DOI: https://doi.org/10.26565/1992-2337-2024-2-21
УДК 355/359

Живило Євген Олександрович,
кандидат наук з державного управління, доцент,
докторант кафедри публічної політики,
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

МЕТОДОЛОГІЯ РОЗРОБКИ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Анотація. З моменту свого створення інформаційно-комунікаційні технології перетворилися на основу сучасного бізнесу, критично важливих послуг та інфраструктури, соціальних мереж і глобальної економіки в цілому.

Як наслідок, національні лідери почали впроваджувати цифрові стратегії та фінансувати проекти, спрямовані на розширення доступу до Інтернету та використання переваг, що випливають з використання інформаційно-комунікаційних технологій, для стимулювання економічного зростання, підвищення продуктивності та ефективності, покращення надання послуг та розширення можливостей, забезпечення доступу до бізнесу та інформації, уможливлення електронного навчання, підвищення кваліфікації персоналу та сприяння належному врядуванню.

Хоча залежність нашого суспільства від цифрової інфраструктури зростає, технології залишаються вразливими за своєю суттю. Конфіденційності, цілісності та доступності інфраструктурі інформаційно-комунікаційних технологій загрожують ризики, що швидко розвиваються. Трансформаційна сила інформаційно-комунікаційних технологій та Інтернету як каталізаторів економічного зростання та соціального розвитку досягла критичної межі, коли довіра громадян та держави до використання ІТ підривається кібербезпекою.

В статті підкреслено важливість узгодження національних стратегій з пріоритетами національної безпеки, зокрема в контексті кібербезпеки. При цьому неправильне балансування між економічними вигодами та ризиками може призвести до загроз національній безпеці та перешкодити досягненню поставлених цілей. Створення Національної стратегії кібербезпеки, що включає пріоритизацію інвестицій та ресурсів, є необхідним для ефективного управління ризиками та забезпечення стійкості національної цифрової екосистеми. Важливим етапом цього процесу є визначення чітких показників для оцінки результатів та забезпечення виконання стратегії в межах бюджетів і термінів.

Ключові слова: національна стратегія, кіберпростір, кібербезпека, кіберзагрози, кібервплив, державно-приватне партнерство.

Як цитувати: Живило Є. О. Методологія розробки національної стратегії кібербезпеки. *Державне будівництво.* 2024. № 2 (36). С. 307–321. DOI: https://doi.org/10.26565/1992-2337-2024-2-21
In cites: Zhyvylo, Y.O. (2024). Methodology for developing a national cybersecurity strategy. *State Formation, no. 2 (36), 307–321.* DOI: https://doi.org/10.26565/1992-2337-2024-2-21 [in Ukrainian].

Постановка проблеми. Сучасне цифрове середовище має великий потенціал для прискорення економічного зростання, соціального прогресу та зміцнення суспільних цінностей, зокрема, покращення надання державних послуг, сприяння міжнародній торгівлі та розвитку належного врядування. Однак зростаюча залежність суспільства від цифрових технологій вимагає підвищеної уваги до кібербезпеки (далі – КБ) [1]. При цьому КБ не повинна розглядатися як самоціль, вона є невід'ємною частиною цілісної стратегії розвитку цифрової екосистеми країни.

Національна стратегія КБ (далі – Стратегія) повинна визнавати важливість захисту прав людини в онлайн-середовищі, адже права, які люди мають в офлайні, повинні бути також захищені в Інтернеті. Важливо, щоб Стратегія була узгоджена з міжнародними правовими нормами, такими як Загальна декларація прав людини та Міжнародний пакт про громадянські і політичні права, а також відповідними регіональними та багатосторонніми нормативно-правовими(ою) актами/базою.

Одним з ключових аспектів Стратегії є забезпечення захисту свободи вираження поглядів, конфіденційності комунікацій і персональних даних [2]. Вона повинна запобігати свавільному та незаконному спостереженню, перехопленню комунікацій або обробці персональних даних. У той же час, Стратегія має забезпечити здатність держави вживати заходи для захисту своїх законних інтересів, дотримуючись при цьому прав людини.

Важливо, щоб будь-які заходи, спрямовані на спостереження, перехоплення повідомлень чи збір даних, здійснювались у рамках чіткої нормативно-правової бази. Це має відбуватись в контексті конкретних розслідувань або судових справ, з дозволу відповідного національного органу і відповідно до публічно доступної, всеосяжної та недискримінаційної правової системи, яка забезпечує належний нагляд, процесуальні гарантії та ефективні засоби правового захисту [3].

Таким чином, Стратегія повинна бути частиною більш широкої національної політики, спрямованої на досягнення соціально-економічних цілей, зміцнення довіри громадян до цифрових технологій та забезпечення безпеки держави в умовах зростаючих кіберзагроз.

Отже, Стратегія має сприяти створенню цифрового середовища, якому громадяни та організації можуть довіряти. Зміцнення довіри до національної цифрової екосистеми, в якій права та інтереси користувачів захищені, а безпека даних і систем функціонує належним чином, має важливе значення для реалізації повного потенціалу соціальних, політичних та економічних можливостей, що відкриваються завдяки використанню інформаційно-комунікаційних технологій. (далі – ІКТ). Стратегія повинна сприяти політиці, процесам і діям на національному рівні з метою надання безпечних критично важливих послуг (включаючи електронне урядування, електронну комерцію, цифрові фінансові транзакції, телемедицину, тощо), що підтримуються ІКТ і використовуються громадянами. Такі дії сприятимуть утвердженню принципу

довіри не лише серед населення, а й серед державних та приватних організацій, які надаватимуть громадянам послуги, пов'язані з ІКТ [4].

Аналіз останніх досліджень і публікацій. Перша спроба сформулювати державну політику в галузі КБ відбулась у 2016 році з затвердженням Стратегії кібербезпеки України на фоні агресії РФ проти України. Документ мав низку прогалин, які позначились на ефективності реалізації поставлених цілей, прогрес у досягненні яких становив лише 40%.

Досвід реалізації Стратегії за п'ять років виявив низку проблем, що завадили її повноцінній імплементації. Однак за цей час відбулись певні позитивні зміни.

Так у 2017 році ухвалено Закон України "Про основні засади забезпечення кібербезпеки України" [5], а у 2020 році затверджено порядок формування переліку об'єктів критичної інформаційної інфраструктури, хоча сам список так і не був сформований. Також було створено спеціалізовані підрозділи в Нацбанку, Міністерстві інфраструктури, СБУ, а Національний координаційний центр КБ при РНБО почав координувати діяльність суб'єктів державного кіберсектору. Налагоджено міжнародне партнерство, зокрема розпочато кібердіалог зі США.

Введення нової Стратегії національної безпеки України 14 вересня 2020 р. стало поштовхом для розробки низки стратегічних документів, серед яких була і Стратегія кібербезпеки України 2021 року. Ця стратегія визначила три основні пріоритети: безпечний кіберпростір (далі – КП), захист прав громадян у цифровому середовищі та інтеграція в європейське та євроатлантичне співтовариство, а також поставила цілі щодо створення дієвої кібероборони, протидії кібертероризму, кіберзлочинності та розвідувально-підривній діяльності, розвитку національної кіберготовності, професійного вдосконалення та міжнародного співробітництва в галузі КБ [2].

У контексті радикальних змін у середовищі безпеки НАТО, яке зміцнює колективну оборону за новим підходом "360 градусів" та розвиває спроможності для багатодоменних операцій, Україна повинна відповідно адаптувати свою оборонну стратегію.

Проект Закону України "Про Кіберсили Збройних Сил України" (від 19.12.2024 р. № 12349) передбачає визначення правового статусу та засад діяльності Кіберсил, які відповідатимуть за кібероборону та захист суверенітету України в КП [6].

Враховуючи, що провідні країни світу запроваджують трирівневу модель кібероборони на політичному, військовому та технічному рівнях, Україні важливо оперативно реагувати на глобальні геополітичні зміни [7]. Створення Стратегії з пріоритизацією інвестицій та ресурсів є необхідним кроком для ефективного управління ризиками та забезпечення стійкості національної цифрової екосистеми.

Мета статті полягає в аналізі та визначені ключових аспектів розробки загальної методології управління ризиками КБ для захисту критично важливої інфраструктури держави, порушення функціонування якої може призвести до

негативних наслідків в системі забезпечення національної безпеки України (далі – НБ України).

В роботі обґрунтовано необхідність створення комплексної Стратегії, яка включає формування узгодженої методології для ефективного управління ризиками. Розробка такої методології дозволить забезпечити єдність дій усіх державних органів та операторів критичної інфраструктури в контексті КБ, підвищуючи їхню здатність оперативно реагувати на нові загрози та мінімізувати потенційні наслідки для НБ України.

Стаття підкреслює важливість дотримання міжнародних стандартів для забезпечення ефективної співпраці між державними та приватними організаціями, зокрема для полегшення обміну інформацією про загрози та ризики. Така співпраця є основою для розробки та впровадження Стратегії, яка повинна визначати та оцінити еволюцію середовища кіберзагроз, а також потенційний вплив і наслідки для критично важливих об’єктів інфраструктури та основних послуг.

Виклад основного матеріалу. Існує декілька національних та міжнародних визначень терміну “кібербезпека”. В статті термін “кібербезпека” означає сукупність інструментів, політик, керівних принципів, підходів до управління ризиками, заходів, тренінгів, найкращих практик, гарантій і технологій, які можуть бути використані для захисту доступності, цілісності та конфіденційності активів у підключених інфраструктурах, що належать уряду, приватним організаціям і громадянам. Зазначені активи включають підключені комп’ютерні пристрої, персонал, інфраструктуру, сервіси, додатки, цифрові послуги, телекомунікаційні системи та дані в цифровому середовищі [8].

В цілому Стратегії КБ можуть приймати різні форми і мати різний рівень деталізації, залежно від цілей і рівня кіберготовності конкретної країни. Тому не існує усталеного і загальноприйнятого визначення того, що являє собою Стратегія.

Спираючись на існуючі дослідження в цій сфері, пропонується розглядати Стратегію як:

– вираз бачення, цілей високого рівня, принципів та пріоритетів, якими керується країна у вирішенні питань КБ;

– огляд зацікавлених сторін, яким доручено покращити КБ країни, та їхніх відповідних ролей і обов’язків;

– опис кроків, програм та ініціатив, які країна буде здійснювати для захисту своєї національної кіберінфраструктури і, в процесі, підвищення її безпеки та стійкості.

Стратегія має важливу роль у забезпеченні синергії між пріоритетами КБ та іншими цілями, пов’язаними з ІКТ. Оскільки КБ є ключовим елементом для досягнення соціально-економічних цілей сучасної економіки, необхідно, щоб вона була органічно інтегрована в загальний контекст розвитку країни [9].

Для цього важливо чітко визначити, яким чином КБ підтримується та реалізується в рамках національних ініціатив. Це може бути досягнуто шляхом посилання на існуючі політики, спрямовані на реалізацію цифрового порядку денного або національних програм розвитку. Оцінка того, як КБ може бути

інтегрована в ці програми, дозволить забезпечити її ефективну реалізацію та посилити роль КБ як невід'ємної частини економічного та соціального прогресу [10].

Зрештою, життєвий цикл Стратегії, як показано на рисунку 1, допомагає розробникам документа зосередитися на стратегічному мисленні щодо КБ на національному рівні. Він містить огляд різних етапів і кроків, розробки Стратегії які необхідно здійснити державі для її розробки, а також можливих механізмів її реалізації відповідно до конкретних потреб і вимог країни, інтегруючи основні принципи та найкращі практики.

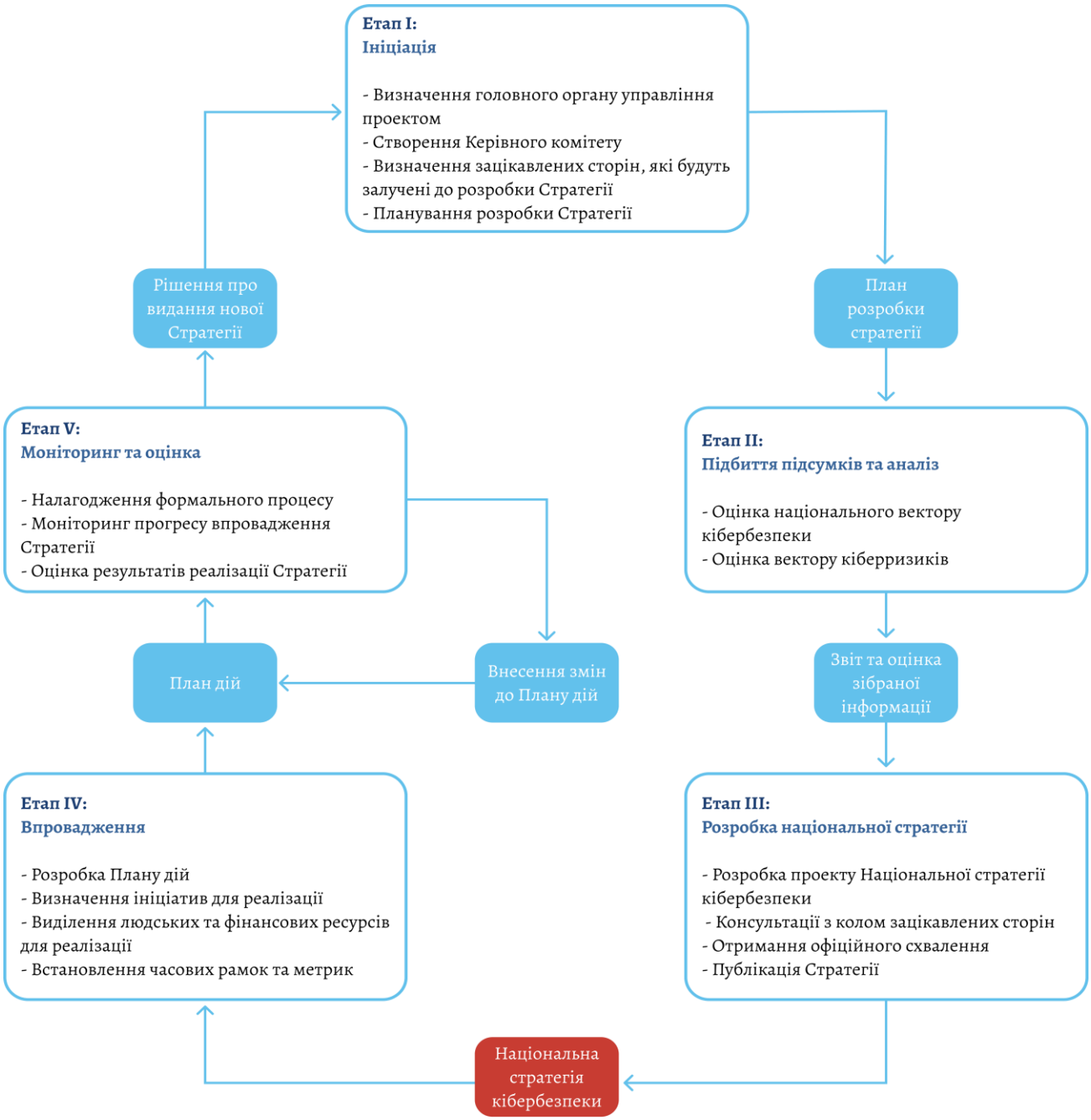

Рисунок 1. – Життєвий цикл Стратегії.
Figure 1. – Strategy Life Cycle.

У подальшому пропонується розглянути кожний етап і крок більш детально. Отже, процес розробки Стратегії має координуватися єдиним компетентним органом, який призначається виконавчою владою. Це може бути вже існуюча або новостворена державна установа, така як міністерство, відомство чи департамент, відповідальний за розробку Стратегії. Цей орган, названий Головним органом проекту (далі – Орган проекту), повинен призначити осіб, відповідальних за керівництво процесом.

Орган проекту повинен залишатися нейтральним у процесі розробки Стратегії, тому рекомендується, щоб він відрізнявся від органу, що буде відповідати за її реалізацію. Також необхідно впровадити механізми для уникнення упередженості та внутрішньої конкуренції за ресурси.

Виконавча влада повинна створити керівний комітет, який працюватиме з Органом проекту над розробкою Стратегії. Комітет матиме повноваження надавати рекомендації та забезпечувати якість процесу. Також він буде відповідати за прозорість та інклюзивність, що відповідає принципу чіткого керівництва, ролей і розподілу ресурсів. Роль, структура та склад керівного комітету мають бути чітко визначені з самого початку.

Оскільки комітету, ймовірно, доведеться працювати з документами з обмеженим доступом, його склад повинен бути відповідним чином сформований. Важливо, щоб склад комітету відображав різні обов’язки, покладені на цей орган, зокрема через старшинство призначень.

Отже, Орган проекту повинен визначити початковий склад зацікавлених сторін (рисунок 2), які братимуть участь у розробці Стратегії, уточнити їхні ролі та визначити механізми співпраці для управління очікуваннями протягом усього процесу.

Під час розробки Стратегії Органу проекту може знадобитися залучення додаткових зацікавлених сторін для використання всіх відповідних знань та досвіду. Це відповідає принципу інклюзивності, який передбачає співпрацю з урядом, приватним сектором та громадськими об’єднаннями/групами. Наприклад, можуть бути залучені ІКТ-компанії, оператори критичної інфраструктури, наукові експерти та неурядові організації, які займаються підвищенням обізнаності щодо КБ [11].

Для координації співпраці Орган проекту може створити консультативний комітет, який буде сприяти призначенню членів керівного комітету та надавати консультації на різних етапах розробки Стратегії. Його склад має бути достатньо різноманітним, щоб включати представників усіх секторів, на які Стратегія матиме вплив.

Окрім того, не виключається можливість залучення міжнародних організацій, неурядових установ та приватних компаній, які можуть допомогти національним урядам у сфері КБ щодо проведення додаткової підтримки чи експертизи [12].

Рисунок 2. – Склад зацікавлених сторін.
Figure 2. – Composition of stakeholders.

Вкрай важливо визначити необхідні людські та фінансові ресурси для розробки та впровадження Стратегії, а також джерела їх отримання. Особливу увагу слід приділити забезпеченню довгострокового фінансування всього життєвого циклу Стратегії, включаючи її розробку, впровадження та вдосконалення.

На завершальному етапі ініціативної фази Орган проекту повинен підготувати план розробки Стратегії. Після його розробки, він має бути поданий на затвердження керівному комітету та Виконавчому органу відповідно до національних процесів управління.

При розробці плану Орган проекту повинен також визначити, чи буде Стратегія прийнята у формі закону чи політики, оскільки це вплине на формальні процеси та терміни її прийняття.

План розробки Стратегії повинен містити основні кроки та заходи, ключові зацікавлені сторони, часові рамки та потреби в ресурсах, зокрема людських і фінансових. У плані розробки має бути чітко зазначено, як і коли відповідні зацікавлені сторони будуть залучені до процесу розробки, виконання встановлених термінів та у разі потреби – коригування.

Метою етапу підбиття підсумків та аналізу є збір даних для оцінки національного ландшафту КБ та поточних і майбутніх кіберризиків, що забезпечить основу для підготовки Стратегії. Результатом цього етапу, який здійснюється консультативним комітетом, є звіт, що містить огляд стратегічного стану національної КБ та ландшафту ризиків, який повинен бути представлений керівному комітету.

Перед початком фактичної підготовки або оновлення тексту Стратегії, Орган проекту має ретельно проаналізувати зібрану інформацію, щоб виявити можливі прогалини в спроможності забезпечення КБ та запропонувати шляхи їх усунення. Результатом цього аналізу повинна бути оцінка того, наскільки існуючі політичні, регуляторні та операційні умови відповідають потребам країни, а також виявлення сфер, де вони є недостатніми [13].

Аналіз також має бути використаний для виявлення конкретних ключових питань, таких як прогалини в освіті та підготовці кадрів у галузі КБ [14]. Нарешті, результатом аналізу має стати оцінка бажаних результатів Стратегії та наявних ресурсів, які можуть бути використані для досягнення цих цілей.

Метою етапу розробки Стратегії є створення тексту Стратегії через активне залучення ключових зацікавлених сторін з державного та приватного секторів, а також громадських об'єднань/груп, шляхом публічних консультацій та робочих груп. Орган проекту координує цей процес, забезпечуючи ефективну співпрацю усіх учасників, які відповідатимуть за визначення загального бачення та обсягу Стратегії.

У рамках цього етапу будуть сформульовані високорівневі цілі, проведено аналіз поточної ситуації та визначено пріоритети з урахуванням їхнього впливу на суспільство, громадян та економіку. Одним із важливих завдань також є забезпечення необхідного фінансування для реалізації визначених цілей Стратегії.

На завершальному етапі розробки Стратегії Орган проекту повинен забезпечити її офіційне затвердження органами виконавчої влади. Процедура затвердження буде залежати від нормативно-правової бази країни і може варіюватися, наприклад, передбачати прийняття через парламентську процедуру або урядову постанову.

Крім того, важливо, щоб Стратегія не лише була схвалена найвищими органами влади, але й зберігала політичну підтримку протягом усієї стадії реалізації. Відповідні посадові особи повинні нести відповідальність за її виконання та отримувати підтримку як у вигляді політичного капіталу, так і ресурсів, що забезпечить ефективну імплементацію Стратегії.

Стратегія повинна бути публічним документом, легко доступним для громадськості. Її впровадження та реалізація має супроводжуватися внутрішніми та зовнішніми заходами з просування, що забезпечить обізнаність про пріоритети та цілі уряду у сфері КБ. Це також підтримуватиме зусилля з підвищення обізнаності з питань КБ [15]. Якщо Стратегія включає план дій, він повинен вказувати на можливості для подальшого залучення та співпраці з громадськими об'єднаннями/групами, приватним сектором і міжнародними партнерами.

Етап реалізації є найважливішим елементом життєвого циклу Стратегії. Для її успішної імплементації необхідний структурований підхід, який включає належне забезпечення людськими та фінансовими ресурсами. Цей етап має бути невід'ємною частиною процесу розробки Стратегії. Основною складовою етапу імплементації є план дій, який регулює виконання запланованих заходів.

Як і у випадку з розробкою Стратегії, її реалізація не може бути виключною відповідальністю одного органу чи установи. Для успішного впровадження необхідне залучення та координація різних зацікавлених сторін в уряді, а також підтримка громадянського суспільства та приватного сектору [16]. План дій, розроблений відповідно до принципу чіткого керівництва, ролей та розподілу ресурсів, може суттєво сприяти ефективному виконанню Стратегії.

Розробка плану дій є майже такою ж важливою, як і сама Стратегія. Цей процес, організований Органом проекту, має стати механізмом для об'єднання відповідних зацікавлених сторін, узгодження цілей і результатів, а також для координації зусиль та об'єднання ресурсів.

Розробка та реалізація Стратегії є безперервним процесом. Компетентний орган повинен розробити офіційний цикл моніторингу та оцінки Стратегії. На етапі моніторингу уряд має забезпечити реалізацію Стратегії відповідно до її плану дій. На етапі оцінювання уряд і національний компетентний орган повинні визначити, чи залишається Стратегія актуальною і відповідає мінливому середовищу ризиків, чи відображає вона цілі уряду, а також які корективи необхідно внести для її оновлення.

Для забезпечення ефективного моніторингу та оцінки реалізації Стратегії уряд повинен визначити незалежний орган, відповідальний за моніторинг прогресу та оцінку ефективності її виконання. Ідеально цей орган має бути залучений до визначення відповідних показників моніторингу та оцінки, що стосуються Стратегії та її плану дій, на етапах підготовки та ініціювання.

Моніторинг і вимірювання ефективності виконання плану імплементації Стратегії мають стати частиною механізмів управління, запроваджених у країні. Постійна оцінка плану (оцінка сталості/коригування) допомагає вдосконалювати Стратегію. Механізми належного врядування повинні чітко розмежовувати підзвітність і відповідальність за успішне виконання. Встановлення метрик або ключових показників ефективності для короткострокових, середньострокових і довгострокових цілей [17] посилює механізми управління і забезпечує прозорість у процесі реалізації Стратегії.

Ключові показники ефективності або метрики повинні бути SMART:

– Конкретними. Вони мають бути націленими на визначену сферу для покращення існуючого стану та зосереджуватися на очікуваних змінах.

– Вимірюваними, а саме кількісно визначати результат або принаймні запропонувати індикатор прогресу.

– Досяжними. Вказувати на реальні, досяжні результати з урахуванням наявних ресурсів.

– Релевантними, фокусуватись на важливих індикаторах прогресу.

– Відповідальними, власне чітко визначати, хто несе відповідальність за досягнення результату.

– Часовими. Необхідно вказувати, коли результат може бути досягнутий.

Встановлення базових показників дозволяє ефективніше відстежувати прогрес і виявляти сфери, які потребують покращення. Крім того, розподіл

бюджетних коштів має відповідати рівню амбіцій та складності бажаного впливу.

Особа, відповідальна за моніторинг реалізації Стратегії, повинна здійснювати його відповідно до узгодженого графіка протягом усього життєвого циклу Стратегії. Результати моніторингу (наприклад, звіт) мають містити інформацію про відхилення від термінів і причини затримок, такі як зміна пріоритетів, недостатнє кадрове забезпечення чи ресурси. Крім того, необхідно періодично інформувати Орган проекту про хід реалізації Стратегії за різними напрямками. Усі відповідні зацікавлені сторони мають бути активно залучені до цього процесу.

Такий підхід забезпечує підзвітність зацікавлених сторін і дозволяє на ранніх етапах виявляти проблеми, що виникають під час реалізації. Це дасть змогу уряду своєчасно коригувати ситуацію або адаптувати плани на основі отриманих результатів.

Окрім оцінки прогресу за узгодженими показниками, важливо періодично оцінювати результати та порівнювати їх з початково поставленими цілями. Це дає змогу зрозуміти, чи досягнуті цілі Стратегії, або чи потрібні додаткові заходи.

У рамках цього процесу також необхідно регулярно переоцінювати середовище ризиків, щоб виявити можливий вплив зовнішніх змін на результати Стратегії. Це фактично є постійним переглядом профілю ризиків країни.

Результати оцінки, разом з рекомендаціями, мають бути представлені у вигляді звіту для Органу проекту. Звіт повинен включати пропозиції щодо оновлення плану дій, щоб він залишався актуальним і відповідав змінюваній політиці та ландшафту ризиків.

Зрештою, звіти, підготовлені протягом життєвого циклу Стратегії, повинні стати основою для загального огляду Стратегії згідно з графіком, встановленим на етапі ініціювання. Цей огляд повинен враховувати досягнутий прогрес, зміни в зовнішньому середовищі та переоцінку пріоритетів і цілей уряду.

Отже, запропонована методологія розробки Стратегії є важливим інструментом для узгодження пріоритетів КБ з іншими цілями, що стосуються сучасних ІКТ. Сьогодні КБ має вирішальне значення для досягнення соціально-економічних цілей сучасного громадянського суспільства, тому Стратегія повинна чітко відображати, яким чином ці цілі можуть бути досягнуті. У статті враховано існуючі політики, які сприяють реалізації цифрового і національного розвитку, а також розглянуто можливості інтеграції КБ в ці політики для забезпечення їх ефективності.

Пріоритети Стратегій кібербезпеки можуть суттєво відрізнятися залежно від конкретних умов та балансу в якому перебуває кожна країна. У той час як для однієї країни основним завданням може бути захист критичної інфраструктури, для іншої пріоритетними напрямками можуть стати захист

інтелектуальної власності, зміцнення довіри в онлайн-середовищі або підвищення обізнаності громадськості щодо кіберзагроз. Тому важливо враховувати, що дана методика може комбінувати кілька таких аспектів, залежно від специфічних потреб та викликів, що постають перед країною.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Сучасні ІКТ стали основою для розвитку бізнесу, інфраструктури, соціальних мереж і глобальної економіки. Вони сприяють економічному зростанню, підвищенню ефективності державних послуг, розширенню доступу до інформації та бізнесу, а також розвитку освіти і підвищенню кваліфікації персоналу.

Однак, попри численні переваги, ці технології мають значні вразливості, зокрема перед різноманітними кіберзагрозами. Сучасний потенціал ІКТ досяг критичної точки, коли КБ стала ключовим фактором довіри до цифрових технологій.

Відповідно, важливим аспектом Стратегій є узгодження пріоритетів КБ з цілями НБ України. Неправильне балансування між економічними вигодами від технологічних досягнень і потенційними кіберризиками може серйозно вплинути на НБ будь-якої держави з подальшим ускладненням досягнення нею власних стратегічних цілей.

На сьогоднішній день провідні країни активно розвивають як наступальні, так і оборонні спроможності для захисту від незаконної і протиправної діяльності в КП та попередження інцидентів до того, як вони можуть завдати шкоди [18]. Ця стаття зосереджена на оборонних заходах, зокрема на розробці Стратегій.

Розробка за новими принципами, чи корегування існуючої Стратегії є вимогою сучасності щодо ефективного управління кіберризиками та забезпечення сталого функціонування національної цифрової інфраструктури. Ключовими елементами цього процесу є пріоритизація інвестицій у КБ, а також встановлення чітких показників для оцінки результатів, що дозволить здійснювати моніторинг прогресу та забезпечити виконання Стратегії в межах визначених бюджетів і термінів.

Отже, для ефективної побудови системи захисту інформації та КБ необхідно інтегрувати ці заходи в загальну національну стратегію розвитку, визначити ключові пріоритети та забезпечити необхідні ресурси для їх реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber risk management technology to strengthen the information security of the national economy, S. Onyshchenko, Ye. Zhyvylo, A. Hlushko, S. Bilko. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. No 5. С. 136–142.

2. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 28.10.2024).

3. Живило Є. О. Геостратегічні гравці сучасного кіберпростору. загрози, виклики, наслідки : монографія. C91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. pp. 29–63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (дата звернення: 28.10.2024).

4. Живило Є. О., Орлов О. В. Сутність кібербезпеки національного сегменту кіберпростору держави в умовах кризового управління. Публічне управління XXI століття в умовах гібридних загроз : зб. наук. матер. XXII Міжнар. наук. конгресу, 27 квітня 2022 р. Київ : ХНУ імені В. Н. Каразіна, 2022. С. 248–254.

5. Закон України від 05.10.2017 р. № 2469-VIII. "Про основні засади забезпечення кібербезпеки України": Дата оновлення: 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.10.2024).

6. Проект Закону України від 19.12.2024 № 12349, "Про Кіберсили Збройних Сил України" URL: https://ips.ligazakon.net/document/ji12124a?an=2 (дата звернення: 28.10.2024).

7. Живило Є. О., Докіль В. М. Нормативно-правові шляхи вирішення існуючих колізій у сфері кібербезпеки в умовах створення кіберсил Збройних Сил України. *Збірник наукових праць "Теорія та практика державного управління"*. 2024. Вип. 1 (78). С. 183–196. DOI: http://doi.org/10.26565/1727-6667-2024-1-11

8 Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologie*s. 2022. 5(9-119)). P. 34–44.

9. The EY/IIF global risk management survey results surface new challenges faced by today's CRO as their strategic and tactical remit expands. URL: https://www.ey.com/en_gl/industries/banking-capital-markets/ey-iif-global-bank-risk-management-survey

10. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 5 (13 (125)). P. 65–76.

11. Mahdi Q. A., Zhyvotovskyi R., Kravchenko S., Borysov I., Panchenko I., Zhyvylo Y., Kupchyn A., Koltovskov D., Boholii S. (2021). Development of a method of structural-parametric assessment of the object state. *Eastern-European Journal of Enterprise Technologies*. 5 (4 (113)). P. 34–44. DOI: https://doi.org/10.15587/1729-4061.2021.240178

12. Постанова Кабінету міністрів України від 11 листопада 2020 р. № 1176 "Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом". URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

13. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. Дата оновлення: 04.04.2023. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 (дата звернення: 28.10.2024).

14. Zhyvylo Y. Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. *Pressing Problems of Public Administration.* 2023. 2(63). С. 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08

15. Zhyvylo Y. O., & Zhyvylo I. O. Joint training of the cyber security defense forces personnel in the conditions of total state defense. *Theory and Practice of Public Administration.* 2021. 2(73). 144–153. DOI: https://doi.org/10.34213/tp.21.02.16

16. Данілов О. Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни. 2020. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html (дата звернення: 28.10.2024).

17. Живило Є. О., Черноног О. О. Стратегія кібероборони України. *Збірник наукових праць ВІТІ*. 2017. № 4. С. 30–37. URL: https://www.researchgate.net/publication/380979172_STRATEGIA_KIBEROBORONI_UKRAINI (дата звернення: 28.10.2024).

18. Живило Є. О., Докіль В. М. Організаційно-функціональні трансформації кіберсил геостратегічних гравців світового кіберпростору. C91 Moderní aspekty vědy: XLIX. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. P. 218–263. URL: http://perspectives.pp.ua/public/site/mono/mono-49.pdf

Стаття надійшла до редакції 30.10.2024 р.
Стаття рекомендована до друку 02.12.2024 р.

Zhyvylo Y. O.,
PhD in Public Administration, Associate Professor,
doctoral candidate the Public Policy Department,
Education and Research Institute of Public Administration
of V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

METHODOLOGY FOR DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

Annotation. Since their inception, ICTs have become the foundation of modern business, critical services and infrastructure, social networks and the global economy as a whole.

As a result, national leaders have begun to implement digital strategies and finance projects aimed at expanding access to the Internet and harnessing the benefits of ICTs to stimulate economic growth, increase productivity and efficiency, improve service delivery and empowerment, ensure access to business and information, enable e-learning, improve workforce skills and promote good governance.

While our societies are increasingly dependent on digital infrastructure, technologies remain inherently vulnerable. The privacy, integrity and availability of ICT infrastructure are threatened by rapidly evolving risks. The transformative power of information and communication technologies and the Internet as catalysts for economic growth and social development has reached a critical point, when the trust of citizens and the state in the use of IT is undermined by cybersecurity.

The author emphasizes the importance of aligning national strategies with national security priorities, particularly in the context of cybersecurity. The wrong balance between economic benefits and risks can lead to threats to national security and hinder the achievement of set goals. The creation of a National Cybersecurity Strategy, which includes prioritizing investments and resources, is necessary for effective risk management and ensuring the sustainability of the national digital ecosystem. An important stage in this process is the definition of clear indicators for assessing results and ensuring the implementation of the strategy within budgets and deadlines.

Keywords: national strategy, cyberspace, cybersecurity, cyber threats, cyber impact, public-private partnership.

REFERENCES

1. Onyshchenko, S., Zhyvylo, Ye., Hlushko, A., Bilko, S. (2024). Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, no 5. 136–142.*

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14.05.2021 r. "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. (2021). URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 28.10.2024). [in Ukrainian].

3. Zhyvylo, Ye.O. (2024). Heostratehichni hravtsi suchasnoho kiberprostoru. Zahrozy, vyklyky, naslidky: Monohrafiia. C91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o. 29–63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (data zvernennia: 28.10.2024). [in Ukrainian].

4. Zhyvylo,Ye.O., Orlov, O.V. (2022). Sutnist kiberbezpeky natsionalnoho sehmentu kiberprostoru derzhavy v umovakh kryzovoho upravlinnia. *Publichne upravlinnia KhKhI stolittia v umovakh hibrydnykh zahroz: zbirnyk naukovykh materialiv KhKhII Mizhnarodnoho naukovo-ho konhresu 27 kvitnia 2022 r.* Kyiv: Kharkivskyi natsionalnyi universytet imeni Vasylia Nazarovycha Karazina, *248–254.*

5. Zakon Ukrainy vid 05.10.2017 r. № 2469-VIII. "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy": Data onovlennia: 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 28.10.2024).

6. Proekt Zakonu Ukrainy vid 19.12.2024 № 12349. "Pro Kibersyly Zbroinykh Syl Ukrainy". URL: https://ips.ligazakon.net/document/ji12124a?an=2 (data zvernennia: 28.10.2024).

7. Zhyvylo, Ye.O., Dokil, V.M. (2024). Normatyvno-pravovi shliakhy vyrishennia isnuiuchykh kolizii u sferi kiberbezpeky v umovakh stvorennia kibersyl Zbroinykh Syl Ukrainy *Teoriia ta praktyka derzhavnoho upravlinnia, vyp. 1 (78), 183–196.* DOI: http://doi.org/10.26565/1727-6667-2024-1-11 [in Ukrainian].

8. Koval, M., Sova, O., Orlov, O., Zhyvylo, Y., Zhyvylo, I. (2022). Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies. 5(9-119), 34–44.*

9. The EY/IIF global risk management survey results surface new challenges faced by today's CRO as their strategic and tactical remit expands [Elektronnyi resurs]. – Rezhym dostupu: URL: https://www.ey.com/en_gl/industries/banking-capital-markets/ey-iif-global-bank-risk-management-survey

10. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies, vol. 5 (13 (125)), 65–76.*

11. Mahdi, Q.A., Zhyvotovskyi, R., Kravchenko, S., Borysov, I., Oleksandr, O., Panchenko, I., Zhyvylo, Y., Kupchyn, A., Koltovskov, D., Boholii, S. (2021). Development of a method of structural-parametric assessment of the object state. *Eastern-European Journal of Enterprise Technologies, 5 (4 (113)), 34–44.* DOI: https://doi.org/10.15587/1729-4061.2021.240178

12. Postanova Kabinetu ministriv Ukrainy vid 11 lystopada 2020 r. № 1176 "Pro zatverdzhennia Poriadku provedennia ohliadu stanu kiberzakhystu krytychnoi informatsiinoi infrastruktury, derzhavnykh informatsiinykh resursiv ta informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom". URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

13. Poriadok reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori: Postanova Kabinetu Ministriv Ukrainy vid 04.04.2023 r. № 299. Data onovlennia:

04.04.2023. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 (data zvernennia: 28.10.2024).

14. Zhyvylo Y. (2023). Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. *Pressing Problems of Public Administration, 2(63), 111–127*. DOI: https://doi.org/10.26565/1684-8489-2023-2-08 (data zvernennia: 28.10.2024). [in Ukrainian].

15. Zhyvylo, Y.O., & Zhyvylo, I.O. (2021). Joint training of the cyber security defense forces personnel in the conditions of total state defense. *Theory and Practice of Public Administration, 2(73), 144–153*. DOI: https://doi.org/10.34213/tp.21.02.16

16. Danilov, O. (2020). Kiberzakhyst derzhavnykh informatsiinykh resursiv – vazhlyva skladova u protsesi tsyfrovoi transformatsii krainy. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html (data zvernennia: 28.10.2024). [in Ukrainian].

17. Zhyvylo Ye.O., Chernonoh O.O. (2017). Stratehiia kiberoborony Ukrainy. *Zbirnyk naukovykh prats VITI, no. 4, 30–37*. URL: https://www.researchgate.net/publication/380979172_STRATEGIA_KIBEROBORONI_UKRAINI (data zvernennia: 28.10.2024). [in Ukrainian].

18. Zhyvylo, Ye.O., Dokil, V.M. (2024). Orhanizatsiino-funktsionalni transformatsii kibersyl heostratehichnykh hravtsiv svitovoho kiberprostoru. C91 Moderní aspekty vědy: XLIX. Díl mezinárodní kolektivní monografie. Mezinárodní Ekonomický Institut s.r.o.. Česká republika: *Mezinárodní Ekonomický Institut s.r.o., 218–263*. URL: http://perspectives.pp.ua/public/site/mono/mono-49.pdf [in Ukrainian].

The article was received by the editors 30.10.2024.
The article is recommended for printing 02.12.2024.