УДК 355.45:004.056.5

# ІНТЕГРАЦІЯ КІБЕРБЕЗПЕКИ В СИСТЕМУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: НОВІ ВИКЛИКИ, МОЖЛИВОСТІ ТА РЕЗУЛЬТАТ

**Вікторія Мельничук**

INTEGRATION OF CYBERSECURITY INTO THE NATIONAL SECURITY SYSTEM OF UKRAINE: NEW CHALLENGES, OPPORTUNITIES AND RESULT

Victoria Melnuchyk

*Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна*

***Abstract.*** *The text reveals the role of the digital sphere as a key element of the modern national security system of Ukraine. The emphasis is on the growing threat of cyberattacks, espionage, IPSO and other forms of hybrid warfare, which require a coordinated state response. The main challenges to integrating cybersecurity into the national security strategy are identified, in particular, the imperfection of the legislative framework, institutional fragmentation, personnel shortage, technological dependence and limited funding. At the same time, significant opportunities are emphasized: the development of public-private partnerships, international cooperation, a national cyber defense industry and the formation of a culture of digital security.*

У сучасному світі цифрова сфера перетворилася на один із фундаментальний аспектів національної безпеки, стоячи поруч із традиційними сферами – військовими, політичними, економічними, екологічними та інформаційними. Цифровізація всіх сфер життєдіяльності суспільства та державного управління відкриває широкі перспективи, а й загрожує повнявою нових ризиків і загроз. До них належать кібератаки на критичні об’єкти інфраструктури, несанкціоноване втручання в інформаційні системи органів влади, кібершпіонаж, ІПСО та прості інформаційні операції, які стали ключовими інструментами ведення сучасних гібридних війн які вимагають ефективної відповіді держави [1].

Інтеграція кіберскладової в систему національної безпеки зіштовхується з різними перешкодами. Найсуттєвішою є недосконаліть законодавчої бази. Що ускладнює встановлення правил функціонування цифрового простору, та обмежує кількість спеціалістів належної кваліфікації, здатних ефективно протидіяти сучасним кіберзагрозам. Проте ці труднощі стимулюють розробку передових технологічних рішень, сприяють взаємодії між державними структурами та активізують міжнародне співробітництво в цій галузі, зокрема з країнами партнерами ЄС та НАТО.

Важливою складовою є формування національної системи кібербезпеки, що об’єднує державні органи, приватний сектор, наукові установи та громадські організації. Координація цієї системи повинна здійснюватися через Раду національної безпеки та оборони України (РНБО) та її спеціалізовані підрозділи, які забезпечують швидку реакцію на кіберінциденти та зміцнення захисту об’єктів критичної інфраструктури [ 2 ].Такий підхід дозволить не тільки захищати державні інтереси на міжнародній арені, а й підтримувати довіру суспільства до цифрових технологій і сприяти сталому розвитку цифрової економіки.

Для України, яка перебуває під тиском з боку зовнішніх кіберзагроз, інтеграція кібербезпеки в загальну систему національної безпеки є стратегічно важливою. Розбудова ефективної кібербезпеки має включати не лише технічні засоби, але й політичні, військові, правові, екологічні, освітні, економічні та міжнародні аспекти. В той же час ці виклики відкриють нові можливості для зміцнення національного суверенітету, розвиток інновацій та

поглиблення міжнародного співробітництва, та можливо допоможе Україні стати провідною країною на міжнародній арені і допоможе вступити в ЄС та НАТО.

Однак цей процес супроводжується серйозними викликами та можливостями, такими як:

ВИКЛИКИ.

Недосконаліть правового підґрунття. Нормативна база у сфері кіберзахисту залишається недосконалою , що перешкоджає реалізації єдиної політики кібербезпеки. Спостерігається термінологічна неузгодженість, демонструються чіткі імплементацій ні механізми та невідповідність міжнародним стандартам, зокрема ЄС.

Інституційна неузгодженість та дублювання функцій. Множинність державних структур з нечітко розмежованими повноваженнями у сфері кібербезпеки до розпорошення ресурсів та зниження ефективного реагування. Відсутність єдиного координаційного органу ускладнює прийняття рішень та міжвідомчого робітництва, що негативно впливає на загальнодержавну систему кіберзахисту.

Кадровий дефіцит та освітні виклики. Критична нестача кваліфікованих фахівців з кібербезпеки суттєво обмежує сприятливість держави протидіяти цифровим загрозам. А освітня система не забезпечує достатньої підготовки кадрів відповідно до вимог, адже державний сектор програє приватним компаніям у конкурсі для талановитих спеціалістів через низький рівень заробітної плати.

Технологічна залежність та вразливість критичної інфраструктури. Більшість об’єктів критичної інфраструктури – від енергетичних мереж до медичних закладів – залишаються вразливими до кібератак через застарілі технічні рішення, видають резервні системи та недосконалі протоколи реагування на інциденти, що створюють загрози національного масштабу.

Технологічна залежність від зовнішніх постачальників. Перевага іноземних програмних та апаратних рішень у державному секторі підриває цифровий суверенітет Україниби та обмежує можливості контролю за безпечною критичною системою, створюючи певні канали для зовнішнього втручання.

Обмеженість фінансових ресурсів. Недостатні обсяги та неефективний розподіл державного бюджету на кіберзахист суттєво гальмує розвиток національної системи кібербезпеки. Відсутність стратегічного підходу до фінансування за рахунок нераціонального використання обмежених ресурсів та низької ефективності впроваджуваних заходів

МОЖЛИВОСТІ.

Розширення державно – приватного партнерства. Активніше залучення потужного приватного ІТ – сектора до національної системи кібербезпеки відкриває перспективи для суттєвого посилення технологічних та інтелектуальних ресурсів держави у протидії кіберзагрозам. Створення прозорих механізмів взаємодії стимулюватиме спільні ініціативи та обмін досвідом.

Посилення міжнародної кооперації. Поглиблення співробітництва з міжнародними організації та провідними країнами у сфері кібербезпеки надасть доступ до передових практик, навчальних програм та систем раннього передування.

Інтеграція України до глобальних безпекоаих ініціатив забезпечить її сприятливість протистояти транскордонним загрозам.

Стимулювання розвитку національної індустрії кіберзахисту. Зростання запиту на рішення у сфері кібербезпеки створює сприятливі умови для розвитку вітчизняних технологічних компаній, підтримки інноваційних стартапів та формування екосистеми цифрового захисту. Це не тільки посилює кіберстійкість держави, але й стимулюватиме економічне зростання та створення високооплачуваних робочих місць.

Формування культури цифрової безпеки. Підвищення рівня цифрової грамотності населення на впровадження освітніх ініціатив з кібергігієни змінить загальнонаціональні стійкість до соціальної інженерії та інших видів кіберзагроз.

Розвиток усвідомленого ставлення громадян до власної цифрової безпеки перетворює людський фактор із вразливості на елемент захисту держави.

Впровадження комплексного кіберзахисту у структуру безпеки держави принесло вагомі практичні досягнення. Міжвідомча координація значно пришвидшила ідентифікацію загроз та реагування на інциденти, що дозволяє блокувати атаки на початкових етапах. Сформована законодавча база чітко визначила сфери відповідальності та правила взаємодії між державними і приватними суб'єктами, зробивши процеси прозорішими та більш ефективними. Зміцнена система захисту критичної інфраструктури забезпечила неперервність роботи життєво важливих сервісів навіть під час потужних кібератак [ 3]. Впроваджені технології моніторингу суттєво зменшили кількість успішних проникнень. Міжнародна співпраця розширила арсенал технологій та методик протидії загрозам, а спільні тренування підвищили готовність до відбиття складних атак. Налагоджений обмін даними допомагає завчасно виявляти потенційні небезпеки. Просвітницька діяльність помітно знизила вразливість до соціальної інженерії та фішингу, підвищивши цифрову грамотність громадян і службовців. Аналітична робота спеціалізованих центрів дозволяє прогнозувати тенденції та адаптувати захисні механізми до еволюції загроз.

Повномасштабна війна рф проти України наочно показала, наскільки важливим є кіберпростір у сучасних збройних конфліктах. Масові кібератаки на урядові структури, енергетичний сектор, засоби зв'язку та інші елементи інфраструктури стали невід`ємною частиною гібридної тактик ворога, спрямованої на підрив стабільності, деморалізацію населення та ускладнення управління державою. У таких умовах питання кібербезпеки набуло ключового значення для обороноздатності та зміцнення національної безпеки.

Впровадження кібербезпеки у структуру національної безпеки України сформувало надійний захисний контур проти цифрових загроз сучасності. Ця інтеграція створила взаємопов'язану систему, що охоплює всі ключові сфери від державного управління до приватного сектору. Результатом стала помітно підвищена стійкість держави до кібернетичних атак та спроможність підтримувати стабільне функціонування критичних систем навіть в умовах інтенсивного гібридного протистояння, що значно зміцнило загальну безпекову позицію України.

**Бібліографія**


1. Худолій А. Кібербезпека: сучасні виклики перед Україною // Аналітичний вісник. – 2022. – № 4. – С. 14–20.
2. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства // Право і суспільство. – 2023. – № 1(48). – С. 122–128.
3. Кібербезпека в Україні: шляхи розвитку та можливості - https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html дата звернення: 17.05.2025).