УДК 342.951

**ТКАЧУК Н.А.**, *кандидат юридичних наук,*
старший науковий співробітник НДІІП НАПрН України

# СТАН ТА ПРОБЛЕМНІ ПИТАННЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

***Анотація.*** *У статті досліджено стан і проблемні питання реалізації Стратегії кібербезпеки України та запропоновано шляхи удосконалення стратегічного планування у сфері кібербезпеки держави.*

***Ключові слова:*** *Стратегія кібербезпеки України, план реалізації Стратегії кібербезпеки України, кібербезпека, стратегічне планування, нормативно-правове регулювання.*

***Summary.*** *The article examines the state and problematic issues of implementing the Cybersecurity Strategy of Ukraine, and suggests ways to improve the strategic planning in the field of cybersecurity of the state.*

***Keywords:*** *the Cybersecurity Strategy of Ukraine, Ukraine's Cybersecurity Strategy Implementation Plan, cyber security, strategic planning, legal regulation.*

***Аннотация.*** *В статье исследуется состояние и проблемные вопросы реализации Стратегии кибербезопасности Украины, а также предложены пути усовершенствования стратегического планирования в сфере кибербезопасности государства.*

***Ключевые слова:*** *Стратегия кибербезопасности Украины, план реализации Стратегии кибербезопасности Украины, кибербезопасность, стратегическое планирование, нормативно-правовое регулирование.*

**Постановка проблеми.** Протягом останніх років в Україні триває активна розбудова національної системи кібербезпеки, що обумовлено перетворенням кіберпростору на невід'ємну складову суспільного життя у поєднанні з актуалізацією кіберзагроз життєво важливим інтересам держави, правам та свободам громадян в умовах гібридної агресії з боку Російської Федерації.

Фундаментом дієвої системи кібербезпеки, безумовно, є ефективна нормативно-правова база, основою якої в Україні стала ухвалена у березні 2016 року "Стратегія кібербезпеки України" (далі – Стратегія) [1].

Стратегія забезпечила підґрунтя для розроблення подальших нормативно-правових актів з питань кібербезпеки та визначила основні засади та напрями державної політики у цій сфері. Кожного року Розпорядженням Кабінету Міністрів України затверджується річний план заходів з її реалізації, який включає конкретні завдання для органів державної влади, спрямовані на виконання положень Стратегії, вирішення існуючих проблемних питань та розбудову кібербезпекового потенціалу України.

Разом з тим, сьогодні в державі відсутній механізм оцінки ефективності реалізації Стратегії, а більшість заходів, передбачених планами її реалізації на 2016 – 2018 роки, залишаються невиконаними. Ситуація, що склалася, негативно впливає на стан та ускладнює формування дієвої державної політики у цій царині, зводить нанівець ефективність документів стратегічного планування кібербезпекової сфери.

**Результати аналізу наукових публікацій.** Проблематика правового регулювання сфери кібербезпеки України висвітлювалася у наукових працях О. Довганя, Д. Дубова, Р. Лукянчука, А. Марущака, М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева та

ін. вітчизняних дослідників. Проблеми стратегічного планування у сфері державного управління вивчалися такими вітчизняними вченими як А. Гнатенко, О. Берданова, М. Латинін, О. Лебединська, М. Лесечко, І. Лех, Т. Тарасюк, Ю. Шаров та ін. Водночас, слід констатувати, що питання реалізації Стратегії кібербезпеки України залишилося поза увагою комплексних наукових досліджень. На практиці це призводить до недооцінення ролі документів стратегічного планування, як однієї із важливих складових організаційно-правової основи функціонування національної системи кібербезпеки та формування державної кібербезпекової політики.

**Метою статті** є визначення стану та проблемних питань реалізації Стратегії кібербезпеки України на сучасному етапі.

**Виклад основного матеріалу.** Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики у сфері кібербезпеки. Вказаний документ є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [2].

Цей документ є базисом стратегічного планування держави у сфері кібербезпеки, що за своєю суттю є адаптивним процесом, за допомогою якого повинні здійснюватись регулярні розроблення й корекція системи планів, перегляд змісту заходів щодо їх виконання на основі безперервного контролю й оцінки змін, які відбуваються ззовні та всередині системи [3, с. 55].

Контроль за виконанням стратегій, досягненням цільових орієнтирів, а також їх коригування сучасна теорія державного управління визначає як невід'ємний елемент стратегічного управління. Як зазначає Г. Тарасюк, роль контролю як функції управління полягає в тому, що він є засобом здійснення зворотного зв'язку в системі управління. Головний його сенс полягає у створенні гарантій виконання планових рішень [4, с. 290].

Разом із тим, в Україні дієва система стратегічного контролю, яка б забезпечувала об'єктивну оцінку та здійснення корегуючого впливу щодо стану реалізації Стратегії кібербезпеки, а також гарантій виконання її положень, на сьогодні відсутня.

Наразі реалізація положень Стратегії відбувається в рамках виконання щорічних планів, які формуються Держспецзв'язку України та затверджуються відповідними Розпорядженнями Кабінету Міністрів України. Водночас, аналіз стану виконання на загальнодержавному рівні планів реалізації Стратегії кібербезпеки України на 2016 – 2018 роки [5 – 7], проведений автором, засвідчив, що вказані документи носять переважно декларативний характер. Так, більшість заходів, передбачених ними, наразі, не виконано або виконано частково та/або із простроченням встановлених термінів. Кінцевий результат наявний лише щодо деяких із пунктів. Наприклад, прийнято Закон України "Про основні засади забезпечення кібербезпеки України", створено Ситуаційний центр забезпечення кібербезпеки СБ України, удосконалено вимоги до захисту інформації в ІТС банківської сфери (шляхом прийняття відповідного відомчого нормативно-правового акту НБУ[1]).

Багато інших важливих питань на сьогодні не вирішено: не створено перелік інформаційно-телекомунікаційних систем критичної інфраструктури, не імплементовано Конвенцію ЄС про кіберзлочинність, не побудовано захищений дата-центр для органів державної влади, не вжито ефективних заходів щодо стимулювання розроблення

[1] Постанова Правління НБУ "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" від 28.09.17 р. № 95.

вітчизняного програмного забезпечення, не впроваджено регламенти та директиви щодо стандартів ЄС із захисту об'єктів критичної інфраструктури, відсутня система аудиту інформаційної безпеки таких об'єктів, не сформовано основні індикатори стану кібербезпеки та показники ефективності виконання Стратегії кібербезпеки України, не створено єдину систему виявлення кіберзагроз та платформу обміну інформацією (даними) між суб'єктами кібербезпеки тощо.

Хоча всі пункти планів, якими були передбачені ці завдання, містили конкретні кінцеві дати виконання та відповідальних за їх виконання державних суб'єктів. Наприклад, відповідальним органом за виконання 15-ти пунктів із наявних 18-ти, передбачених Планом реалізації Стратегії кібербезпеки України на 2018 рік (затвердженим розпорядженням КМУ від 11.07.18 р. № 481-р), є Державна служба спеціального зв'язку та захисту інформації України.

Крім того, своєчасне та ефективне виконання заходів з реалізації Стратегії значно ускладнює той факт, що плани її реалізації формуються Держспецзв'язку України, і відповідно, затверджуються Урядом із порушенням встановленого рішенням РНБО України терміну (до початку планового року) [1].

Так, план реалізації Стратегії на 2017 рік було затверджено КМУ у березні 2017 року (із простроченням терміну на 3 місяці), а на 2018 рік – у липні 2018 року (із простроченням терміну на 7 місяців). Станом на березень 2019 року (під час написання даної статті) план реалізації Стратегії на 2019 рік також відсутній. Ситуація, що склалася, апріорі унеможливлює своєчасне виконання окремих планових позицій суб'єктами кібербезпеки.

Наприклад, відповідно до Розпорядження КМУ "Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки" від 11.07.18 р. № 481-р [7], звітувати про хід виконання Плану необхідно було до 10 липня 2018, незважаючи на те, що цей план було затверджено на день пізніше строку звітування. Цей приклад ілюструє абсурдність ситуації, яка склалася у сфері стратегічного планування та контролю за виконанням заходів з реалізації Стратегії кібербезпеки України.

Безумовно, для того, щоб існуючі законодавчі та підзаконні нормативно-правові акти мали не лише декларативний характер, а дійсно були фундаментом подальшої реалізації конкретних заходів у сфері забезпечення кібербезпеки, необхідно запровадити дієвий механізм контролю щодо їх своєчасного та належного виконання всіма без виключення суб'єктами забезпечення кібербезпеки України. А у разі не виконання – повинен працювати механізм дієвого реагування та вжиття відповідних заходів правового впливу та притягнення до відповідальності.

Відповідно до чинних нормативно-правових актів[2], суб'єктами, на які покладені завдання із здійснення контролю із цього питання, є Секретар РНБО України (у частині забезпечення контролю за виконанням указу Президента України, яким затверджена Стратегія кібербезпеки) [8] та Секретаріат Кабінету Міністрів України (у частині забезпечення контролю та моніторингу стану виконання розпоряджень КМУ, якими затверджуються щорічні плани реалізації Стратегії) [9]. Крім того, питання стану реалізації Стратегії кібербезпеки України щорічно розглядається на засіданні Національного координаційного центру кібербезпеки, який повинен забезпечувати координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки

[2] Положення про порядок організації та здійснення контролю за виконанням указів, розпоряджень і доручень Президента України, затвердженого Указом Президента України від 19.02.02 р. № 155, та Регламенту Кабінету Міністрів України, затвердженого Постановою Кабінету Міністрів України від 18.07.07 р. № 950.

України, підвищувати ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки [10].

Водночас, основні завдання стратегічного контролю із надання об'єктивної оцінки та вжиття заходів впливу щодо неналежної реалізації Стратегії кібербезпеки відповідальними суб'єктами, на сьогодні, не здійснюються, а невиконані завдання просто переносяться на наступний рік (про що свідчить аналіз планів реалізації Стратегії на 2016 – 2018 роки).

Крім того, не створені умови, які б забезпечили можливість ефективного контролю за станом реалізації Стратегії кібербезпеки з боку громадянського суспільства. Закон України "Про національну безпеку" [2] визначає дотримання засад демократичного цивільного контролю (одним із елементів якого є громадський контроль) за функціонуванням сектору безпеки і оборони одним із основних принципів формування державної політики у всіх сферах національної безпеки. Предметом такого контролю визначено стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони, тобто у т.ч. Стратегії кібербезпеки України. Наявність дієвого громадського контролю є невід'ємною умовою демократії та ознакою правової держави.

Водночас, здійснення такого контролю у сфері кібербезпеки ускладнює відсутність відповідної публічної інформації з боку компетентних державних органів, в першу чергу Державної служби спеціального зв'язку і захисту інформації України, як органу, на який покладено завдання із узагальнення інформації про хід виконання планових заходів із реалізації Стратегії кібербезпеки України, а також Національного координаційного центру кібербезпеки. Сприяти вирішенню цього питання могло б оприлюднення на офіційних веб-ресурсах вказаних органів узагальнених матеріалів щодо стану та конкретних результатів діяльності суб'єктів національної системи кібербезпеки із виконання планів реалізації Стратегії з урахуванням вимог Закону України "Про державну таємницю".

Відповідно до основоположних засад державного управління невід'ємною умовою ефективності стратегічного планування є обов'язковий стратегічний моніторинг, саме на підставі якого має відбуватися корегування основних цілей та завдань стратегічних документів [11]. Планування щорічних заходів з реалізації Стратегії кібербезпеки України має ґрунтуватися на оцінці поточного стану реалізації Стратегії, конкретних результатів виконання планових заходів за попередні періоди, а також аналізі стану кіберзахисту та кібербезпеки держави.

Законом України "Про національну безпеку" запроваджено проведення комплексного огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, підготовка якого покладена на Держспецзв'язку України. У контексті кібербезпеки цей огляд і повинен, у тому числі, відігравати функцію стратегічного моніторингу та бути основою подальшого розроблення документів стратегічного планування кібербезпекової сфери.

Водночас, незважаючи на вимоги закону, підготовка вказаного огляду, на сьогодні, зазначеним відомством не проводилася, що негативно впливає на якість стратегічного планування у сфері кібербезпеки та кіберзахисту.

Також відсутня методика формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України, створення якої відповідно до розпоряджень Кабінету Міністрів України мало бути вже завершене Державною службою спеціального зв'язку та захисту інформації України.

Зокрема, планом реалізації Стратегії кібербезпеки України на 2017 рік (пунктом 15) було передбачено протягом 2017 року здійснити *"формування переліку основних показників ефективності виконання Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик"* [6]. Планом реалізації Стратегії на 2018 рік (пунктом 13) знову передбачалось здійснити *"розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик"* вже протягом 2018 року [7]. Але ні у 2017, ні у 2018 роках ці завдання виконані не були (відповідальний за їх виконання орган – Держспецзв'язку). Отже, на сьогодні, будь-яка офіційна методика та показники ефективності виконання Стратегії кібербезпеки України відсутні, що фактично дозволяє уникати проведення відповідальним органом огляду стану її виконання, результати якого, вочевидь, продемонструють неефективність та формальний підхід до реалізації документів стратегічного планування в державі.

Сьогодні в державі поступово починається процес розроблення проекту нової Стратегії кібербезпеки України на 2021 – 2025 роки. Однак, без здійснення належної оцінки та вирішення проблемних питань щодо стану реалізації існуючої – така робота лише засвідчить формальний підхід до стратегічного планування у сфері кібербезпеки та пріоритетність не результату, а власне, процесу заради процесу. В умовах гібридної агресії та необхідності протистояння кіберзагрозам Україна собі це дозволити не може.

**Висновки.**

1. На сьогодні, стан реалізації Стратегії кібербезпеки України є незадовільним, що негативно впливає на всю сферу кібербезпеки та кіберзахисту України та є свідченням формального підходу з боку відповідальних державних органів до стратегічного планування, формування та реалізації державної політики, а також здійснення стратегічного контролю у цій сфері.

2. З метою підвищення ефективності стратегічного планування та сприяння належній реалізації Стратегії кібербезпеки пропонується:

- терміново розробити критерії та започаткувати впровадження механізму оцінки ефективності реалізації Стратегії кібербезпеки України на державному рівні;
- провести передбачений Законом України "Про національну безпеку України" огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, який обов'язково повинен враховуватись у ході подальшої розробки документів стратегічного планування кібербезпекової сфери та здійснення оцінки їх реалізації;
- запровадити дієвий контроль з боку Кабінету Міністрів та РНБО України та щодо своєчасного та якісного виконання компетентними державними органами завдань, спрямованих на реалізацію Стратегії кібербезпеки України, із здійсненням (або ініціюванням) заходів дисциплінарного впливу щодо відповідальних посадових осіб, які не забезпечили їх належне виконання;
- систематично розміщувати інформацію на офіційних веб-ресурсах Держспецзв'язку України та Національного координаційного центру кібербезпеки при РНБО України щодо стану виконання відповідальними державними органами поточних планів реалізації Стратегії кібербезпеки України та отриманих кінцевих результатів (з урахуванням вимог Закону України "Про державну таємницю");
- забезпечити своєчасне (до початку звітного періоду) формування Держспецзв'язку України та, відповідно, затвердження Урядом щорічних планів реалізації Стратегії кібербезпеки України.

## Використана література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про стратегію кібербезпеки України": Указ Президента України. URL: http://zakon.rada.gov.ua/laws/show/96/2016

2. Про національну безпеку України: Закон України від 21.06.18 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19

3. Гнатенко А.І. Стратегічне планування у сфері державного управління: концептуальні підходи. *Державне управління та місцеве самоврядування*: зб. наук. пр. Дніпропетровськ: Вид-во ДРІ НАДУ. 2013. № 3(18). С. 51-60.

4. Тарасюк Г.М. Контроль в системі управління плановою діяльністю підприємства. *Міжнародний збірник наукових праць*. 2010. № 1(16). С. 284-299.

5. Про затвердження Плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 24.06.16 р. № 140-р. URL: https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80

6. Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.17 р. № 155-р. URL: http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80

7. Про затвердження Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 11.07.18 р. № 481-р. URL: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80

8. Про порядок організації та здійснення контролю за виконанням указів, розпоряджень і доручень Президента України: Указ Президента України від 19.02.02 р. № 155. URL: https://zakon.rada.gov.ua/laws/show/155/2002

9. Про затвердження Регламенту Кабінету Міністрів України: Постанова Кабінету Міністрів України від 18.07.07 р. № 950. URL: https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF

10. Президент затвердив Положення про Національний координаційний центр кібербезпеки. URL: https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-nacionalnij-koordinacijn-37329

11. Назаров В.П. Стратегічне планування як важливий чинник підвищення ефективності державного управління. *Влада.* 2013. № 12. С. 4-11.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~