ПІДГОТОВКА ФАХІВЦІВ

УДК 004.056:37
DOI 10.32461/2409-9805.2.2025.350080

Цитування:
Дубова С. В. Матвієнко О. В., Парченко Н. В. Визначення рівня зрілості кіберосвіти в Україні: методологічний підхід. *Бібліотекознавство. Документознавство. Інформологія*. 2025. № 2. С. 61–68.

Dubova S., Matviienko O., Parchenko N. (2025). Determining the Maturity Level of Cyber Education in Ukraine: Methodological Approach. Library Science. Record Studies. Informology, 2, 61–68 [in Ukrainian].

Дубова Світлана Володимирівна,
кандидат історичних наук,
голова правління ГО «Центр аналізу і розробки ефективних політик»
https://orcid.org/0000-0002-0374-2099
s.dubova@cadep.org.ua

Матвієнко Оксана Володимирівна,
доктор педагогічних наук, професор,
професор кафедри інформаційної діяльності та зв'язків з громадськістю
Київського національного університету культури і мистецтв
https://orcid.org/0000-0001-5772-848X
oxmix2017@gmail.com

Парченко Наталія Володимирівна,
експерт ГО «Центр аналізу і розробки ефективних політик»
https://orcid.org/0009-0007-3293-582X
ngo.cadep@gmail.com

ВИЗНАЧЕННЯ РІВНЯ ЗРІЛОСТІ КІБЕРОСВІТИ В УКРАЇНІ: МЕТОДОЛОГІЧНИЙ ПІДХІД

Метою статті *є охарактеризувати методологію Агенції ЄС з питань кібербезпеки (ENISA), запропоновану для оцінювання рівня зрілості кібербезпекової освіти.* ***Методи дослідження:*** *аналіз і узагальнення наукових джерел та методик – для вивчення теоретичних підходів до розуміння кібербезпекової освіти та сучасних методологічних інструментів для оцінки зрілості кіберосвіти, зокрема методології ENISA.* ***Наукова новизна*** *дослідження полягає в методологічному обґрунтуванні застосування та адаптації моделі ENISA до національного контексту України, що дозволяє використати її як комплексний інструмент оцінювання рівня зрілості кіберосвіти в початковій та середній школі. Запропоновано авторське бачення етапності національної адаптації методології ENISA, що включає інтеграцію експертних інтерв'ю, аналіз нормативних документів та інструментів оцінювання освітніх результатів. Це створює підґрунтя для розроблення національної моделі оцінювання кіберзрілості освіти. Запропоновано інтерпретацію кіберосвіти як цифрової платформи соціокультурної взаємодії, що формується на перетині освіти, цифрових компетентностей та громадянської активності. Використання методології ENISA створює умови для розроблення національної «дорожньої карти» кіберосвіти як цифрової платформи, що передбачає побудову цілісної освітньої екосистеми «школа – університет – професія».* ***Висновки.*** *Методологія ENISA є релевантним та ефективним інструментом для комплексного оцінювання стану кіберосвіти в Україні, оскільки враховує нормативний, стратегічний та операційний аспекти формування цифрової і кібербезпекової компетентності на рівні*

© Дубова С. В., 2025. CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/)
© Матвієнко О. В., 2025. CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/)
© Парченко Н. В., 2025. CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/)

початкової та середньої освіти. Інтерпретація кіберосвіти як цифрової платформи дає змогу комплексно оцінити стан української системи, включно з нормативною базою, стратегічною узгодженістю, практиками навчання та механізмами моніторингу. ENISA пропонує модель, що дозволяє охопити ці аспекти системно й порівнювано. Використання методології дає змогу системно діагностувати сильні й слабкі сторони національної освітньої політики, визначати прогалини в нормативному забезпеченні, в узгодженості стратегій та практичній реалізації навчальних програм.

Ключові слова: *кіберосвіта, кібербезпека, рівень зрілості, методологія ENISA*.

Dubova Svitlana*,*
PhD in History, Chair of the Board,
NGO "Centre for Analysis and Development of Effective Policies"

Matviienko Oksana*,*
Doctor of Pedagogical Sciences, Professor, Professor of the Department of Information Activity and Public Relations, Kyiv National University of Culture and Arts

Parchenko Nataliia*,*
Expert, NGO "Centre for Analysis and Development of Effective Policies"

DETERMINING THE MATURITY LEVEL OF CYBER EDUCATION IN UKRAINE: METHODOLOGICAL APPROACH

The purpose of the article *is to describe the methodology of the EU Agency for Cybersecurity (ENISA) proposed for assessing the maturity level of cybersecurity education.* ***Research methods:*** *analysis and synthesis of scientific sources and methodologies used to study theoretical approaches to understanding cybersecurity education and modern methodological tools for assessing the maturity of cyber education, including the ENISA methodology.* ***The scientific novelty*** *of the study lies in the methodological justification for the application and adaptation of the ENISA model to the national context of Ukraine, which makes it possible to use it as a comprehensive tool for assessing the maturity level of cyber education in primary and secondary schools. An original vision of the stages of national adaptation of the ENISA methodology is proposed, including the integration of expert interviews, analysis of regulatory documents, and tools for assessing educational outcomes. This provides the basis for developing a national model for assessing the maturity of cyber education. The article proposes an interpretation of cyber education as a digital platform of socio-cultural interaction formed at the intersection of education, digital competencies, and civic engagement. The use of the ENISA methodology creates the conditions for developing a national 'roadmap' for cyber education as a digital platform that envisages building an integrated educational ecosystem 'school – university – profession'.* ***Conclusions****. The ENISA methodology is a relevant and effective tool for a comprehensive assessment of the state of cyber education in Ukraine, as it takes into account the regulatory, strategic, and operational aspects of forming digital and cybersecurity competencies at the level of primary and secondary education. Interpreting cyber education as a digital platform makes it possible to comprehensively assess the state of the Ukrainian system, including the regulatory framework, strategic coherence, teaching practices, and monitoring mechanisms. ENISA provides a model that enables these aspects to be examined systematically and comparatively. The use of the methodology makes it possible to systematically diagnose the strengths and weaknesses of national educational policy, identify gaps in regulatory support, consistency of strategies, and the practical implementation of curricula.*

Keywords: *cyber education, cybersecurity, maturity level, ENISA methodology.*

Актуальність теми дослідження. Використання цифрових технологій протягом останніх десятиліть актуалізує проблематику кібербезпеки і, відповідно, кіберосвіти. Об'єктивно посилюється увага країн та урядів не тільки до знань, умінь та навичок громадян у цифровому світі, а й загалом до *рівня зрілості* кіберосвіти - показника того, наскільки освітня система, організація або підхід до навчання є розвиненими, ефективними та системно впровадженими.

Окреслюючи методологічні підходи до оцінки рівня зрілості кіберосвіти в Україні, згадаємо висловлювання Маршала Маклюена, відомого культуролога, соціолога та педагога, зроблене у 1964 р.: «Якщо й надалі зберігатимуться нинішні зразки фрагментованої несистемності, наші шкільні навчальні програми забезпечать появу громадян, нездатних зрозуміти кібернетизований світ, у якому вони живуть» [11, 383]. Зазначимо, що це зауваження не втратило актуальності й донині і

актуалізує увагу до знань школярів, які вже з раннього віку активно взаємодіють із цифровим простором, є критично важливою цільовою групою для формування навичок безпечної поведінки в Інтернеті.

Бачиться, що шкільна кіберосвіта є «цифровою платформою» не тільки для подальшої освіти (зокрема професійної кіберосвіти), а й загалом для формування «цифрового громадянства» – сукупності знань, умінь, цінностей і практик, які забезпечують відповідальну, етичну й активну участь особи у цифровому суспільстві. Цифрове громадянство охоплює здатність користуватися цифровими технологіями безпечно й ефективно, дотримуватися правових і моральних норм, критично оцінювати інформацію та здійснювати громадянську активність у мережевому середовищі.

При цьому будемо розуміти цифрову платформу у соціокультурному контексті не просто як «технологію», а як середовище взаємодії, що трансформує освіту, культуру й комунікації у суспільстві.

Актуальність дослідження рівня зрілості кіберосвіти в Україні зумовлюється суперечностями між інтенсивним розвитком цифрового середовища, появою нових кіберзагроз і повільним оновленням освітніх стандартів та навчальних програм, а також між міжнародними підходами до оцінювання зрілості кіберосвіти й відсутністю в Україні адаптованої методології.

Аналіз досліджень і публікацій. Проблема кіберосвіти у різних аспектах знаходиться у полі наукової уваги українських дослідників. Так, наголошуючи тому, що знання з кібербезпеки у тих, хто навчається, повинні формуватися в рамках базових курсів всіх без винятку навчальних закладів, Ю. Даник та А. Зінченко [1] пропонують варіант реалізації організації системи освіти з питань кібербезпеки, який охоплює всі рівні освіти від дошкільної та середньої до вищої та післядипломної.

Українські дослідники [2] звертаються до вивчення підходів європейських країн наголошуючи, що в Україні не набули поширення педагогічні практики щодо підтримки цифрового громадянства та недостатньо поширені форми та методи впровадження громадянської освіти засобами ІКТ.

У Концепції цифрового громадянства [10], представленій на сайті Ради Європи, подано таке розуміння поняття «цифрові громадяни» - люди, здатні використовувати цифрові інструменти для створення, споживання, спілкування та позитивної й відповідальної взаємодії з іншими. Вони розуміють і поважають права людини, приймають різноманітність і стають людьми, які навчаються протягом усього життя, щоб йти в ногу з еволюцією суспільства.

Наголошується, що освіта в галузі цифрового громадянства – це розширення можливостей учнів різного віку через освіту або набуття компетенцій для навчання та активної участі в цифровому суспільстві, щоб вони могли здійснювати та захищати свої демократичні права та обов'язки в Інтернеті, а також сприяти та захищати права людини, демократію та верховенство права в кіберпросторі. Європи визначає DCE як цілісний підхід, спрямований на розвиток основних навичок та знань, необхідних в сучасному взаємопов'язаному світі, а також сприяння формуванню цінностей і ставлень, що забезпечать їх відповідальне використання.

Іманентною складовою формування компетентностей цифрового громадянства є кіберосвіта.

У статті О. Пучкова та О. Уваркіної [3] запропоновано концептуальний каркас сталого розвитку формальної кіберосвіти. Проведений дослідниками аналіз освітніх програм з кібербезпеки ЄС засвідчив характерну мінливість освітнього ландшафту кібербезпеки в ЄС та дав змогу визначити основні прогалини у підготовці майбутніх професіоналів.

На неформальну освіту як сучасне «вікно можливостей» звертається увага у публікації О. Уваркіної, О. Шевчук та І. Горнійчук [4]. Автори розкривають, яким чином такий підхід дає змогу самостійно вивчати та розвивати навички в області кібербезпеки, програмування, веб-розробки, аналізу даних та інших сфер інформаційних технологій.

У термінологічному предметному полі також наявний термін «кібергігієна», під яким зазвичай розуміють практичний набір щоденних дій та правил користування цифровими технологіями для забезпечення безпеки

У працях зарубіжних дослідників «кібергігієна» позначається як нова концепція, зосереджена на тому, як можна захистити себе від онлайн-ризиків та загроз, а також як використовувати технології безпечним та розумним способом [8].

Водночас, звертаючись до поняття «кіберосвіта» у розумінні його як *систематичного процесу навчання*, що охоплює широке коло знань про кібербезпеку, загрози в інтернеті, методи захисту даних, цифрові права, етичне використання інформаційних технологій, зауважимо, що в українському науковому дискурсі не вдалось виявити публікації, предметно присвячені кіберосвіті школярів.

У зарубіжному науковому дискурсі простежується системне опрацювання цього напряму.

Так, чеські дослідники Д. Ондрушкова та Р. Поспішил [12] представили результати експерименту, який виявив обізнаність дітей у сфері

кібербезпеки у чеських початкових школах. Експеримент засвідчив, що одноразові тренінги не впливають на відповідальну поведінку школярів у Інтернеті і не є підходящим рішенням для ефективного покращення навичок онлайн-безпеки. Завдання полягає в тому, щоб включити навчання з кібербезпеки у весь навчальний процес. Структура освіти з кібербезпеки має бути зміщена від окремих курсів безпосередньо до щоденного викладання уроків у послідовний спосіб. Для успішної імплементації необхідно також запровадити ефективний інструмент для оцінки кібербезпекових здібностей учнів, оскільки небезпеки та ризики поступово зростають. Оскільки майбутня еволюція ризиків заслуговує на те, щоб оцінка обізнаності з кібербезпеки проводилася більш послідовно прийнятої та здійснюваної на національному рівні, увага майбутніх досліджень має бути спрямована на ефективні метричні інструменти для виявлення слабких місць, нових потенційних ризиків і небезпек в Інтернеті.

Пропозиції стратегій для навчальних закладів для підвищення обізнаності своїх учнів щодо кібербезпеки та одночасної мотивації їх до кар'єри в галузі кібербезпеки представлено у публікації У. Тріплета [13]. Було проведено систематичний огляд досліджень, результати якого засвідчили, що ігрові стратегії були ефективними у підвищенні обізнаності учнів про кібербезпеку та їхньої зацікавленості в кар'єрі в галузі кібербезпеки.

Зважаючи на брак у наукових публікаціях чітких визначень понять «кіберосвіта» та «кібербезпекова освіта», на основі досліджених джерел окреслимо їх таким чином.

Кіберосвіта – поняття, яке охоплює всю сферу навчання та підготовки, пов'язаної з цифровими технологіями, інтернетом, інформаційними системами тощо. Включає основи комп'ютерної грамотності, програмування, роботу з цифровими інструментами, штучним інтелектом, хмарними технологіями тощо. Може бути адресована як дітям, так і дорослим – усім, хто користується цифровими технологіями.

Умовно, *кіберосвіта* – це все навчання про кіберсвіт, а кібербезпекова освіта – це навчання про те, як у цьому світі залишатися в безпеці.

Вибудовуючи тезу необхідності шкільної кіберосвіти зазначимо, що:

- кіберосвіта у школі виступає не тільки як навчання цифровим навичкам, а як системне формування компетентностей у сфері кібербезпеки, цифрової грамотності та відповідального використання технологій;
- вона є *базовим рівнем* цифрової соціалізації, який забезпечує наступність між середньою та вищою освітою;
- забезпечує наступність освітніх програм: від базової цифрової грамотності до спеціалізованих компетентностей (інформаційна аналітика, кіберзахист, цифрові комунікації);
- створює єдиний освітній екосистемний простір, у якому школяр → студент → фахівець рухається через послідовні рівні цифрової освіти;
- підвищує рівень готовності абітурієнтів до навчання у цифровому середовищі університету;
- виховує цифрову ідентичність та культуру критичного мислення;
- формує відповідальність за цифрові дії (етика, дотримання авторського права, захист персональних даних);
- розвиває активну громадянську позицію через участь у цифрових спільнотах, проєктах, волонтерських та просвітницьких ініціативах;
- готує молодь до життя в умовах інформаційних ризиків (фейки, дезінформація, кібербулінг).

Кібербезпекова освіта – це підвид кіберосвіти, що спеціалізується на питаннях захисту інформації, безпеки в цифровому середовищі, захисту даних, інфраструктури та боротьби з кіберзагрозами. Охоплює такі теми як кібергігієна, захист паролів, фішинг, соціальна інженерія, реагування на кіберінциденти тощо.

Зважаючи на вищевикладене та сформульований фактичний імператив важливості кіберосвіти на всіх рівнях освітніх та життєвих траєкторій сучасної людини, постає питання про інструменти, які можуть застосувати науковці та державні органи до вимірювання її якості та повноти, а фактично - рівня зрілості кіберосвіти. Хоча методологій та дієвих інструментів такого вимірювання все ще недостатньо, однак окремі з них цілком можуть бути застосовані для вимірювання кіберзрілості освіти в Україні. Одним з таких інструментів є методологія, запропонована Агенцією ЄС з питань кібербезпеки (ENISA).

Отже, метою дослідження є охарактеризувати методологію Агенції ЄС з питань кібербезпеки (ENISA), запропоновану для оцінювання рівня зрілості кіберпезпекової освіти.

Виклад основного матеріалу. Рівень зрілості систем освіти з питань кібербезпеки суттєво різниться між країнами. ENISA здійснила дослідження рівня зрілості низки освітніх систем країн Європейського Союзу, визначивши ключові виклики, з якими стикаються держави-члени, а також виокремила найкращі практики впровадження кібербезпекової освіти. Україна, активно рухаючись шляхом європейської інтеграції, має запозичувати наявний європейський досвід, водночас чітко розуміючи власні виклики та потреби у сфері кібербезпекової освіти.

Базова методологія пропонує такий поділ рівнів зрілості кібербезпекової освіти:

- *несформований рівень* (0–20%): держава не визначилась щодо політики освіти з кібербезпеки. Відсутні політичні чи стратегічні рамки, стратегії (кібербезпекові чи освітні) не піднімають тему кібербезпекової освіти, не існує планів дій чи дорожніх карт в цій сфері. У школах ця тема не впроваджується, а освіта з кібербезпеки недоступна у початковій або середній школі;

- *початковий/епізодичний рівень* (20–40%): держава не має чітко визначеного підходу до кібербезпекової освіти у початковій та середній школі, однак можуть бути певні загальні цілі щодо такої освіти та впроваджуються окремі заходи з кібербезпекової освіти. Існують окремі програми для досягнення цієї мети, імплементуються деякі вимоги європейського законодавства. Водночас щодо шкільної освіти з кібербезпеки немає конкретної політичної та стратегічної основи, хоча і присутні певні рекомендації та правила які стосуються цієї теми;

- *ранній рівень* (40–60%): наявний чіткий національний підхід до впровадження кібербезпекової освіти. Існують початкові політики, плани дій, дорожні карти та інші ініціативи, які безпосередньо впливають на освіту з кібербезпеки на всіх рівнях (від початкової школи до старших класів). Крім того, починають залучатись активні стейкхолдери;

- *стабільний рівень* (60–80%): наявна чітка державна стратегія надання та поширення кібербезпекової освіти, яка підтримується політичними кроками, ініціативами, а також програмами, до яких залучені різні стейкхолдери. Практики та заходи запроваджуються однаково на національному та регіональному рівнях. Діяльність визначена та задокументована з чітким розподілом ресурсів та управлінням, а також встановленими термінами реалізації. Застосовується довгострокове бачення, і кібербезпека є важливою частиною навчальних програм у початковій та середній школі;

- *оптимізований/адаптивний рівень* (80–100%): щодо освіти з кібербезпеки є не лише окрема стратегія, а й для неї відбувається постійний процес оцінки: визначаються пріоритети, оперативно проводиться оптимізація, існує надійна система показників реалізації, є коротко-, середньо- та довгострокові цілі. Ефективність освітньої діяльності з кібербезпеки регулярно вимірюється та контролюється за допомогою усталеної системи показників. Визначаються фактори успіху, виклики та прогалини в реалізації заходів, а програми, ініціативи та стратегія оптимізуються та коригуються.

Окреслену методологію застосувала Агенція для підготовки дослідження Cybersecurity Education Maturity Assessment [9]. Пропонована методологія дозволяє визначити сильні сторони та проблемні аспекти національної освітньої системи, а також окреслити шляхи її подальшого вдосконалення. Методологія включає комплекс з 25 питань, 18 – з яких підлягають кількісній оцінці, а ще 7 – спрямовані на виявлення якісних характеристик розвитку системи початкової та середньої освіти. Питання зосереджені в трьох макроблоках: Урядовий (Governmental), Стратегія (Strategic) та Операційні заходи (Operational).

Урядовий блок містить такі підблоки:

Регуляторна база (Regulatory framework) – оцінка наявної в країні регуляторної бази, яка визначає обов'язковість кібербезпекової освіти та визначення обсягів її викладання.

Політики (Policies) – оцінка наявності чи відсутності спеціальної політики, розробленої щодо освіти з кібербезпеки в межах початкової та середньої освіти.

Підтримка (Support) – наявність будь-яких національних програм які підтримують кібербезпекову освіту, а також розроблених рекомендацій/настанов для підтримки цієї освіти.

Стратегія **(**Strategic **)** оцінює:

• *національну стратегію (National Strategies*) – визначення того, чи є питання кібербезпекової освіти на рівні шкіл частиною національної стратегії кібербезпеки;

• *план дій (Action Plan)* – чи існують національні освітні стратегії / їх плани дій, що прямо підтримують впровадження кібербезпекової освіти в школах;

• *співпрацю (Cooperation)* – чи налагоджено міждержавну, національну чи регіональну співпрацю в питаннях, пов'язаних з кібербезпековою освітою.

Операційні заходи (Operational) мають визначити:

• *забезпечення навчання* (Provision of education) – фактичне включення кібербезпекової компоненти у програми навчання початкової та середньої школи;

• *наявність механізму оцінювання* (Implementation evaluation mechanism) – чи існують інструменти моніторингу успішності навчання та контролю його якості.

Базова модель дослідження ENISA передбачає проведення глибинних інтерв'ю з експертами та подальший аналіз отриманих результатів. Цей підхід видається цілком раціональним для загальноєвропейської агенції, яка не має достатньої кількості ресурсів та окремих фахівців в кожній країні, які глибоко спеціалізуються на відповідній тематиці. Відтак метод «глибинних інтерв'ю» вбачається раціональним з огляду на необхідність знайти лише окремих експертів для оцінки ситуації на рівні країни не заглиблюючись у

особливості місцевого законодавства чи практик. Цей підхід дає можливість швидко і досить точно (але часто без деталей) оцінити загальну ситуацію та окреслити перспективи подальших досліджень.

Однак для застосування цієї методології на рівні окремої країни підхід потребує певного корегування (незалежно від того, хто проводить відповідну оцінку – державний орган чи науковець/група науковців). Фокусування на національному рівні змушує змінити логіку проведення такого дослідження і сконцентруватись на таких етапах:

1. Кабінетне дослідження в частині вивчення нормативних та стратегічних документів, що регулюють процес навчання для первинної та середньої освіти, а також ключові стратегічні напрямки кібербезпеки закріплені на рівні національних стратегічних документів. Також цей етап дослідження охоплює аналіз публічно доступних даних про заходи кіберосвіти, що здійснювались різними стейкхолдерами.

2. Аналіз результатів запитів, надісланих до урядових структур, які опікуються питаннями освіти чи релевантними питаннями кібербезпеки.

З огляду на стратегічний курс України на євроінтеграцію та побудову цифрової держави, методологія ENISA щодо оцінки зрілості кіберосвіти є актуальною для національного контексту з кількох причин:

1. *Гармонізація з європейськими стандартами:* методологія ENISA розроблена у межах політики ЄС у сфері кібербезпеки й освіти. Її використання дозволяє синхронізувати українську систему з європейськими підходами.

2. *Інституційна прозорість і вимірюваність:* ENISA пропонує структуровану модель з чіткими критеріями оцінки, що дозволяє об'єктивно діагностувати сильні та слабкі сторони національної політики й освітньої практики, а також здійснювати повторне вимірювання прогресу.

3. *Недостатність національних інструментів оцінки*: в Україні відсутні власні стандартизовані інструменти для вимірювання рівня впровадження кіберосвіти на шкільному рівні. ENISA може заповнити цю прогалину до моменту розробки національного механізму.

4. *Відповідь на виклики безпеки в освіті:* масове впровадження цифрових платформ у школах і водночас зростання інцидентів кіберзагроз потребують цілісного підходу до навчання учнів і вчителів цифровій безпеці. Метод ENISA дозволяє стратегічно визначити пріоритети.

Прикладом застосування методології в українському дискурсі є дослідження та аналітичний звіт Центру аналізу та розробки ефективних політик [5]. На основі методології ENISA здійснено дослідження та підготовлено аналітичний звіт «Оцінка рівня зрілості кіберосвіти: стан в Україні», на основі якого зроблено висновки: Україна лише на початку шляху до вищих рівнів кіберзрілості освіти; поняття «кібербезпекова освіта» артикулюється на рівні ключових стратегічних документів, зокрема, Стратегії кібербезпеки України; вивчення питань кібербезпеки запроваджено на рівні національного освітнього стандарту, завдяки чому «кібергігієна», як складова, інтегрована в усі освітні програми; в Україні реалізується чимало національних ініціатив спрямованих на підвищення знань учнів, батьків та вчителів з окремих аспектів кібербезпеки. Разом з тим, відмічено брак ефективної моделі оцінки знань школярів щодо якості їх кіберосвіти: немає механізму моніторингу, конкретних показників для оцінки результативності впроваджених освітніх ініціатив з кібербезпеки тощо.

Наукова новизна дослідження полягає у методологічному обґрунтуванні застосування та адаптації моделі ENISA до національного контексту України, що дозволяє використати її як комплексний інструмент оцінювання рівня зрілості кіберосвіти у початковій та середній школі.

Запропоновано авторське бачення етапності національної адаптації методології ENISA, що включає інтеграцію експертних інтерв'ю, аналіз нормативних документів та інструментів оцінювання освітніх результатів. Це створює підґрунтя для розроблення національної моделі оцінювання кіберзрілості освіти.

Запропоновано інтерпретацію кіберосвіти як цифрової платформи соціокультурної взаємодії, що формується на перетині освіти, цифрових компетентностей та громадянської активності. Використання методології ENISA створює умови для розроблення національної "дорожньої карти" кіберосвіти як цифрової платформи, що передбачає побудову цілісної освітньої екосистеми «школа – університет – професія».

Висновки. Методологія ENISA є релевантним та ефективним інструментом для комплексного оцінювання стану кіберосвіти в Україні, оскільки враховує нормативний, стратегічний та операційний аспекти формування цифрової та кібербезпекової компетентності на рівні початкової та середньої освіти.

Інтерпретація кіберосвіти як цифрової платформи дає змогу комплексно оцінити стан української системи, включно з нормативною базою, стратегічною узгодженістю, практиками навчання та механізмами моніторингу. ENISA пропонує модель, що дозволяє охопити ці аспекти системно та порівнювально.

Використання методології дає змогу системно діагностувати сильні й слабкі сторони національної освітньої політики, визначати прогалини у

нормативному забезпеченні, узгодженості стратегій і практичній реалізації навчальних програм.

Подальші дослідження мають бути спрямовані на емпіричну перевірку адаптованої моделі ENISA, розробку інструментарію для регулярного моніторингу знань і створення національної моделі оцінювання рівня кіберосвіти та розроблення національної системи індикаторів, що враховуватиме платформну природу кіберосвіти та її зв'язок з розвитком цифрового громадянства.

Список використаних джерел

1. Даник Ю., Зінченко А. Кіберосвіта та її особливості. *Військова освіта*. 2018. № 2. С. 67–84.

2. Овчарук О. Сучасні підходи до розвитку цифрової компетентності людини та цифрового громадянства в європейських країнах. *Інформаційні технології і засоби навчання*. 2020. Т. 76. № 2. С. 1–13.

3. Пучков О., Уваркіна О. Сталий розвиток системи формальної кіберосвіти: рефлексія сучасних концептів. *Information Technology and Security. January-June* 2023. Vol. 11. Iss. 1 (20). С. 60–68.

4. Уваркіна О. В., Шевчук О. С., Горнійчук І. В. Неформальна кіберосвіта: сучасне «вікно можливостей». *Modern educational strategies under the influence of the development of the information society and European integration* : Scientific monograph. Riga, Latvia : Baltija Publishing, 2024. P. 491–506. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/435/11674/24413-1?inline=1 (дата звернення: 26.10.2025).

5. Центр аналізу та розробки ефективних політик. Оцінка рівня зрілості кіберосвіти: стан в Україні. URL: https://cadep.org.ua (дата звернення: 26.10.2025).

6. AlSanad J. H. Cybersecurity In Education. International Journal of Computer Science and Information Technology Research Vol. 12. Iss. 2. P: 51–61. URL: https://www.researchpublish.com/upload/book/Cybersecurity%20in%20education-27062024-1.pdf (дата звернення: 20.09.2025).

7. Amankwa E. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*. 2021. № 12. P. 233–249. URL: https://doi.org/10.4236/jis.2021.124013 (дата звернення: 19.10.2025).

8. Basholli A., B Mema, Basholli F. The role of education in cyber hygiene July 2023. Conference: 7th Advanced Engineering Days. URL: https://www.researchgate.net/publication/373077128_The_role_of_education_in_cyber_hygiene (дата звернення: 26.09.2025).

9. Cybersecurity Education Maturity Assessment. URL: https://www.enisa.europa.eu/publications/cybersecurity-education-maturity-assessment (дата звернення: 26.08.2025).

10. Digital Citizenship Education (DCE). URL: https://www.coe.int/en/web/education/dce-concept (дата звернення: 26.09.2025).

11. McLuhan M. Understanding Media. The extensions of man. McGraw-Hill, New York, 1964. URL: https://designopendata.wordpress.com/wp-content/uploads/2014/05/understanding-media-mcluhan.pdf (дата звернення: 14.09.2025).

12. Ondrušková D., Pospíšil R. The good practices for implementation of cyber security education for school children Contemporary Educational Technology. 2023. №15(3). P. 435. URL: http://creativecommons.org/licenses/by/4.0/ (дата звернення: 20.10.2025).

13. Triplett W. Addressing Cybersecurity Challenges in Education. January International Journal of STEM Education for Sustainability.2023. № 3(1). P. 47–67 URL: https://www.journal.gmpionline.com/index.php/ijses/article/view/132 (дата звернення: 15.10.2025).

References

1. Danyk, Ju. & Zinchenko, A. (2018). Cyberworld and its particularities. Military Education, 3, 67–84 [in Ukrainian].

2. Ovcharuk, O. (2020). Current approaches to the development of digital competence of people and digital communities in European countries. Information technologies and technologies, 76, 1–13 [in Ukrainian].

3. Puchkov, O. & Uvarkina, O. (2023). Steel development of the system of formal cyber education: reflection of current concepts. January-June 2023, 11 (1) (20), 60–68 [in Ukrainian].

4. Uvarkina, O. V., & Shevchuk, O. S., & Horniichuk, I. V. (2024). Non-formal cyber-education: contemporary 'oportunities window'. In Modern educational strategies under the influence of the development

of the information society and European integration. Baltija Publishing, 491–506. Retrieved from: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/435/11674/24413-1?inline=1 [in Ukrainian].

5. Centre for analysis and development of effective policies. (2025). Assessment of the level of maturity of cyber awareness: a country in Ukraine. https://cadep.org.ua/ [in Ukrainian].

6. AlSanad, J. H. (2024). Cybersecurity in Education. International Journal of Computer Science and Information Technology Research, 12 (2), 51–61. Retrieved from: https://www.researchpublish.com/upload/book/Cybersecurity%20in%20education-27062024-1.pdf [in Ukrainian].

7. Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12, 233–249. DOI: https://doi.org/10.4236/jis.2021.124013 [in English].

8. Basholli, A., Mema, B. & Basholli, F. (2023). The role of education in cyber. Conference: 7th Advanced Engineering Days. Retrieved from: https://www.researchgate.net/publication/373077128_The_role_of_education_in_cyber_hygiene [in English].

9. Cybersecurity Education Maturity Assessment (2024). Retrieved from: https://www.enisa.europa.eu/publications/cybersecurity-education-maturity-assessment [in English].

10. Digital Citizenship Education (DCE) (2025). Retrieved from: https://www.coe.int/en/web/education/dce-concept [in English].

11. McLuhan, M. (1964). Understanding Media. The extensions of man. McGraw-Hill. Retrieved from: https://designopendata.wordpress.com/wp-content/uploads/2014/05/understanding-media-mcluhan.pdf [in English].

12. Ondrušková, D., & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. Contemporary Educational Technology, 15(3), 435. Retrieved from: http://creativecommons.org/licenses/by/4.0/ [in English].

13. Triplett, W. (2023). Addressing Cybersecurity Challenges in Education. January International Journal of STEM Education for Sustainability, 3(1), 47–67. Retrieved from: https://www.journal.gmpionline.com/index.php/ijses/article/view/132 [in English].

Стаття надійшла до редакції 06.11.2025
Отримано після доопрацювання 08.12.2025
Прийнято до друку 16.12.2025
Опубліковано 29.12.2025