DOI: https://doi.org/10.26565/1992-2337-2025-1-17
УДК 354.1

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

ПРІОРИТЕТНІ НАПРЯМИ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ІНТЕГРАЦІЇ ДО ТРИРІВНЕВОЇ МОДЕЛІ КІБЕРОБОРОНИ

Анотація. У сучасному цифровому середовищі "зацікавлені сторони" отримують значні економічні та соціальні переваги, однак водночас стикаються з дедалі зростаючими ризиками у сфері кібербезпеки. Проблема полягає в тому, що стрімкий розвиток інформаційно-комунікаційних технологій випереджає здатність держав регулювати та ефективно захищати цифровий простір від новітніх загроз. Відсутність комплексного розуміння цифрового середовища, адаптованого до конкретних умов та національних пріоритетів, створює суттєві перешкоди для забезпечення безпечного функціонування критичних інформаційних інфраструктур і цифрових послуг.

Кібербезпека є не лише технічним, а й багатовимірним суспільним викликом, що охоплює аспекти національної та міжнародної безпеки, правозастосування, зовнішньої політики, цифрової економіки та сталого розвитку. Провідні держави світу активно інвестують у розвиток як оборонних, так і активних кіберспроможностей наступального характеру, визнаючи важливість стратегічного контролю над цифровим простором. Це створює потребу для інших країн формувати власні адаптивні та проактивні підходи до кіберзахисту.

Аналіз наявних в відкритому доступі національних стратегій кібербезпеки, демонструє значну варіативність у визначенні пріоритетів: від захисту критичної інфраструктури до протидії крадіжці інтелектуальної власності, зміцнення довіри до цифрових платформ і підвищення кіберграмотності населення. Успішні приклади свідчать про ефективність комплексного підходу, який поєднує зазначені напрями з урахуванням національних особливостей.

У цьому контексті розробка та реалізація Національної стратегії кібербезпеки набуває особливої важливості. Вона дозволяє системно узгодити кібербезпекові цілі з ширшими завданнями цифрової трансформації держави, передбачити механізми реалізації політик, визначити необхідні ресурси та забезпечити їх ефективне використання.

Як цитувати: Живило Є. О. Пріоритетні напрями Національної стратегії кібербезпеки в контексті інтеграції до трирівневої моделі кібероборони. *Державне будівництво. 2025. № 1 (37).* С. 229–252. DOI: https://doi.org/10.26565/1992-2337-2025-1-17

In cites: Zhyvylo, Ye.O. (2025). Priority Areas of the National Cybersecurity Strategy in the Context of Integration into the Three-Tier Cyber Defense Model. *State Formation, no. 1 (37), 229–252.* DOI: https://doi.org/10.26565/1992-2337-2025-1-17 [in Ukrainian].

Такий стратегічний підхід є ключовим фактором підвищення стійкості національного кіберпростору до сучасних і майбутніх викликів.

Ключові слова: стратегія, об'єкти критичної інфраструктури, об'єкти критичної інформаційної інфраструктури, інформаційно-комунікаційні технології, інформаційна безпека, кібербезпека, кібервплив, кіберризики.

Постановка проблеми. У сучасному світі кіберзагрози (далі – КЗаг) набувають дедалі більшого масштабу, складності та динаміки, охоплюючи як технічні аспекти, так і соціальні, політичні та економічні виміри. Їх еволюція становить серйозну загрозу для безпеки державних інституцій, приватного сектору та громадянського суспільства. В умовах глобалізації та цифрової трансформації держав, особливо в період збройних конфліктів нового покоління, зростає потреба у створенні надійної системи захисту національних інтересів у кіберпросторі (далі – КП), що базується на цілісному, інтегрованому підході.

Одним із ключових інструментів забезпечення кіберстійкості держави є розробка та впровадження Національної стратегії кібербезпеки (далі – Стратегія), яка має ґрунтуватися на трирівневій моделі кібероборони (далі – КО) – на рівнях держави, бізнесу та суспільства. Такий підхід забезпечує багатокомпонентну відповідь на загрози, дозволяючи враховувати специфіку функціонування об'єктів критичної інфраструктури (далі - ОКІ) та критичної інформаційної інфраструктури (далі - ОКІІ).

Однак нинішній стан системи кібербезпеки (далі – КБ) в Україні характеризується рядом суттєвих проблем. По-перше, спостерігається фрагментованість та недостатня координація дій між суб'єктами КБ, що ускладнює оперативне реагування на КЗаг. По-друге, існує нестача ефективних систем раннього виявлення, моніторингу та протидії новим типам атак, особливо в умовах воєнного часу. По-третє, наявні міжнародні та національні нормативно-правові бази (далі – НПБ) є недостатньо адаптованими до сучасних реалій кіберсередовища та не забезпечують належного правового механізму взаємодії між усіма залученими сторонами.

З огляду на вищезазначене, постає нагальна потреба у вдосконаленні підходів до формування національної КБ шляхом розробки Стратегії, інтегрованої до трирівневої моделі КО. Це передбачає не лише визначення чітких завдань для кожного рівня взаємодії, а й формування єдиної концепції захисту ОКІ та ОКІІ, розвиток міжсекторального партнерства, зміцнення нормативно-правової бази та впровадження сучасних технологій кіберзахисту.

Таким чином, системне вирішення виявлених проблем потребує цілеспрямованої державної політики у сфері КБ, орієнтованої на довгостроковий розвиток національного потенціалу у сфері кібероборони, посилення міжнародного співробітництва та створення адаптивної, стійкої та динамічної системи реагування на сучасні КЗаг.

Аналіз останніх досліджень і публікацій. Останнє десятиліття XX століття ознаменувалося глибокими трансформаціями у світовій геополітиці, що дало старт новим формам конкуренції за глобальне лідерство. Відбулися зміни у пріоритетах держав щодо збереження могутності, зокрема у військовій, економічній, технологічній та інформаційно-культурній сферах. Зокрема, Сполучені Штати Америки залишаються провідним гравцем на міжнародній арені, зосереджуючи зусилля на просуванні демократії та збереженні впливу на західну частину Євразії. У той же час Франція та Німеччина залишаються ключовими гравцями в європейському регіоні, а Китай дедалі активніше формує свій статус як центральна геополітична сила в азійсько-тихоокеанському регіоні [1].

Глобальне протистояння між ключовими геополітичними акторами дедалі більше зміщується у площину кіберпростору, який стає ареною для стратегічного суперництва. Дослідження свідчать, що такі країни, як Китай, Росія, Іран і Північна Корея, активно використовують свої кіберспроможності для досягнення політичної, військової та економічної переваги. Вони реалізовують заходи пов'язані з кібершпигунством, здійснюють атаки на критичну інфраструктуру і проводять кампанії впливу, спрямовані на дестабілізацію внутрішніх процесів в інших країнах [1]. Така активність створює безпрецедентний тиск на державні системи безпеки та вимагає нових форм захисту на всіх рівнях.

Окрему увагу вчені та аналітики приділяють доступності комерційних кіберінструментів, які дозволяють навіть неспеціалізованим суб'єктам здійснювати складні кібератаки. Це спричиняє зростання неатрибутивної кіберактивності, що ускладнює виявлення джерел загроз і підвищує ризик неетичної реакції з боку як урядових, так і приватних структур.

У контексті сучасних гібридних загроз Україна змушена активно розвивати власний кіберпотенціал. Провідні українські дослідники та практики вказують на необхідність формування ефективної системи кібероборони, інтегрованої до загальної архітектури національної безпеки. Важливим кроком у цьому напрямі стало подання Проєкту Закону України "Про Кіберсили Збройних Сил України" від 19.12.2024 р. № 12349 [2], який визнає КП не лише об'єктом, а й середовищем воєнного протистояння. Законодавча ініціатива передбачає створення кіберпідрозділів у складі Збройних Сил України за стандартами НАТО, що є важливим кроком до забезпечення ефективної КО держави.

Також слід відзначити важливість формування належного правового поля для розвитку національних кіберспроможностей - аспект, на якому послідовно акцентується увага у сучасній науковій літературі. Значна частина публікацій стосується необхідності оновлення нормативно-правової бази відповідно до нових реалій. Дослідники підкреслюють, що без чіткого законодавчого регулювання кібероперацій, питання координації між органами державної

влади, приватним сектором та громадянським суспільством залишається відкритим.

Однак, незважаючи на наявність окремих стратегічних документів, сучасні наукові розвідки недостатньо системно висвітлюють взаємозв'язок між національними стратегіями кібербезпеки та практичним механізмом реалізації трирівневої моделі КО. Це створює наукову нішу для подальших досліджень, пов'язаних із формуванням інтегрованої системи державного управління КБ, здатної ефективно реагувати на динамічний характер КЗаг.

Таким чином, аналіз сучасних досліджень і публікацій свідчить про необхідність перегляду пріоритетів національної кіберстратегії, з урахуванням змін у глобальному безпековому середовищі. При цьому нагальною потребою є розробка дієвих механізмів державного регулювання систем захисту інформації та КБ, що базуються на принципах адаптивності, інтегрованості та відповідності сучасним викликам. У цьому контексті основними завданнями є підвищення кіберстійкості країни, забезпечення надійного захисту її КІ, послуг та цифрових активів, що в сукупності є ключовими елементами національної безпеки в умовах цифрової епохи.

Метою статті є визначення пріоритетних напрямів Національної стратегії кібербезпеки України в контексті її інтеграції до трирівневої моделі кібероборони, а також обґрунтування необхідності формування ефективного державного механізму управління у сфері кібербезпеки.

За цих умов, особливої уваги приділено аналізу нормативно-правових, інституційних та організаційно-технологічних аспектів забезпечення кіберстійкості країни, а також розробці практичних рекомендацій щодо удосконалення національної системи кіберзахисту з урахуванням сучасних гібридних загроз і кращих міжнародних практик.

Виклад основного матеріалу. КБ має суттєвий вплив на багато сфер соціально-економічного розвитку, при цьому вона схильна до ризиків, зумовлених низкою факторів у національному контексті. В статті представлено набір елементів передового досвіду, які можуть представити Стратегію всеосяжною та ефективною, дозволяючи при цьому адаптувати її до національного контексту.

Зазначені елементи передового досвіду згруповані в окремі пріоритетні напрямки, які фактично є наскрізними тематиками для Стратегії. Хоча як пріоритетні напрямки, так і елементи передового досвіду наведені лише, як приклади. Тому особливо важливо, щоб визначені елементи розглядалися в контексті національних реалій, оскільки деякі з них можуть виявитися неактуальними або не відповідати сучасним вимогам, зважаючи на специфіку поточної ситуації.

Запропонована методика розробки Стратегії зосереджена виключно на алгоритмі її відпрацювання. Робочий орган відповідних представників розробки Стратегії повинен визначити та дотримуватися елементів належної практики, що відповідають власним цілям і пріоритетам держави, ґрунтуючись на

баченнях, визначених у національних стратегіях та концепціях. Порядок окремих елементів або пріоритетних напрямків, що наведено нижче, не слід розглядати як індикатор їхнього рівня важливості або пріоритетності.

Таким чином, у рамках узагальненої моделі Стратегії доцільно передбачити сім основних пріоритетних напрямів, а саме:

Пріоритетний напрям 1 – Управління. Цей пріоритетний напрямок представляє елементи передового досвіду, які слід розглянути для включення в текст Стратегії при розгляді структури управління національною КБ (включаючи всі організації, які мають обов'язки та повноваження щодо розвитку цифрової економіки та зменшення ризиків кібернетичної незахищеності). Не буде перебільшенням сказати, що сьогодні лідером є той суб'єкт фінансового ринку, який більш технологічно розвинутий, приділяє особливу увагу високоякісному та стійкому обслуговуванню рахунків, проведенню споживчих готівкових і безготівкових операцій [3].

У Стратегії мають бути чітко визначені цілі та результати, яких уряд прагне досягти для підвищення стійкості країни та зменшення ризиків для КІ, послуг та активів. Стратегія повинна чітко визначати ролі та обов'язки зацікавлених сторін, відповідальних за її реалізацію, та запроваджувати заходи для забезпечення підзвітності органів влади та посадових осіб за реалізацію, моніторинг, оцінку та досягнення результатів Стратегії.

З цією метою Стратегія повинна визначити компетентний орган, відповідальний за виконання Стратегії, та надати йому відповідні повноваження; створити механізм для визначення державних органів, на які впливає реалізація Стратегії або які несуть за неї відповідальність; зобов'язати включити до плану реалізації Стратегії конкретні, вимірювані, досяжні, орієнтовані на результат та часові рамки цілі; визнати необхідність виділення ресурсів (наприклад, політичної волі, фінансування, часу та людей) для досягнення бажаних результатів.

Вкрай важливо забезпечити найвищий рівень підтримки. Стратегія повинна мати офіційне схвалення на найвищому державному рівні. Таке схвалення переслідує дві важливі мети. По-перше, вона підвищує ймовірність виділення достатніх ресурсів і успішної координації зусиль. По-друге, воно сигналізує ширшій національній екосистемі про те, що КБ країни взаємопов'язана з її цифровою економікою та іншими соціальними і політичними аспектами, які залежать від цифрових систем, і повинна бути національним пріоритетом.

Можливо, Стратегію також потрібно буде кодифікувати у національній правовій базі, щоб забезпечити її актуальність та пріоритетність на національному рівні.

За цих умов необхідно створити компетентний орган, відповідальний за питання КБ. Саме Стратегія повинна визначати цей спеціальний національний орган, який буде відповідати за її реалізацію. Керівництво органом має здійснювати досвідчена особа, яка забезпечить ефективне керівництво,

координацію дій та контроль за виконанням Стратегії, зокрема на найвищому державному рівні. Компетентний орган також повинен нести відповідальність за звітування, хід і результати реалізації Стратегії.

Такий національний компетентний орган повинен також виступати в ролі органу управління, який визначає ролі, обов'язки, процеси, права на прийняття рішень і завдання, необхідні для забезпечення ефективної реалізації Стратегії. Це включає визначення зацікавлених сторін, які здійснюватимуть нагляд за реалізацією Стратегії, а також встановлення цільових показників ефективності для різних міністерських або урядових департаментів, установ або окремих осіб, відповідальних за конкретні аспекти Стратегії та подальшого плану дій. У деяких випадках позиція національного компетентного органу з питань КБ може бути формалізована в політиці або законі, щоб надати йому повноваження для виконання покладених на нього завдань.

Враховуючи той факт, що КБ перетинається з багатьма різними сферами, важливо забезпечити, щоб національний компетентний орган мав можливість залучати та спрямовувати відповідні зацікавлені сторони. Для реалізації зазначеного завдання можливо знадобиться додаткове нормативно-правове регулювання, яке зобов'яже державні органи звітувати перед національним компетентним органом про хід виконання та досягнення визначених результатів. При цьому, прорахунок ключових показників ефективності стане ефективним інструментом для оцінки прогресу та результативності виконання запланованих заходів.

У рамках забезпечення міжвідомчої співпраці необхідно розробити механізм для визначення та залучення державних установ, на діяльність яких безпосередньо впливатиме реалізація Стратегії. Це дозволить ефективно координувати дії різних органів влади та забезпечити їхню активну участь у виконанні завдань.

Внутрішньоурядова прихильність, координація та співпраця є основними функціями цих державних установ, необхідними для забезпечення того, щоб механізми управління (наприклад, стандарти, нормативно-правові акти, ринкові стимули, тощо) та ресурси давали бажані результати, передбачені Стратегією. Залучення представників Національної системи КБ забезпечить посилення внутрішньоурядової координації та співпраці.

Ефективна комунікація та координація гарантують, що всі міністерства та урядові установи будуть обізнані з відповідними повноваженнями, місіями та завданнями один одного. Прикладом механізму координації може бути проведення періодичних зустрічей за участю всіх зацікавлених сторін для спільного перегляду планів дій. Прикладом механізму співпраці може бути створення внутрішньоурядової робочої групи для вирішення конкретного питання. Прикладом прихильності є узгодженість між внутрішньою і зовнішньою політикою країни, щоб одне міністерство не підривало довіру до іншого, представляючи різні позиції з одного і того ж питання (наприклад,

торговельні потоки проти експортного контролю над технологіями подвійного використання).

Розглядаючи забезпечення міжсекторальної співпраці Стратегія повинна відображати розуміння залежності уряду від приватного сектору та інших національних неурядових зацікавлених сторін (і навпаки) у досягненні більш захищеної, безпечної та стійкої екосистеми (принцип інклюзивності). З цією метою в Стратегії має бути чітко визначено, як уряд залучатиме ці різні зацікавлені сторони, а також їхні ролі та обов'язки. Наприклад, Стратегія повинна передбачити розгортання мережі базових індикаторів стану КБ в ключових галузях, що є необхідним для забезпечення функціонування та відновлення критично важливих послуг і інфраструктури.

Стратегія має бути узгоджена з іншими національними пріоритетами, такими як забезпечення доступності, наявності та інклюзивності зв'язку; захист даних і приватності з одночасним просуванням інновацій; посилення стійкості інфраструктури та доступності послуг до катастроф, зміни клімату та пандемій; вивчення нових технологій, таких як штучний інтелект, блокчейн, квантові обчислення тощо.

Стратегія повинна передбачати виділення спеціальних бюджетних коштів та відповідних ресурсів для її реалізації, підтримки та періодичного перегляду. Забезпечення достатнього, послідовного та безперервного фінансування є основою для побудови ефективної Національної системи КБ.

Ресурси для реалізації Стратегії повинні бути визначені через фінансовий еквівалент (спеціальний бюджет), людські ресурси та матеріально-технічне забезпечення. Успішне виконання також залежить від політичної підтримки та лідерства, що базуються на надійних партнерських відносинах. Цілі та завдання Стратегії не можна розглядати як одноразовий розподіл ресурсів. Потреба в ресурсах повинна регулярно переглядатися, з урахуванням прогресу або труднощів у виконанні поставлених завдань та досягненні цілей.

Уряд може розглянути можливість створення централізованого бюджету для КБ, який управлятиметься єдиним центральним органом. Це може бути як об'єднання різних джерел фінансування в узгоджену програму, так і створення єдиного внутрішньодержавного бюджету. Важливо, щоб загальна програма КБ була чітко керована та контрольована через визначення проміжних етапів, що дозволить забезпечити її успішну реалізацію.

Не менш важливою складовою є супроводження Стратегії детальним планом її реалізації, який описує, як будуть досягатися стратегічні цілі, або містить посилання на нього. Ефективні плани імплементації визначають відповідальні організації за виконання кожного завдання та мети, ресурси, необхідні для їх виконання в межах конкретних термінів (короткострокових, середньострокових, довгострокових), а також процеси, які будуть використовуватися, і очікувані результати.

Пріоритетний напрям 2 – Управління ризиками у сфері національної КБ. У цьому пріоритетному напрямі представлено передовий досвід забезпечення

КБ через управління ризиками. Як зазначалося вище, необхідно застосовувати підхід до управління ризиками, оскільки кіберризики (Далі - КРр) неможливо повністю усунути. Замість цього, забезпечення належного розуміння всіх можливих ризиків дозволить ефективно ними управляти. Оцінка ризиків повинна зосереджуватися на виявленні взаємозалежностей і враховувати ризики, що виникають через залежності за межами національних кордонів. Підхід до управління ризиками має охоплювати весь життєвий цикл, починаючи від розробки або закупівлі і до експлуатації та заміни.

Важливо також зазначити, що, оскільки загрози КБ є надзвичайно динамічними та непередбачуваними, будь-який підхід до управління ризиками повинен регулярно переглядатися. Таким чином, Стратегія повинна передбачати моніторинг та оцінку діяльності з управління ризиками для забезпечення постійного вдосконалення.

Розглядаючи оцінку КЗаг та узгодження політик з ландшафтом КЗаг, що постійно розширюється необхідно передбачати визначення та оцінку еволюції середовища КЗаг, а також здійснити аналіз потенційного впливу та наслідків для критично важливих об’єктів інфраструктури та основних послуг. При цьому, особлива увага має бути приділена визначенню внутрішньої КІ та послуг країни – як фізичних, так і кібернетичних систем та активів, які є ключовими для сталого функціонування суспільства та економіки.

У разі порушення сталості роботи або знищення таких об’єктів, матиме серйозний вплив на фізичну та економічну безпеку, громадське здоров’я та загальну безпеку країни. Стратегія також повинна узгоджувати політики в контексті постійно змінюваного ландшафту КЗаг, що дозволить оперативно реагувати на нові виклики та мінімізувати потенційні ризики.

Оцінка ландшафту КЗаг повинна проводитись з метою визначення конкретних КРр для критично важливих інфраструктур і послуг, а також для осіб, які використовують ці системи та залежні від них. Така оцінка дозволить пріоритизувати ресурси для їх захисту, а також узгодити стратегії управління КРр з національним планом реагування на кризові ситуації. Крім того, вона допоможе визначити необхідні людські та фінансові ресурси, спроможності, а також стратегії для посилення загального рівня КБ в країні.

Стратегія має визначити узгоджений підхід до управління ризиками, якого мають дотримуватися всі державні установи та оператори КІ, визначені на національному рівні.

Підхід має ґрунтуватися на оцінці КЗаг та створенні національного реєстру ризиків, який надійно зберігатиметься та передаватиметься, щоб уможливити урядовий нагляд за ризиками та підходами до управління ними. Крім того, підхід має передбачати розробку методу визначення пріоритетів на основі розрахунку ймовірності реалізації ризиків та їхнього впливу. Крім того, він має визначати обов’язки ключових суб’єктів у кожному секторі щодо оцінки, прийняття та управління ризиками КБ на національному рівні.

Стратегія має визначити загальну методологію управління ризиками КБ. Це забезпечить ефективність та узгодженість у всіх установах/організаціях і полегшить обмін інформацією про загрози та ризики між взаємозалежними системами. Слід надавати перевагу методології, що базується на міжнародних стандартах, оскільки вона може зменшити витрати та забезпечити кращу взаємодію з приватним сектором.

Методологія повинна містити вказівки щодо розподілу ролей і відповідальності за різні аспекти управління ризиками, такі як оцінка загроз, оцінка активів, впровадження та підтримка заходів зі зниження ризиків, а також прийняття залишкового ризику. Методологія повинна включати програму сертифікації, яка допоможе оцінити і, зрештою, покращити дотримання вимог.

Важливо, що для закупівель і розвитку інфраструктури або послуг методологія управління ризиками повинна надавати рекомендації щодо мінімізації ризиків за допомогою безпечної архітектури та дизайну, а також регулярних оцінок/аудитів, визнаючи, що безпека найкраще досягається тоді, коли вона є невід'ємною частиною процесу проектування, розробки та впровадження продукту, процесу або послуги.

Стратегією повинно бути передбачено галузеві профілі ризиків КБ. Це кількісний аналіз типів загроз, з якими стикається сектор. Мета профілю ризику - забезпечити менш суб'єктивне розуміння ризику шляхом присвоєння числових значень змінним, що представляють різні типи загроз та небезпеку, яку вони становлять. Стратегія повинна рекомендувати розробку профілів ризиків для тих секторів, які вважаються найбільш важливими для суспільства та економіки.

Використання галузевих профілів ризиків створює основу для точних оцінок ризиків на рівні окремих організацій, забезпечуючи при цьому узгодженість між секторами на національному рівні. Це також сприяє зменшенню ресурсів, необхідних для оцінки ризиків на рівні організації. Профілі ризиків повинні регулярно оновлюватися, щоб зберігати свою актуальність і відповідність змінюваним умовам та новим загрозам.

Важливою складовою є розробка політик КБ для органів державної влади та операторів критично важливих інфраструктур. Така політика повинна бути розроблена на основі належного набору інструментів і охоплювати управлінські, операційні та технічні вимоги. Вона також повинна інформувати зацікавлені сторони про їхні ролі та обов'язки, а також визначати або санкціонувати конкретні підходи до забезпечення КБ в цих сферах.

Наприклад, така політика може охоплювати КБ під час закупівель, розробки чи модернізації, визначати порядок взаємодії, координувати розкриття вразливостей, встановлювати мінімальні стандарти безпеки та базові рівні безпеки. Вона також може передбачати програми сертифікації на відповідність і зобов'язувати організації повідомляти компетентні органи про інциденти КБ.

Як результат, скоординований підхід на національному рівні забезпечить більш ефективне та дієве управління КБ, оскільки гармонізує практики, сприяє кращій координації та взаємодії між усіма зацікавленими сторонами.

Пріоритетний напрям 3 – Готовність і стійкість. Зазначений напрямок охоплює передові практики для створення ефективних національних спроможностей у підготовці, запобіганні, виявленні, пом'якшенні наслідків та реагуванні на серйозні кіберінциденти (далі – КІ), а також підвищення кіберстійкості країни.

У рамках розвитку спроможностей реагування на КІ важливою складовою є створення військових та технічних організаційних структур для реагування на інциденти КБ. Це включає формування груп реагування на комп'ютерні надзвичайні ситуації (CERT), груп реагування на інциденти комп'ютерної безпеки (CSIRT) або груп реагування на комп'ютерні інциденти (CIRT).

Організаційні форми можуть варіюватися залежно від приналежності, але ці спеціалізовані команди повинні виконувати проактивні та оперативні функції, а також реалізовувати превентивні заходи. Це сприятиме швидкому реагуванню на кібератаки, відновленню після них та зменшенню економічних і операційних втрат.

Покращення навичок національних кібергруп швидкого реагування потрібно зосередити на обміні інформацією про кібератаки та кіберінциденти, проведенні спільних кібероперацій та розслідуваннях міжнародних кіберзлочинів, регулярних спільних кібернавчаннях та тренінгах, обміні досвідом та найкращими практиками із відповідними підрозділами держав – членів НАТО [4].

CERT/CSIRT/CIRT повинні забезпечити реагування на інциденти, координацію, управління вразливостями, ситуаційну обізнаність, обмін інформацією про загрози та розвідувальні дані. Необхідно забезпечити розгортання цих складових у приватному секторі, зокрема для забезпечення безпеки продукції (PSIRT), що включає пропозиції, рішення, компоненти та/або послуги, які організація виробляє та/або продає. Це дозволить значно покращити здатність протидіяти вразливостям ІКТ-продуктів.

Крім того, Стратегія повинна визначити механізми співпраці між національними, галузевими групами реагування на інциденти та міжнародними партнерами.

Стратегія має передбачати розробку національного плану дій на випадок надзвичайних ситуацій і криз у сфері КБ. Цей план повинен бути інтегрований у загальний національний план дій на випадок надзвичайних ситуацій або бути з ним узгоджений. Окрім того, варто розглянути можливість розробки спеціалізованого плану для ОКІІ.

Національний план повинен базуватися на результатах національної оцінки КРр і враховувати міжгалузеві залежності, які можуть вплинути на безперервність роботи КІ. Він також має охоплювати механізми аварійного

відновлення та визначати національні механізми реагування на інциденти. Крім того, план повинен описувати, як класифікуються і ескалуються інциденти КБ залежно від їхнього впливу на критичні активи та послуги.

Стратегія повинна сприяти створенню механізмів обміну інформацією для забезпечення взаємодії між державним і приватним секторами, щоб ця інформація про загрози та розвідувальні дані могла бути використана на практиці. Однак, офіційні та неофіційні програми обміну інформацією можуть значно полегшити ефективну координацію та належну комунікацію під час реагування на інциденти і відновлювальних заходів. Враховуючи це, вони сприятимуть швидкому обміну інформацією про загрози та розвідувальні дані між постраждалими сторонами та іншими зацікавленими учасниками.

Таким чином, обмін інформацією допоможе покращити розуміння того, як і які сектори стали об'єктами атак. Це також дозволить поширювати інформацію про методи захисту і зменшення шкоди, завданої постраждалим об'єктам. В результаті, така взаємодія дозволить знизити вразливість та ризики, пов'язані з КЗаг.

Стратегія повинна визначити одну або кілька інституційних структур, відповідальних за передачу точної та дієвої інформації серед національної спільноти з питань КБ, враховуючи як державний, так і приватний сектори.

Обмін інформацією має бути двостороннім процесом. Якщо уряд налагодить ефективну взаємодію, це не лише продемонструє його партнерство з приватним сектором, але й сприятиме покращенню готовності до реагування на загрози.

Реалізація практичної складової повинна зосереджуватися на формуванні та набутті сучасних компетентностей з КБ, що включає розвиток навичок та здатності застосовувати нові знання на практиці. Для цього важливо активно брати участь у національних та міжнародних навчаннях з КБ та реагування на інциденти. Навчання можуть бути різних форматів і орієнтуватися як на технічну, так і на нетехнічну аудиторію.

Застосування цих практик дозволяє розвивати інституційну спроможність до ефективного реагування на інциденти, тестувати процедури управління ризиками та оцінювати здатність CERT/CSIRT/CIRT діяти в умовах обмеженого часу. Вони також допомагають виявити міжгалузеві залежності та покращити механізми взаємодії між секторами.

Загалом, міжнародні навчання з КБ сприяють розвитку спроможностей країн реагувати на кібератаки, сприяють кращому розумінню транскордонних залежностей та зміцнюють довіру й стійкість міжнародної спільноти.

Також важливо передбачити створення механізмів для оцінки впливу КІ, зокрема на основі їхнього впливу на критичні активи, послуги, інфраструктуру та людей. Така оцінка дозволить отримати більш глибоке розуміння контексту інциденту, враховуючи не лише його фактичний вплив, а й потенційні наслідки для різних секторів та груп населення, а також каскадні ефекти.

Процес оцінки повинен здійснюватися за участю широкого кола зацікавлених сторін у відкритий, інклюзивний і прозорий спосіб. Результати таких оцінок повинні бути інтегровані в національні плани відновлення після катастроф та надзвичайних ситуацій, а також враховуватися при реагуванні на КІ в цілому.

Пріоритетний напрям 4 – Критична інфраструктура та основні послуги. Зазначений напрямок зосереджується на дослідженні передового досвіду у сфері ідентифікації та захисту КІ та критичної інформаційної інфраструктури (Далі - КІІ), а також на посиленні їхньої стійкості для забезпечення безперервної роботи важливих галузей.

Як правило, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізацію відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади [5].

Однак визначення та класифікація цих галузей можуть змінюватися залежно від геополітичних, економічних та культурних особливостей.

Стратегія повинна передбачати розробку комплексного підходу до управління ризиками для захисту КІ та КІІ від КЗаг, базуючись на принципах стійкості. Оцінка ризиків має визначити національні КІ та КІІ, а також критичні послуги, порушення яких можуть мати значний вплив на здоров'я, безпеку або економіку країни.

Стратегія повинна включати перелік КІ та КІІ, який регулярно оновлюється. При цьому можна застосовувати галузеві критерії, враховуючи взаємозалежність інфраструктури та її здатність підтримувати мінімальний рівень послуг.

Слід використовувати підхід, заснований на оцінці ризиків, для визначення та пріоритетного впровадження політик і практик, спрямованих на захист і посилення безпеки КІ та КІІ. Ці програми мають відповідати базовим стандартам безпеки, зберігаючи при цьому гнучкість для адаптації до специфічних ризиків і пріоритетів. Для інтеграції вітчизняної промисловості у глобальні ІКТ-ланцюги постачання та уникнення проблем інтероперабельності КІ/КІІ, доцільно застосовувати міжнародні стандарти управління ризиками.

Стратегія повинна визначати чітку модель управління з розподілом обов'язків для захисту КІ та КІІ. Для ефективного виконання програми необхідно визначити ролі та обов'язки зацікавлених сторін, а також створити координаційний механізм для оперативного вирішення питань. Оскільки окремі КІ та КІІ не знаходяться під контролем держави, важливо призначити координатора з питань КБ. Модель управління повинна включати визначення відповідальних органів, обов'язків операторів та канали співпраці між державним і приватним секторами для відновлення критичних послуг і

інфраструктури. Крім того, вона має передбачати механізми координації між державними установами та галузевими регуляторами для уникнення дублювання завдань та оптимізації зусиль з дотримання вимог безпеки.

Визначаючи мінімальні базові рівні КБ необхідно передбачати або адаптацію існуючих, або розробку нових законодавчих та регуляторних рамок для встановлення мінімальних стандартів КБ для операторів КІ та КІІ. Ці стандарти повинні охоплювати ключові аспекти управління ризиками, включаючи виявлення КРр, створення структур управління ними, захист даних та систем за допомогою контролю доступу, моніторинг цифрового середовища для виявлення аномалій, а також реагування на інциденти та відновлення після них.

Сучасна методологія оцінки ІТ ризиків доволі змістовно описані Національним Інститутом стандартів та технологій США (National Institute of Standards and Technology - NIST). При цьому, пріоритетними сферами, до яких NIST вносить поправки і на яких планує концентрувати свої зусилля є криптографія, освіта, новітні технології, управління ризиками, ідентифікація та управління доступом, вимірювання, конфіденційність, надійність мережі та стале функціонування платформ [6].

При формуванні базових стандартів необхідно орієнтуватися на міжнародно визнані норми і передові практики, що забезпечують високий рівень безпеки та ефективності. Загальні стандарти, які підходять для всіх секторів, мають стати відправною точкою для забезпечення сумісності та узгодженості практик у різних галузях, полегшуючи дотримання вимог міжсекторальними організаціями.

Стратегія також повинна акцентувати увагу на орієнтації базових показників на результат, що дозволяє забезпечити гнучкість при розвитку технологій і зміні КРр. Замість конкретних методів (наприклад, “використовувати двофакторну автентифікацію”), цілі мають бути сформульовані так, щоб організації могли вдосконалювати рівень безпеки з часом (наприклад, “контролювати доступ до критичних ресурсів”). Додатково, галузеві інструкції повинні впроваджувати відповідні практики на корпоративному рівні.

Окрім цього, базові стандарти мають включати вимоги до закупівель, щоб постачальники ІКТ застосовували відповідні заходи безпеки, що підлягають аудиту. Стратегія повинна сприяти формуванню національного середовища, яке гарантуватиме стійкість КІ та КІІ, а також підготує зацікавлені сторони до ефективного реагування, пом’якшення наслідків і відновлення після КІ. Підхід до управління ризиками має включати процеси для кризового управління, безперервності бізнесу та відновлення.

Особливо необхідно враховувати широкий спектр політик, щоб забезпечити реальну зацікавленість усіх організацій та осіб у виконанні своїх обов’язків з КБ відповідно до ризиків, з якими вони стикаються, а також з урахуванням принципу комплексного підходу та індивідуальних пріоритетів.

Виявлення розривів між можливостями та обов'язками ринків і реальними вимогами середовища ризиків є важливим кроком для визначення, коли і як слід застосовувати доступні стимули та стримуючі фактори для підвищення рівня безпеки. Для стимулювання впровадження стандартів та практик КБ серед ОКІ та ОКІІ. Стратегія повинна передбачати, що уряд розгляне різноманітні політичні та ринкові інструменти, які можуть бути використані для досягнення цієї мети [7].

Для ефективного захисту КІ та КІІ Стратегія повинна підтримувати ініціативи, які сприяють розвитку державно-приватного партнерства. Такі партнерства є основою для ефективного управління КРр в короткостроковій та довгостроковій перспективі. Вони допомагають зміцнити довіру між урядом та бізнесом, а також між іншими зацікавленими сторонами.

Ключовим фактором для створення стійких взаємовідносин є чітке розуміння цілей співпраці та визначення взаємних вигод у сфері КБ. Це може включати розробку базових принципів КБ на міжсекторальному та секторальному рівнях, створення ефективних координаційних структур, налагодження протоколів обміну інформацією, підвищення довіри серед учасників, а також активний обмін ідеями та найкращими практиками для підвищення рівня безпеки. Крім того, важливим є посилення міжнародної координації для забезпечення спільного реагування на КЗаг.

Пріоритетний напрям 5 - Розбудова спроможностей і потенціалу та підвищення обізнаності. Цей пріоритетний напрямок зосереджений на розвитку спроможностей у сфері КБ, включаючи людські та інституційні ресурси, та підвищення обізнаності серед усіх зацікавлених сторін. Це важливо для розвитку цифрової економіки. До ключових практик належать координація навчальних програм, підвищення кваліфікації, прийняття міжнародних сертифікацій та підтримка інновацій у науково-дослідних та дослідно-конструкторських роботах.

Стратегія повинна визначити чіткі ролі та обов'язки органів, відповідальних за координацію заходів з розбудови та нарощування спроможностей, а також підвищення обізнаності на національному рівні. Це дозволить ефективно використовувати ресурси, уникнути дублювання та встановити підзвітність. Відповідні органи повинні також моніторити реалізацію і оцінювати результати, а за потреби надавати рекомендації щодо коригувань.

Розбудова спроможностей і підвищення обізнаності з КБ повинні ґрунтуватися на науковому підході та стратегічному плануванні. Оцінка національного ландшафту КБ дозволить виявити прогалини в навичках і знаннях, що сприятиме прийняттю обґрунтованих рішень. Зібрана інформація повинна бути використана для розробки адаптованих підходів, що відповідатимуть конкретним умовам та потребам. Відповідальні органи також можуть розробити план бюджетних дій, визначити часові рамки та показники для моніторингу прогресу, що дозволить ефективно оцінювати виконання завдань.

Стратегія повинна підтримувати розробку та розширення навчальних програм для розвитку навичок і обізнаності з КБ у формальній освіті. Навчальні програми мають бути міждисциплінарними, охоплюючи як технічні, так і нетехнічні аспекти КБ, такі як цифрова грамотність, право, етика, управління ризиками та міжнародні відносини.

Беззаперечним є той факт, що в умовах подальшого розвитку високотехнологічного суспільства потреба у фахівцях із КБ буде постійно зростати, а за умов тотальної оборони держави роль об'єднаної підготовки персоналу складових сил оборони та цивільного сектору в сфері КБ взагалі не піддається ніякому сумніву. [8].

Оскільки освіта з КБ є міждисциплінарною, варто заохочувати співпрацю між факультетами університетів та іншими навчальними закладами для оптимізації ресурсів. Вони можуть стати осередками навчання як для цивільних, так і для військових, поєднуючи теорію та практичні навички.

Навчальні програми також повинні стимулювати інтерес до кар'єрного зростання в сфері КБ. Для підтримки цього процесу уряд може започаткувати стипендії для приватних освітніх програм та грантів для стажувань у цій сфері.

Стратегія має передбачити розробку схем навчання та розвиток навичок у сфері КБ для експертів і не експертів як у державному, так і в приватному секторах. Ці зусилля можуть включати в себе забезпечення підготовки керівних кадрів та короткострокового навчання, офіційне стажування та навчання, а також (національну та міжнародну) сертифікацію фахівців з безпеки, виходячи з потреб, визначених промисловістю та урядом. Стратегія також повинна заохочувати спеціальну підготовку для національних суб'єктів, що беруть участь у внутрішній і зовнішній політиці, в тому числі регуляторів і законодавців. Навчання має доповнюватися ініціативами, спрямованими на управління КРр, а також практичними вправами в державних установах та між ними й іншими зацікавленими суб'єктами, такими як навчання та симуляції.

Стратегія також має сприяти ініціативам, спрямованим на розвиток кар'єри у сфері КБ та ефективного резерву майбутніх працівників, зокрема для державного сектору, а також стимулювати збільшення кваліфікованих фахівців з КБ та сприяти утриманню талановитих кадрів. В умовах сьогодення постає доволі суттєва проблематика щодо формування кіберрезервістів Збройних Сил України що мають відповідний рівень професійних знань та навичок для планування і виконання окремих завдань КО [9].

Вони повинні створюватися у партнерстві з науковими колами, приватним сектором і суспільством. Для подолання існуючого гендерного розриву серед експертів з КБ слід розглянути можливість застосування гендерно збалансованого підходу, який би мотивував, заохочував та сприяв більшій участі жінок у цих заходах, спрямованих на розвиток навичок та навчання, забезпечуючи інклюзивність у майбутньому.

Органи, відповідальні за освітньо-комунікаційні кампанії, інформаційні ініціативи та заходи спрямовані на поширення проблематики з КБ на

національному рівні, повинні співпрацювати з усіма зацікавленими сторонами для розробки і реалізації програм підвищення обізнаності з КБ. Ці програми повинні фокусуватися на інформуванні громадськості про ризики та загрози КБ, а також про найкращі практики для їх подолання.

Програма підвищення обізнаності може включати інформаційні кампанії для широкої аудиторії, дітей, осіб з обмеженими можливостями, освітні програми, а також ініціативи для керівників державного та приватного секторів. Важливо, щоб програми мали чіткі ключові показники ефективності та метрики для оцінки їхнього впливу та результативності.

У рамках сприяння інноваціям та дослідженням у сфері КБ необхідно створити умови, що стимулюють фундаментальні та прикладні дослідження у за напрямком КБ в різних секторах з залученням зацікавлених сторін. Ключовими напрямками таких ініціатив є підтримка національних дослідницьких зусиль, які узгоджуються з цілями Стратегії, розробка науково-дослідних програм у державних наукових установах, а також ефективне впровадження та поширення нових технологій, методів, процесів та інструментів у сфері КБ.

Окрім цього, Стратегія повинна сприяти розвитку ринку послуг у сфері КБ, створюючи сприятливі умови для його зростання. Важливим аспектом є також налагодження міжнародного співробітництва у наукових галузях, що стосуються КБ, таких як інформатика, криптографія, прикладна математика, а також у соціальних науках, бізнесі, політиці, кримінології та психології.

У рамках Стратегії мають бути передбачені механізми стимулювання інновацій через гранти, податкові пільги, конкурси та інші ініціативи, що заохочують розробку нових рішень, продуктів і послуг у сфері КБ.

Стратегія повинна визначити групи, які потребують особливої уваги в розбудові спроможностей та підвищенні обізнаності з КБ. Це включає малі та середні підприємства, громадські організації та громади з обмеженим доступом до ресурсів або низьким рівнем доходів.

Пріоритетний напрям 6 – Законодавство та регулювання. Цей пріоритетний напрямок фокусується на розробці НПБ для захисту суспільства від кіберзлочинності (далі – КЗл) та створення безпечного кіберсередовища, дотримуючись принципів інклюзивності, прав людини та довіри. Така система має включати: законодавство, яке визначає незаконну кіберактивність, а також інструменти для розслідування і переслідування злочинів на національному та міжнародному рівнях; механізми забезпечення дотримання законів; розвиток потенціалу органів, що здійснюють правозастосування; інституціоналізацію критичних суб'єктів та міжнародне співробітництво в боротьбі з КЗл.

За цих умов вагомим завданням для України є створення умов для захисту суверенітету та забезпечення обороноздатності держави у КП шляхом підтримки спроможностей сил оборони здійснювати активний кіберзахист власної інформаційної інфраструктури і підготовку держави до відбиття воєнної агресії в КП як у мирний час так і воєнний стан (особливий період) [10].

Стратегія має визначати ролі і обов'язки суб'єктів, що відповідають за застосування законів, забезпечуючи при цьому відповідність чинним правовим принципам. Вона повинна відображати поточну НПБ та вказувати на необхідність оновлення або прийняття нових законів і нормативних актів.

Доволі важливим є сприяння розвитку національної правової бази для КБ та захисту даних, охоплюючи запобігання, моніторинг і реагування на КІ.

Законодавча та НПБ України потребує суттєвих змін. Необхідно провести реальну імплементацію міжнародних стандартів ISO/IEC 27k, NIS Directive, NIST CS Framework, зокрема щодо запровадження базового рівня відповідності вимогам з КБ, оцінювання ризиків, реагування на кіберінциденти і врегулювання інцидентів, відновлення сталого функціонування КІ держави у відповідності до кращих міжнародних практик [11].

Документ повинен включати правила інформаційної безпеки, визначення КІ, створення органів КБ, сертифікацію та національні правила безпеки КП. Крім того, Стратегія має передбачати регуляторні підходи щодо обміну інформацією, розвідданими, кримінальної звітності та державно-приватного співробітництва.

Стратегія повинна сприяти розробці національної правової бази, яка визначає сферу КЗл, надає процесуальні повноваження для ефективного розслідування та судового переслідування за допомогою електронних доказів. Це може включати нові закони або зміни до існуючих, зокрема в кримінальному кодексі та регулюванні банківської і телекомунікаційної сфер. Законодавство має визначати кримінальні правопорушення, засоби збору доказів та механізми міжнародного співробітництва.

Стратегія також має включати інструкції для оперативних аспектів розслідувань, як-от створення спеціалізованих підрозділів і стандартних процедур. Також потрібно запровадити відстеження законодавства для виявлення прогалин та оновлення застарілих норм.

Суттєвим є сприяння розвитку НПБ, яка захищає права людини в контексті КБ та КЗл. Важливо розрізняти технічні аспекти безпеки і кримінальне правосуддя, враховуючи технології, що можуть впливати на ці права. Стратегія повинна забезпечити дотримання прав на справедливу правову процедуру, захист приватного життя, охорону персональних даних і свободу вираження думок, а також гарантувати захист осіб, постраждалих від КІ.

Стратегія повинна забезпечити створення механізмів дотримання законодавства для запобігання і протидії КЗаг, зокрема через реагування на КІ, кримінальні розслідування та обробку електронних доказів. Важливо вдосконалити механізми управління та взаємодії складовими (х) сектору безпеки і оборони під час планування підготовки держави до КО, проведення заходів з нейтралізації та активної протидії кіберзагрозам в національному сегменті КП держави [12].

Також необхідно посилити фахові компетенції правоохоронних органів у боротьбі з КЗл шляхом проведення регулярного навчання для суддів,

прокурорів, поліцейських та інших спеціалістів, що сприятиме підвищенню їх кваліфікації в цій сфері. Необхідно запровадити та за-забезпечити об'єднаний підхід навчання для цивільного та військового секторів, що дозволить максимально ефективно використовувати єдині системи електронного зв'язку на основі захищеного інформаційного середовища [13].

Не менш важливим елементом є визначення повноважень органів, відповідальних за дотримання законодавства про КЗл, запобігання КІ, захист КІ та забезпечення відповідності національних законів міжнародним зобов'язанням. При цьому необхідно враховувати і той факт, що імплементація і взаємосумісність адаптивних комунікаційних систем та мереж суб'єктів КБ відбувається з урахуванням національних особливостей щодо захисту суверенітету, територіальної цілісності і недоторканності України [14].

Розглядаючи міжнародне співробітництво у боротьбі з КЗаг та КЗл необхідно зосередитись на ратифікації міжнародних угод, приведення національного законодавства у відповідність до міжнародних зобов'язань та сприянню транскордонним розслідуванням, обміну інформацією і екстрадиції.

Також важливо розвивати неформальні механізми співпраці між державними та приватними суб'єктами КБ. Співпраця правоохоронних органів, зокрема через Інтерпол, Європол та інші регіональні організації, є ключовою для ефективної боротьби з КЗл.

Пріоритетний напрям 7 – Міжнародне співробітництво. Цей пріоритетний напрямок підкреслює важливість врахування зовнішніх зобов'язань країни в сфері КБ на регіональному та міжнародному рівнях. Оскільки цифровізація охоплює всі сфери міжнародних відносин - від прав людини до економічного розвитку, торгівлі, безпеки ланцюгів постачання та міжнародної стабільності, КБ стала невід'ємною частиною зовнішньої політики.

Стратегія має визнавати міжнародний вимір КБ і підкреслювати важливість участі країни в міжнародних дискусіях, співпраці з державними, приватними зацікавленими сторонами, громадянським суспільством та неурядовими організаціями. Міжнародна взаємодія є ключем до конструктивного діалогу, розвитку довіри, спільного пошуку рішень і створення глобального розуміння значення КБ.

У рамках комплексного підходу, регіональне та міжнародне співробітництво має розвиватися в гармонії з політичним, соціальним, культурним і економічним контекстом. Пріоритети в сфері КБ повинні відповідати цілям зовнішньої політики та бути з ними узгодженими.

Стратегія повинна визнати КБ невід'ємною частиною зовнішньої політики країни та сприяти міжнародному співробітництву в цій сфері, охоплюючи такі напрями, як міжнародна кіберстабільність та торговельні переговори. Вона має чітко визначити пріоритети уряду, довгострокові цілі та зацікавлені сторони (державні, приватні, регіональні, глобальні), які братимуть участь у співпраці.

Зокрема, ці пріоритети можуть включати підтримку міжнародних норм КБ, заходи зміцнення довіри, зобов'язання з розвитку кібербезпекового потенціалу та участь у розробці міжнародних стандартів. Стратегія також має передбачати інтеграцію внутрішньої та зовнішньої політики країни, гармонізуючи національну правову базу з міжнародними зобов'язаннями та узгоджуючи національні підходи до КБ з глобальними зусиллями.

Для досягнення цієї мети, необхідно забезпечити координацію між різними державними органами, такими як уряд, Міністерство закордонних справ, Міністерство цифрової трансформації, Міністерство юстиції та інші, щоб політичні позиції на міжнародних переговорах були узгоджені та ефективно скоординовані.

Стратегія повинна визначити ключові міжнародні форуми та механізми для співпраці у сфері КБ, включаючи глобальні та регіональні організації, міжурядові платформи та альянси державного та приватного секторів. Вона має встановити зобов'язання щодо імплементації міжнародного права, включаючи Статут ООН та угоди, як Будапештська конвенція, а також враховувати цифрові аспекти міжнародних торговельних угод.

Стратегія повинна сприяти підтримці добровільних норм поведінки держав у КП та зміцненню довіри через участь у міжнародних форумах, таких як ООН та ОБСЄ. Важливо визначити пріоритети міжнародної взаємодії, забезпечити необхідні ресурси для їх реалізації та ефективно імплементувати узгоджені норми, зокрема розроблені ООН.

Стратегія повинна визначити механізми міжнародного співробітництва, яких країна готова долучитися, включаючи формальні та неформальні ініціативи в державному та приватному секторах. Країна може взяти участь у таких міжнародних платформах, як Інтерпол, Європол, Всесвітня організація інтелектуальної власності, а також в ініціативах з обміну інформацією про загрози, наприклад, FIRST, ISAC.

Це сприятиме кращій координації між органами влади у реагуванні на КЗаг та вразливості, а також забезпечить ефективний обмін інформацією. Транскордонна співпраця з приватним сектором, такими як антивірусні компанії, спільноти з розвідки загроз та глобальні платформи, є важливим елементом для зміцнення КБ.

У рамках розвитку додаткових компетенцій та навичок у кібернетичній сфері для ефективної участі в міжнародних заходах Стратегія повинна включати розбудову спроможностей у таких областях, як міжнародна кібернетична стабільність, захист даних, комерція, контроль над озброєннями та нові технології. Окрім традиційних дипломатичних процесів, необхідно розвивати кібер-дипломатію, торговельні переговори та міжнародне право.

Стратегія має передбачати створення спеціалізованих організаційних структур, офісів або персоналу для дипломатичної взаємодії з кіберпитань. Важливо створити кваліфіковані підрозділи для контролю КРр, здатних регулярно проводити оцінки та здійснювати моніторинг КБ в фінансових установах [15].

Важливо також сприяти розвитку співпраці між CERT/CSIRT, правоохоронними органами та судами для покращення міжнародної співпраці в КБ.

Враховуючи існуючі міжнародні програми, такі як GLACY+ та GFCE, Стратегія повинна заохочувати використання передового досвіду та сприяти гармонізації з міжнародними ініціативами. Взаємне навчання та обмін знаннями з міжнародними партнерами мають стати ключовими елементами для розбудови спроможностей та довіри у сфері КБ.

Висновки з даного дослідження і перспективи подальших розвідок.

У контексті стрімкої цифрової трансформації кібербезпека стає не лише складовою частиною національної безпеки, а й критичним фактором збереження державного суверенітету, сталого економічного розвитку та соціальної стабільності. Сучасні кіберзагрози набули складного, багатовимірного характеру, що вимагає системного й міжсекторального підходу до їх виявлення, нейтралізації та запобігання. В умовах гібридних конфліктів та зростаючої інтенсивності кібероперацій, розробка та реалізація Національної стратегії кібербезпеки України постає як стратегічний пріоритет.

У межах цього дослідження обґрунтовано необхідність інтеграції Стратегії до трирівневої моделі кібероборони, яка передбачає координацію дій державних структур, приватного сектору та громадянського суспільства. Такий підхід сприяє створенню цілісної кіберекосистеми, здатної оперативно реагувати на динамічні загрози, підтримувати безперервність функціонування критичних інформаційних інфраструктур та підвищувати рівень національної кіберстійкості.

Отже, до ключових пріоритетів Стратегії віднесено: захист критичних об’єктів інфраструктури; розвиток ефективної системи управління кіберризиками; удосконалення нормативно-правового забезпечення КБ; підвищення цифрової обізнаності населення; розбудову міжнародного співробітництва у сфері КБ.

Також особливу увагу приділено правовому аспекту, а саме запропоновано законодавче закріплення діяльності Кіберсил Збройних Сил України, що відповідає стандартам НАТО та забезпечує інституційну спроможність держави до ведення оборонних кібероперацій. Водночас окреслено потребу в оновленні нормативно-правової бази у сфері запобігання кіберзлочинності, захисту персональних даних та регулювання діяльності в цифровому середовищі.

Разом з цим, доволі значущим є і міжнародний компонент КБ, адже ефективна протидія КЗаг можлива лише за умов широкого міжнародного партнерства. Саме тому Україна повинна посилювати співпрацю з такими організаціями, як ООН, НАТО, ЄС, ОБСЄ, а також долучатися до глобальних ініціатив і стандартів у сфері КБ. При цьому інтеграція до міжнародних кіберкоаліцій забезпечить доступ до передових технологій, методик реагування та механізмів кібердипломатії.

Не менш важливою складовою є розвиток людського капіталу у сфері КБ. Дослідження підтвердило нагальну потребу в системному підході до професійної підготовки фахівців, формуванні національного кіберрезерву, створенні

спеціалізованих центрів компетенцій, стимулюванні науково-дослідницької діяльності та впровадженні навчальних програм на всіх рівнях освіти.

Таким чином, реалізація запропонованої комплексної Стратегії КБ сприятиме суттєвому зниженню рівня кіберризиків, зміцненню кіберстійкості України, підвищенню захищеності критичних інфраструктур та посиленню національної безпеки в цифрову епоху.

У подальших наукових розвідках доцільно зосередитися на: розробці моделей оцінювання ефективності державної політики у сфері КБ; визначенні показників кіберстійкості та індикаторів ризику; дослідженні впливу новітніх технологій (AI, блокчейн, квантові обчислення) на системи кіберзахисту; поглибленому аналізі механізмів державно-приватного партнерства у сфері КБ; адаптації міжнародних стандартів до українського правового поля з урахуванням воєнного стану.

При цьому розширення міждисциплінарних досліджень у сфері КБ стане важливою запорукою для побудови ефективної та адаптивної національної системи кібероборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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

2. Пояснювальна записка до проєкту Закону України “Про Кіберсили Збройних Сил України”, 27 грудня 2024. URL: https://cybersec.net.ua/normatyvni-dokumenty/774-poiasniuvalna-zapyska-do-proiektu-zakonu-ukrainy-pro-kibersyly-zbroinykh-syl-ukrainy.html

3. Onyshchenko S., Zhyvylo Y., Cherviak A., Bilko S. 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. 5 (13 (125)). С. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175

4. Живило Є., Черноног О. Міжнародні кібернавчання LOCKED SHIELDS – 2022. Проблемні питання в підготовці складових сил оборони та безпеки України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. 43 (1). С. 19–24. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-19-24

5. Zhyvylo Y., Kuz V. Risk Management of Critical Information Infrastructure: Threas-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security. National Technical University of Ukraine.* 2023. Vol. 5 No. 2. P. 68–80. URL: https://www.researchgate.net/publication/380898189_The_risk_management_of_critical_information_infrastructure_threats-vulnerabilities-consequences

6. Zhyvylo Y. Stage Of Risk Assessment Of Critical Infrastructure Cyber Security Breach (ІУСТ-ОДЕСА-2024) : матеріали XII Міжнародної науково-практичної конференції (23-25 вересень 2024 р. Одеса). 2024. С. 52–55. URL: https://icst-conf.com/2024.pdf

7. Проєкт Стратегія кібербезпеки України (2021 - 2025 роки) безпечний кіберпростір - запорука успішного розвитку країни. URL: https://rnbo.gov.ua/files/2021/STRATEGIYA KYBERBEZPEKI/proekt strategii_kyberbezpeki_Ukr.pdf

8. Живило Є. Пошук та засвоєння сучасних кадрових компетентностей сфери кібербезпеки в умовах цифрової трансформації держави. 2023. 2 (63). С. 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08

9. Живило Є. Військовий резерв кіберсил Збройних Сил України – вимога сучасності. *Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку : III Міжнародна науково-технічна конференція.* 2023. С. 147–148. URL: https://www.researchgate.net/publication/380908671_Vijskovij_rezerv_kibersil_Zbrojnih_Sil_Ukraini_-_vimoga_sucasnosti

10. Zhyvylo Y., Dokil V. Regulatory and Legal Ways to Resolve Existing Conflicts in the Field of Cyber Security in the Context of the Creation of Cyber Forces of the Armed Forces of Ukraine. *Theory and Practice of Public Administration*. 2024. 1(78). С. 183–196. DOI: https://doi.org/10.26565/1727-6667-2024-1-11

11. Живило Є. О., Кузь В. С. Об'єктивність дефініцій сфери кібербезпеки відповідно до міжнародних стандартів. *Всеукраїнська науково-практична конференція Theoretical and applied cybersecurity (TACS-2023), присвячена 100-річному ювілею академіка В.М. Глушкова. Київ, Полтава. Київ : КПІ ім. Ігоря Сікорського*. 2023. С. 212–219. URL: https://www.researchgate.net/publication/380898430_OB'EKTIVNIST_DEFINICIJ_SFERI_KIBERBEZPEKI_VIDPOVIDNO_DO_MIZNARODNIH_STANDARTIV

12. Живило Є. О., Ромашко І. В. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків. *Системи управління, навігації та зв'язку*. 2024. Issue 1 (75). P. 66–76. URL: https://www.researchgate.net/publication/378452835_PROTOKOL_SPILNIH_DIJ_SUB'EKTIV_ZABEZPECENNA_KIBERBEZPEKI_PID_CAS_REAGUVANNA_NA_KIBERINCIDENTI_A_TAKOZ_PRI_USUNENNI_IH_NASLIDKIV

13. Zhyvylo Ye. 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). С. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16

14. Живило Є. О. Сутність високотехнологічної війни в організаційно-інституціональному забезпеченні теорії державного управління. *Державне будівництво*. 2023. № 2 (34). С. 8–20. DOI: https://doi.org/10.26565/1992-2337-2023-2-01

15. Живило Є. О. Макрофінансова стабільність держави в умовах кіберзагроз. *Актуальні проблеми державного управління*. 2024. № 2 (65). С. 347–369. DOI: https://doi.org/10.26565/1684-8489-2024-2-18

Стаття надійшла до редакції 06.04.2025 р.
Стаття рекомендована до друку 07.05.2025 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

PRIORITY AREAS OF THE NATIONAL CYBERSECURITY STRATEGY IN THE CONTEXT OF INTEGRATION INTO THE THREE-TIER CYBER DEFENSE MODEL

Annotation. In the modern digital environment, stakeholders gain significant economic and social advantages, yet simultaneously face increasingly complex cybersecurity risks. The core issue lies in the fact that the rapid development of information and communication technologies outpaces the ability of states to regulate and effectively protect digital space from emerging threats. The lack of a comprehensive

understanding of the digital environment, tailored to specific national contexts and priorities, creates substantial barriers to ensuring the secure functioning of critical information infrastructures and digital services.

Cybersecurity is not merely a technical issue, but a multidimensional societal challenge encompassing aspects of national and international security, law enforcement, foreign policy, the digital economy, and sustainable development. Leading global powers actively invest in the development of both defensive and offensive cyber capabilities, recognizing the strategic importance of maintaining control over digital space. This creates a pressing need for other countries to develop their own adaptive and proactive approaches to cybersecurity.

An analysis of publicly available national cybersecurity strategies reveals considerable variation in the definition of strategic priorities-ranging from the protection of critical infrastructure and countering intellectual property theft to fostering trust in digital platforms and improving public cyber awareness. Successful case studies demonstrate the effectiveness of a comprehensive approach that integrates these areas in alignment with national circumstances.

In this context, the development and implementation of a National Cybersecurity Strategy becomes particularly crucial. It enables the systematic alignment of cybersecurity objectives with the broader goals of the country's digital transformation, foresees the mechanisms for policy implementation, identifies the necessary resources, and ensures their effective utilization. Such a strategic approach is a key factor in enhancing the resilience of national cyberspace to both current and future challenges.

Keywords: strategy, critical infrastructure, critical information infrastructure, information and communication technologies, information security, cybersecurity, cyber influence, cyber risks.

REFERENCES

1. 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

2. Pro Kibersyly Zbroinykh Syl Ukrainy: Poiasniuvalna zapyska do proiektu Zakonu Ukrainy, 27 hrudnia 2024. (2024). URL: https://cybersec.net.ua/normatyvni-dokumenty/774-poiasniuvalna-zapyska-do-proiektu-zakonu-ukrainy-pro-kibersyly-zbroinykh-syl-ukrainy.html

3. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., Bilko, S. (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, 5 (13 (125)), 65–76.* DOI: https://doi.org/10.15587/1729-4061.2023.288175

4. Zhyvylo, Ye., Chernonoh, O. (2022). International cyber tests locked shields – 2022. Problem issues in training the composite defense and security forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defence, 2022, 43(1), 19–24*. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-19-24

5. Zhyvylo, Y., Kuz, V. Risk Management of Critical Information Infrastructure: Threas-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", vol. 5, no. 2, 68–80.* URL: https://www.researchgate.net/publication/380898189_The_risk_management_of_critical_information_infrastructure_threats-vulnerabilities-consequences

6. Zhyvylo, Ye. (2024). Stage of Risk Assessment of Critical Infrastructure Cyber Security Breach: MATERIALS OF THE XII INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE «Information Control Systems and Technologies» (ICST – ODESA – 2024), 23-25 September, 2024. 52–55. URL: https://icst-conf.com/2024.pdf

7. Project Ukraine's Cybersecurity Strategy (2021-2025) (2021). A secure cyberspace is the key to the country's successful development. URL: https://rnbo.gov.ua/files/2021/STRATEGIYA KYBERBEZPEKI/proekt strategii_kyberbezpeki_Ukr.pdf

8. Zhyvylo, Y.O. (2023). Exploring and acquiring modern human resource competen-cies 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 [in Ukrainian].

9. Zhyvylo, Ye. (2023). The military reserve of cyber forces of the Armed Forces of Ukraine - a requirement of modernity. *Systems and technologies of communication, informatization, and cybersecurity: current issues and development trends: III International Scientific and Technical Conference, 147–148.* URL: https://www.researchgate.net/publication/380908671_Vijskovij_rezerv_kibersil_Zbrojnih_Sil_Ukraini_-_vimoga_sucasnosti

10. Zhyvylo, Y., & Dokil, V. (2024). Regulatory and Legal Ways to Resolve Existing Conflicts in the Field of Cyber Security in the Context of the Creation of Cyber Forces of the Armed Forces of Ukraine. *Theory and Practice of Public Administration, 1(78), 183–196*. DOI: https://doi.org/10.26565/1727-6667-2024-1-11

11. Zhyvylo, Ye.O., Kuz, V.S. (2023). Objectivity of definitions in the field of cybersecurity in accordance with international standards. *All-Ukrainian Scientific and Practical Conference Theoretical and Applied Cybersecurity (TACS-2023), dedicated to the 100th anniversary of Academician V.M. Glushkov. Kyiv, Poltava. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 212–219.* URL: https://www.researchgate.net/publication/380898430_OB'EKTIVNIST_DEFINICIJ_SFERI_KIBERBEZPEKI_VIDPOVIDNO_DO_MIZNARODNIH_STANDARTIV

12. Zhyvylo, Ye.O., Romashko, I.V. (2024). Protocol for joint actions by cybersecurity entities when responding to cyber incidents and mitigating their consequences. *Management, Navigation, and Communication Systems, issue 1 (75), 66–76.* URL: https://www.researchgate.net/publication/378452835_PROTOKOL_SPILNIH_DIJ_SUB'EKTIV_ZABEZPECENNA_KIBERBEZPEKI_PID_CAS_REAGUVANNA_NA_KIBERINCIDENTI_A_TAKOZ_PRI_USUNENNI_IH_NASLIDKIV

13. Zhyvylo, Ye.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

14. Zhyvylo, Ye.O. Zhyvylo,Y.O. (2023). The essence of high-tech warfare in the organizational and institutional security theory of state administration. *State Formation, no.2(34), 8–20*. DOI: https://doi.org/10.26565/1992-2337-2023-2-01[in Ukrainian]

15. Zhyvylo, Ye.O. Zhyvylo, Ye. O.(2024). National Macrofinancial Stability in the Context of Cyber Threats. *Pressing Problems of Public Administration, 2 (65), 347–369.* DOI: https://doi.org/10.26565/1684-8489-2024-2-18 [in Ukrainian].

The article was received by the editors 06.04.2025.
The article is recommended for printing 07.05.2025.