидія дезінформації, міжнародний імідж, інвестиції, цифрові права та інновації. Таким чином, розроблена система критеріїв є не лише аналітичним інструментом, але й важливим елементом формування кіберполітики держави, що здатна реагувати на сучасні та майбутні виклики у цифровому просторі.

Подальші дослідження потрібно спрямувати на розробку методології оцінювання стану кібербезпеки держави в аспекті кібердипломатичної діяльності на базі сформованої множини критеріїв.

Перелік посилань

1. Global Cybersecurity Index, About International Telecommunication Union (ITU), веб-сайт. URL: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/ (дата звернення: 08.08.2025).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 08.08.2025).

3. Joint Communication To The European Parliament And The Council The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018 (дата звернення: 08.08. 2025).

4. OECD Policy Framework on Digital Security Cybersecurity For Prosperity. URL: https://www.oecd.org/ content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf (дата звернення: 08.08.2025).

5. Global Cybersecurity Index 2024. URL: https:// www.itu.in t/en / ITU-D / Cybersecurity / pages/global-cybersecurity-index.aspx (дата звернення: 08.08.2025).

6. The National Cyber Security Index 3.0. URL: https: // ega.ee / wp-content / upload s/ 2023 / 08/NCSI-3.0_Methodology.pdf (дата звернення: 08.08.2025).

7. Information security, cybersecurity and privacy protection – Information security management systems – Requirements: ISO/IEC 27001:2022: Technical Committee: ISO/IEC JTC 1/SC 27, ICS : 35.030 03.100.70, P. 19.

8. Information security, cybersecurity and privacy protection – Guidance on managing information security risks: ISO/IEC 27005:2022: Technical Committee : ISO/IEC JTC 1/SC 27, ICS : 35.030, P. 64.

9. Information security, cybersecurity and privacy protection – Information security controls: ISO/IEC 27002:2022: Technical Committee : ISO/IEC JTC 1/SC 27, ICS : 35.030 03.100.70, P. 152.

10. Security and resilience – Business continuity management systems – Requirements: ISO 22301:2019: Technical Committee : ISO/TC 292, ICS : 03.100.01 03.100.70, P. 21.

11. The NIST Cybersecurity Framework (CSF) 2.0: National Institute of Standards and Technology URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 12.08.2025).

12. Cybersecurity Capacity Maturity Model for Nations (CMM) Global Cyber Security Capacity Centre URL: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf (дата звернення: 12.08.2025).

13. CYBERSECURITY CAPACITY REVIEW Republic of Cyprus September 2021 URL: https://dsa.cy/images/pdf-upload/cmm_cyprus_report_2021_final.pdf (дата звернення: 12.08.2025).

14. CMM Reviews Around the World. URL: https://gcscc.ox.ac.uk/cmm-reviews (дата звернення: 12.08.2025).

Надійшла 31.03.2025