Віталій Волинець,
доктор юридичних наук,
професор кафедри готельно-ресторанної справи
Київського університету туризму, економіки і права
ORCID: 0009-0003-0714-236X

DOI https://doi.org/10.32782/2306-9082/2025-58-3

УДК 342.951

Правовий аналіз Стратегії кібербезпеки України: деякі актуальні питання

Указом Президента України № 447/2021 від 26 серпня 2021 р. було затверджено Стратегію кібербезпеки України. Цей стратегічний документ визначає основні напрями державної політики у сфері кібербезпеки на період до 2025 р.

На превеликий жаль, щороку зростає кількість кібератак, спрямованих на порушення конфіденційності, цілісності, доступності державних інформаційних ресурсів. Отже, кіберзахист об'єктів критичної інформаційної інфраструктури та безпечне функціонування кіберпростору залишаються пріоритетом держави.

Україна, перебуваючи в умовах повномасштабної збройної агресії Росії, справедливо розглядає кібербезпеку як один із ключових компонентів національної оборони. Стратегія кібербезпеки України, оновлена у 2021 році, передбачає побудову комплексної національної системи кіберзахисту, інтегрованої з європейськими та світовими партнерами. Починаючи з 2022 р. значну роль у кіберзахисті відіграють такі органи, як Держспецзв'язок, СБУ, а також об'єднання «ІТ-армія України».

Особливу увагу наразі приділено захисту урядових ІТ-систем, енергетики, телекомунікацій та банківської сфери. Україна також впроваджує принципи Zero Trust, розширює навчальні програми з кібергігієни, а також налагоджує міжнародну взаємодію з НАТО, ЄС і провідними технологічними компаніями.

На початку нашого аналізу стисло зазначимо про сучасний зарубіжний досвід у досліджуваному в цій статті напрямі.

Сполучені Штати Америки мають сьогодні одну з найрозвиненіших стратегій кібербезпеки у світі. Національна стратегія кібербезпеки, оприлюднена у 2023 р., передбачає всебічний підхід до захисту критичної інфраструктури, зокрема енергетики, транспорту, фінансів та охорони здоров'я. Особливий акцент зроблено на партнерстві між урядом і приватним сектором, який володіє значною частиною відповідної критичної інфраструктури.

Стратегія також передбачає перехід до більш активної та наступальної політики реагування на кіберзагрози. США оголошують про намір не лише

захищатися, а й проводити операції з нейтралізації джерел загроз до того, як вони завдадуть шкоди. Такий підхід називається «disruption forward», тобто йдеться про ефективні превентивні заходи.

В американській стратегії кібербезпеки йдеться про необхідність внесення фундаментальних змін в основну динаміку цифрової екосистеми, переклавши перевагу на бік її захисників і постійно перешкоджаючи силам, які їй загрожують. Головною метою тут виступає захищена, стійка цифрова екосистема, де атакувати системи дорожче, аніж захищати їх, де конфіденційна або приватна інформація безпечна та захищена, і де ані інциденти, ані помилки не призводять до катастрофічних, системних наслідків [1].

Ще одним важливим аспектом тут виступає посилення відповідальності розробників програмного забезпечення. Замість того, щоб уся відповідальність за безпеку лягала на користувачів, уряд США закликає до змін у дизайні та розробці програмного забезпечення, щоб воно з самого початку було безпечним.

Також окрема увага приділяється міжнародній співпраці. США активно зміцнюють кібербезпекові альянси, зокрема в межах НАТО та двосторонніх партнерств, прагнучи встановити єдині глобальні правила кіберповедінки, кіберзахисту.

Своєю чергою, Європейський Союз (ЄС) розвиває засади та основні положення кібербезпеки на основі принципів демократії, верховенства права та захисту прав людини. Основою регіональної політики виступає Європейська стратегія кібербезпеки, доповнена рамковими документами, такими як Директива NIS2 та Європейський акт про кіберстійкість [2].

Наразі ЄС зосереджений на посиленні кіберстійкості всіх держав-членів, на гармонізації стандартів безпеки та захисті критичної інфраструктури – зокрема енергетичних, транспортних і цифрових систем. Створено Агентство з кібербезпеки ЄС (ENISA), яке координує дослідження, інцидент-відповіді та навчання. Однією з головних ідей є формування «цифрового щита Європи», тобто мережі швидкого реагування на масштабні кіберінциденти [3].

Як зауважує М. В. Гуцалюк, спираючись на результати власного аналізу, дослідивши вісімнадцять європейських Стратегій та вісім Стратегій поза межами ЄС, ENISA відзначило чотири важливі етапи реалізації цих програмних документів: власне розробку, впровадження, оцінку та коригування. Відповідно, було запропоновано систему їх оцінювання. Так, відповідно до рекомендацій ENISA основними цілями оцінки стратегії кібербезпеки, заснованої на даному аналізі, є: 1) розробка політики та можливостей кіберзахисту; 2) досягнення кіберстійкості (здатність суб'єкта досягати бажаного результату незважаючи на кіберінциденти); 3) зменшення кіберзлочинності; 4) підтримка промисловості у сфері кібербезпеки; 5) безпека інформаційної критичної інфраструктури [4, с. 91–92].

Велика Британія навіть після виходу з ЄС зберегла тісну співпрацю з європейськими та трансатлантичними партнерами в сфері кібербезпеки. Британська стратегія кібербезпеки (оновлена на 2022–2030 роки) наголошує на створенні «найбезпечнішого місця для ведення бізнесу онлайн». Уряд тісно співпрацює з технологічною галуззю через структури на кшталт Національного центру кібербезпеки (NCSC).

Ключовими напрямами британської стратегії виступають: розвиток національного кіберпотенціалу, «кібергігієна» громадян, боротьба з онлайн-шахрайством, а також посилення кібероборони Збройних сил держави. Велика увага приділяється

інноваціям та партнерствам з приватним сектором. Так, зокрема, було створено програми для підтримки кіберстартапів [5].

Ізраїль також є одним із визнаних світових лідерів у галузі кібербезпеки, і ця сфера справедливо розглядається як частина національної доктрини безпеки. Завдяки співпраці між армією, урядом і технопарками, Ізраїль створив унікальну екосистему інформаційної безпеки та захисту. Центральним органом з відповідними повноваженнями виступає Національне управління з кібербезпеки, яке координує всі ініціативи, від оборони до просвітницьких кампаній.

Ізраїльська стратегія базується на принципі «активного захисту». Ідеться про швидке виявлення та нейтралізація загроз, включно з контроперераціями. Країна також є одним із найбільших експортерів кібертехнологій. Потужна кадрова база формується через службу в спеціальних армійських кіберпідрозділах [6].

Як справедливо підсумовує Я. С. Мануілов, сьогодні більшість держав світу визнають кібербезпеку ключовим елементом національної безпеки. Її забезпечення потребує створення та ефективного функціонування загальнодержавної системи, а також узгодженої й продуманої державної політики у сфері кібербезпеки. Така політика повинна ґрунтуватися на дотриманні міжнародного права, захисті основоположних цінностей, закріплених у національному законодавстві, та реалізації національних пріоритетів у кіберпросторі. У цьому контексті загальновизнаною практикою є доктринальне формулювання основ державної кібербезпекової політики у вигляді стратегічних документів, які окреслюють підходи до забезпечення безпеки в цифровому середовищі. Очевидно, що кожна стратегія в сфері кібербезпеки повинна враховувати не лише внутрішньодержавні політичні реалії, але й сучасні глобальні тенденції, що впливають на формування національної системи кіберзахисту [7, с. 99].

Нижче пропонуємо авторський аналіз ключових положень Стратегії кібербезпеки України, структурований за певними ключовими аспектами.

Стратегія кібербезпеки України спрямована передусім на забезпечення національних інтересів у кіберпросторі, захист прав і свобод громадян, а також на розвиток національного кіберпростору. Документ визначає основні загрози, цілі та завдання державної політики у сфері кібербезпеки.

Основні цілі Стратегії включають: створення ефективної системи управління кібербезпекою; забезпечення стійкості та безпеки національного кіберпростору; розвиток національних спроможностей у сфері кібербезпеки; забезпечення захисту прав і свобод громадян в інформаційному суспільстві.

Водночас Стратегія ідентифікує низку ключових загроз, серед яких зокрема: кібератаки на об'єкти критичної інфраструктури; розповсюдження шкідливого програмного забезпечення; несанкціонований доступ до інформаційних ресурсів; кібершпигунство та кібершахрайство; використання кіберпростору для пропаганди та дезінформації.

Ці загрози мають як внутрішнє, так і зовнішнє походження, що очевидно вимагає комплексного підходу до їх нейтралізації.

Очевидно, що практична реалізація цілей Стратегії є більш складним завданням, аніж нормативне формулювання її положень. А тому для досягнення поставлених цілей Стратегія передбачає реалізацію таких пріоритетних напрямів:

1) розвиток нормативно-правової бази: удосконалення законодавства у сфері кібербезпеки, зокрема гармонізація з міжнародними стандартами та зобов'язаннями;

2) інституційне забезпечення, а саме – посилення ролі Національного координаційного центру кібербезпеки, створення та розвиток спеціалізованих підрозділів у сфері кібербезпеки;

3) захист критичної інфраструктури: запровадження механізмів виявлення та реагування на кіберінциденти, підвищення стійкості об'єктів критичної інфраструктури до кіберзагроз;

4) міжнародне співробітництво також є важливим аспектом, особливо в контексті триваючої війни в Україні. Зокрема йдеться про участь у міжнародних ініціативах та об'єднаннях у сфері кібербезпеки, про обмін інформацією та досвідом з іноземними партнерами;

5) освіта та підготовка кадрів, а саме – розвиток системи освіти у сфері кібербезпеки, підвищення кваліфікації фахівців, проведення інформаційно-просвітницьких кампаній для населення.

Не менш важливим питанням стає запровадження механізмів реалізації Стратегії. Так, для ефективної реалізації Стратегії передбачено запровадження наступних кроків:

1) розроблення та затвердження планів заходів: створення детальних планів дій з визначенням відповідальних органів та строків виконання;

2) моніторинг та оцінка ефективності: запровадження системи моніторингу реалізації Стратегії, регулярна оцінка досягнення поставлених цілей та завдань;

3) фінансування заходів: забезпечення належного фінансування заходів з реалізації Стратегії за рахунок державного бюджету та інших джерел.

Як слушно висловився Д. В. Дубов, аналіз внутрішніх проблем, що перешкоджають ефективній реалізації державної політики у сфері кібербезпеки, потребує системного підходу та розширення кола учасників, зокрема із залученням експертного середовища. Це забезпечить всебічну оцінку ситуації та формування збалансованих рішень.

Серед основних викликів в досліджуваному аспекті потрібно виокремити: використання застарілих ІТ-систем із невиправленими вразливостями, зростання масштабів кібератак на критичну інфраструктуру, активні деструктивні дії РФ, низький рівень кіберобізнаності населення, недостатній розвиток державно-приватного партнерства, ризики, пов'язані з цифровою трансформацією, витоки персональних даних та відсутність актуальної інформації про реальний стан кіберзахисту [8].

А тому стає очевидним, що Стратегія кібербезпеки повинна не лише окреслювати цілі, а й формувати бачення безпечної в «цифровому» контексті України, у якій забезпечується кіберстійкість суспільства, економіки та ефективна міжсекторальна взаємодія. Основною метою є не розбудова системи заради самої системи, а навпаки – гарантування безпеки, добробуту та прав громадян. У цьому контексті теоретично доцільно та практично необхідно структурувати стратегічні цілі за трьома ключовими напрямами: стримування, стійкість, взаємодія.

Важливо підкреслити, що чинна Стратегія кібербезпеки України передбачає комплекс заходів для посилення обороноздатності держави у кіберпросторі, що структуровані за шістьма ключовими цілями. Перша з них (С. 1) спрямована на формування дієвої системи кібероборони. Планується створити кібервійська у структурі Міністерства оборони України та забезпечити їх належними ресурсами. У межах цієї мети передбачено також розроблення плану кібероборони як складової загального оборонного плану держави, а також регулярне проведення спільних навчань із підрозділами країн НАТО не менше двох разів на рік.

Друга стратегічна ціль (С. 2) полягає в розвитку потенціалу сил сектору безпеки і оборони у сфері кібербезпеки. Зокрема, йдеться про формування сучасного кіберпростору в межах інфраструктури Міністерства оборони, вдосконалення механізмів виявлення, попередження і протидії кібератакам, а також розвиток спеціалізованої освіти у цій сфері.

Третя ціль (С. 3) передбачає підвищення рівня кіберзахищеності об'єктів критичної інформаційної інфраструктури. Україна прагне розбудувати єдину систему державного управління захистом таких об'єктів, упровадити обов'язкову сертифікацію та аудит безпеки, а також стимулювати розвиток засобів вітчизняного виробництва для кіберзахисту.

Четверта ціль (С. 4) спрямована на активізацію міжнародного співробітництва у сфері кібербезпеки. Україна планує інтегруватися до єдиного кіберпростору з державами-членами ЄС і НАТО, приєднатися до Будапештської конвенції про кіберзлочинність та зміцнювати двосторонню взаємодію з ключовими партнерами в цьому напрямі.

Окрім стратегічних цілей, документ також містить окремі компоненти К. 1 і К. 2. Зокрема, компонент К. 1 передбачає посилення спроможності правоохоронних органів у протидії кіберзлочинності, у тому числі через впровадження новітніх технологій, обмін інформацією з міжнародними структурами та створення спільних оперативних груп. Компонент К. 2 стосується підвищення цифрової обізнаності населення – планується впровадження освітніх програм, розвиток наукових досліджень у сфері кібербезпеки та створення національного центру кіберосвіти.

Насамкінець звернемо увагу на Положення про організаційно-технічну модель кіберзахисту, яке було затверджено постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426. У цьому документі зокрема наголошено на тому, що організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливостей комунікаційних систем. Своєю чергою, організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки.

Цей нормативний акт також оперує низкою інших важливих в контексті правозастосування термінів, а саме: кібергігієна – уміння та навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз; технологічна інфраструктура кіберзахисту – організована сукупність сил та засобів кіберзахисту, інфраструктурних об'єктів, що забезпечують функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту.

До слова в нашій державі уже напрацьовано чимало інших підзаконних нормативних актів, що покликані регулювати дедалі більш актуальну проблематику кіберзахисту країни, населення, інших стейкхолдерів. Чимало з них запроваджені та активно застосовуються на практиці спеціальним органом влади – Державною службою спеціального зв'язку та захисту інформації України.

Примітно, що 7 березня 2025 р. Кабінет Міністрів України затвердив план заходів з реалізації Стратегії кібербезпеки на 2025 рік. Документ,

підготовлений фахівцями Держспецзв'язку, передбачає виконання комплексу завдань, спрямованих на зміцнення кіберстійкості держави. Ключові напрями включають: удосконалення нормативно-правового регулювання у сфері кібербезпеки; розвиток організаційно-технологічної інфраструктури національної системи кібербезпеки; розширення міжнародного співробітництва; запровадження ризик-орієнтованих підходів для захисту критичної інфраструктури та державних органів; підвищення рівня кадрового забезпечення. На реалізацію цих заходів у Державному бюджеті на 2025 р. передбачено значну суму – 468,8 млн грн.

Також додамо від себе, що в попередніх публікаціях ми аналізували питання, пов'язані з правовим захистом конфіденційності та безпеки даних в електронній комерції [9, с. 1–11]. Переконані, що ця галузь правового регулювання є надзвичайно актуальною та перспективною, особливо в контексті реалізації Стратегії кібербезпеки України.

Висновки. Підсумовуючи проведений аналіз, зазначимо, що Стратегія кібербезпеки України є комплексним документом, який визначає основні напрями державної політики у сфері кібербезпеки на середньострокову перспективу. Реалізація цього документа сприятиме підвищенню стійкості національного кіберпростору, захисту прав і свобод громадян, а також зміцненню позицій України на міжнародній арені у сфері кібербезпеки.

Водночас сьогодні стає очевидним, особливо в умовах захисту України від агресії, що успішне впровадження Стратегії вимагатиме скоординованих дій усіх зацікавлених сторін, належного ресурсного забезпечення та постійного моніторингу ефективності реалізації заходів щодо забезпечення кібербезпеки.

2025 рік є завершальним етапом виконання Стратегії кібербезпеки на 2021–2025 роки. За підсумками оцінювання, проведеного вітчизняними експертами, досягнуто лише 63 % запланованих цілей. Це зумовлює необхідність максимальної концентрації зусиль у поточному році для повної реалізації положень Стратегії.

Список використаних джерел

1. National Cybersecurity Strategy. March 2023. URL: https:/bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 22.05.2025).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 (дата звернення: 22.05.2025).

3. The European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/ (дата звернення: 22.05.2025).

4. Гуцалюк М. В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик. *Інформація і право*. 2019. № 2. С. 90–99.

5. Government Cyber Security Strategy. Building a cyber resilient public sector. URL: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf (дата звернення: 22.05.2025).

6. Meridor D., Eldadi D. Israel's National Security Doctrine: the Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later. Memorandum № 187, 2019. URL: https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf (дата звернення: 22.05.2025).

7. Мануілов Я. С. Огляд новел вітчизняного законодавства у сфері забезпечення кібербезпеки (на прикладі Стратегії кібербезпеки України на 2021–2025 роки. *Інформація і право*. 2021. № 4. С. 98–105.

8. Дубов Д. В. Формуючи нову Стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування? Національний інститут стратегічних досліджень. 2021. URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf.

9. Волинець В. В. Юридичні аспекти захисту конфіденційності та безпеки даних в електронній комерції. *Академічні візії*. 2024. № 29. С. 1–11. DOI: https://doi.org/10.5281/zenodo.11189625.

Волинець В. В. Правовий аналіз Стратегії кібербезпеки України: окремі актуальні питання

У науковій статті досліджено ключові засади та механізми реалізації Стратегії кібербезпеки України на період до 2025 року. Автор акцентує увагу на тому, що в умовах повномасштабної збройної агресії Росії, кібербезпека стала невід'ємною складовою національної безпеки. Стратегія спрямована на створення ефективної системи управління, захист критичної інформаційної інфраструктури, розвиток кадрового потенціалу та міжнародну інтеграцію України у сфері кіберзахисту.

Розглядається міжнародний досвід, зокрема практики США, ЄС, Великої Британії, Ізраїлю, що стали орієнтирами для національного стратегічного планування. Значну увагу приділено структурі української Стратегії, яка містить шість стратегічних цілей (С. 1–С. 4, К. 1, К. 2), що охоплюють формування кібервійськ, протидію кіберзагрозам, захист критичної інфраструктури, посилення міжнародного співробітництва, боротьбу з кіберзлочинністю та розвиток цифрової обізнаності населення.

Окремо проаналізовано організаційно-технічну модель кіберзахисту, а також нормативну базу, включаючи постанови Кабінету Міністрів та роль Держспецзв'язку. Автор підкреслює, що Стратегія має комплексний характер і вимагає міжсекторальної взаємодії, постійного моніторингу та коригування.

Окремо наголошено на тому, що для успішного впровадження Стратегії передбачено реалізацію таких ключових заходів: планування діяльності; моніторинг та оцінювання; ресурсне забезпечення.

Також автором звернуто увагу на те, що Державна служба спеціального зв'язку та захисту інформації України напрацювала чималу кількість підзаконних нормативних актів, що покликані регулювати сферу кіберзахисту нашої держави.

У висновках до роботи зауважено, що реалізація Стратегії сприятиме підвищенню кіберстійкості держави, захисту прав громадян і зміцненню міжнародних позицій України. Однак станом на початок 2025 року досягнуто лише 63% поставлених цілей, що потребує посилення зусиль у фінальний рік її дії.

Ключові слова: кібербезпека, національна стратегія, критична інфраструктура, міжнародне співробітництво.

Volynets V. Legal analysis of the Cybersecurity Strategy of Ukraine: some relevant issues

The research paper examines the key principles and mechanisms for implementing the Cybersecurity Strategy of Ukraine for the period until 2025. The author emphasizes that in the conditions of full-scale armed aggression by Russia, cybersecurity has become an integral part of national security. The strategy is aimed at creating an effective management system, protecting critical information infrastructure, developing human resources and international integration of Ukraine in the field of cyber defense.

International experience is considered, in particular the practices of the USA, EU, Great Britain, Israel, which have become guidelines for national strategic planning. Considerable attention is paid to the structure of the Ukrainian Strategy, which contains six strategic

goals (S. 1–S. 4, K. 1, K. 2), covering the formation of cyber troops, countering cyber threats, protecting critical infrastructure, strengthening international cooperation, combating cybercrime and developing digital awareness of the population.

Separately, the organizational and technical model of cyber defense, as well as the regulatory framework, including the resolutions of the Cabinet of Ministers and the role of the State Service for Special Communications, are analyzed. The author emphasizes that the Strategy is comprehensive in nature and requires intersectoral interaction, constant monitoring and adjustment.

It is especially emphasized that for the successful implementation of the Strategy, the implementation of the following key measures is envisaged: activity planning; monitoring and evaluation; resource provision.

The author also draws attention to the fact that the State Service for Special Communications and Information Protection of Ukraine has developed a considerable number of subordinate regulatory acts designed to regulate the sphere of cyber defense of our state.

The conclusions to the work note that the implementation of the Strategy will contribute to increasing the cyber resilience of the state, protecting the rights of citizens and strengthening the international positions of Ukraine. However, as of the beginning of 2025, only 63 % of the set goals have been achieved, which requires increased efforts in the final year of its operation.

Key words: cybersecurity, national strategy, critical infrastructure, international cooperation.