**Дашковський А. В.,**
викладач кафедри забезпечення
державної безпеки,
Київський інститут Національної
гвардії України
*(м. Київ, Україна)*

# КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ КОМПОНЕНТ ДЕРЖАВНОЇ БЕЗПЕКИ

У сучасному світі кіберпростір відіграє ключову роль у функціонуванні державних інституцій, бізнесу та суспільства. В умовах цифровізації зростає залежність від інформаційних систем, що робить кібербезпеку важливим елементом державної безпеки. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», це сукупність заходів, спрямованих на захист життєво важливих інтересів держави в кіберпросторі.

Кіберпростір охоплює мережі, системи, пристрої та користувачів, які взаємодіють у цифровому середовищі. Його особливості — відсутність кордонів, анонімність та висока швидкість змін — створюють нові виклики для національної безпеки. [1]

Система кібербезпеки включає правове регулювання, діяльність відповідних органів, технічні засоби захисту, підготовку фахівців і міжнародну співпрацю. Успішне функціонування цієї системи можливе лише за умови координації між усіма її елементами та адаптації до постійно змінюваного середовища.

Кіберзагрози стали одним із головних викликів для держав у XXI столітті. Атаки на інформаційні системи можуть призводити до збоїв у роботі критичної інфраструктури, витоку конфіденційних даних, фінансових втрат і дестабілізації суспільства. Особливо небезпечними є дії, що здійснюються з політичними або військовими мотивами, зокрема кібершпигунство, саботаж або інформаційні операції.

Приклади масштабних кібератак, як-от атака вірусу Petya в Україні 2017 року, засвідчують, що кіберзагрози здатні паралізувати діяльність державних органів, енергетичних компаній та банків. Це підкреслює необхідність розробки стратегії активного попередження, швидкого реагування та посилення кіберстійкості держави.

Ще з кінця 1990-х років ЄС почав формувати політику мережевої та інформаційної безпеки (NIS), яка поступово еволюціонувала у системний підхід до захисту цифрової інфраструктури. Важливим етапом стало створення у 2004 році Європейського агентства ENISA, що відіграє ключову роль у координації зусиль держав-членів, підтримці стандартів безпеки та обміні кращими практиками. Прийнята у 2013 році перша Стратегія кібербезпеки ЄС закріпила принципи спільної відповідальності, поваги до прав людини та сприяння міжнародній співпраці. Цей досвід демонструє ефективність інтегрованого

підходу до кіберзахисту, поєднуючи національні зусилля з міждержавною координацією. [2]

Забезпечення кібербезпеки на державному рівні вимагає чіткої взаємодії правових, організаційних і технічних механізмів.

Одним із базових документів, що визначає державну політику у сфері кіберзахисту, є Національна стратегія кібербезпеки України (2021), яка передбачає розбудову стійкої системи кібербезпеки, розвиток міжвідомчої взаємодії та активізацію співпраці з партнерами з НАТО та ЄС. [3]

Ключову роль у системі відіграють державні органи: Держспецзв'язку — координує загальну політику у сфері кіберзахисту; СБУ — здійснює контррозвідувальну діяльність; Нацполіція — розслідує кіберзлочини; Міністерство оборони — забезпечує кіберзахист у секторі безпеки й оборони. Окрім того, в Україні діє Національний координаційний центр кібербезпеки при РНБО, який об’єднує зусилля всіх ключових учасників.

Важливою складовою є партнерство з приватним сектором, яке забезпечує гнучкість та інноваційність рішень. Також розвивається співпраця з міжнародними організаціями, зокрема НАТО, ЄС та ІТ-компаніями, що дозволяє обмінюватися досвідом, технічними рішеннями та інформацією про актуальні загрози.

З огляду на динамічність кіберзагроз, державна політика у сфері кібербезпеки потребує постійного оновлення та вдосконалення. Один із ключових напрямів — посилення нормативно-правової бази, зокрема узгодження українського законодавства із європейськими стандартами та впровадження механізмів оперативного реагування на нові типи атак.

З початку російського вторгнення в 2022 році, кіберпростір став ареною інтенсивних атак, що вражають як корпоративну, так і персональну та державну безпеку. 13–14 січня 2022 року відбулася масова атака на українські урядові веб-сайти з повідомленнями про нібито витік особистих даних. Невдовзі був виявлений шкідливий програмний комплекс WhisperGate, націлений на знищення файлів на урядових, неприбуткових та ІТ-організаціях. [4]

Другим важливим вектором є розвиток людського потенціалу: необхідне створення освітніх програм з кібербезпеки, підвищення кваліфікації фахівців, а також формування культури цифрової гігієни серед населення.

Також слід активізувати публічно-приватне партнерство, яке дозволяє ефективно реагувати на загрози за рахунок поєднання державного контролю й технологічних можливостей приватного сектору. Успішна практика таких взаємодій уже спостерігається у сфері банківської безпеки.

Окремої уваги потребує впровадження сучасних технологій, таких як штучний інтелект для моніторингу загроз, блокчейн для захисту даних і сучасні криптографічні протоколи. Ці інструменти можуть суттєво підвищити стійкість інформаційних систем держави.

Кібербезпека у сучасному світі є невід’ємною складовою державної безпеки, адже цифрові загрози можуть спричинити масштабні політичні, економічні та соціальні наслідки. В умовах постійного розвитку

кіберзлочинності та зростання числа кібератак держава повинна мати чітко вибудовану систему кіберзахисту, яка базується на оновленому законодавстві, ефективній взаємодії між державними структурами, приватним сектором і міжнародними партнерами.

Проаналізувавши основи кібербезпеки, типи загроз та чинну систему захисту в Україні, можна зробити висновок про потребу в її подальшому вдосконаленні. Основні напрями такого вдосконалення мають включати зміцнення правового поля, розвиток людського капіталу, впровадження сучасних технологій і поглиблення міжнародної співпраці.

Отже, тільки комплексний підхід до забезпечення кібербезпеки дозволить гарантувати стабільність функціонування державних інституцій, безпеку громадян і захист національних інтересів в умовах нової цифрової епохи.

***Список використаних джерел:***

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL:https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 14.04.2025).
2. Основні підходи й напрями розвитку політики кібербезпеки Європейського союзу. Електронне фахова наукове видання «Кібербезпека: освіта, наука, техніка» Т.М. Мужанова, С.В. Легомінова, Ю.В. Щавінський, Ю.М. Якименко, Г.П. Нестеренко. 2024 URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/577/469 (дата звернення: 14.04.2025).
3. Стратегія кібербезпеки України від 26.08.2021 № 447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 14.04.2025).
4. Ю.В. Завгородня. Державна політика в сфері кібербезпеки в умовах повномасштабної війни. Актуальні проблеми політики. 2024. Вип. 74 URL: http://app.nuoua.od.ua/archive/74_2024/10.pdf (дата звернення: 14.04.2025).