УДК 681.3 https://doi.org/10.15407/pp2020.02-03.278

# ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ УКРАЇНИ: СУТНІСТЬ, СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

*А.І. Семенченко, В.Л. Плескач, О.А. Заярний, М.В. Плескач*

У дослідженні здійснено аналіз організаційно-правових механізмів державного управління забезпеченням кібернетичної безпеки та кібернетичного захисту України, надано визначення його сутності, місця в системі стратегічного планування та управління сектором безпеки та оборони, проведено оцінку окремих аспектів забезпечення кібернетичної безпеки в Україні. Крім того, у статті містяться рекомендації щодо вдосконалення системи забезпечення кібернетичної безпеки в Україні, зокрема надано пропозиції щодо усунення наявних колізій і прогалин в основних нормативно-правових актах, що регулюють сферу забезпечення національної, інформаційної та кібернетичної безпеки України, у тому числі шляхом гармонізації українського законодавства з міжнародними правовими актами у цій галузі.

Ключові слова: кібербезпека, кіберзахист, об’єкти критичної інфраструктури, система забезпечення кібернетичної безпеки.

В исследовании осуществлен анализ организационно-правовых механизмов государственного управления обеспечением кибербезопасности и кибернетической защиты Украины, дано определение его сущности, места в системе стратегического планирования и управления сектором безопасности и обороны, показана оценка отдельных аспектов обеспечения кибернетической безопасности в Украине. Кроме того, в статье содержатся рекомендации по совершенствованию системы обеспечения кибернетической безопасности в Украине, в частности даны предложения по устранению имеющихся коллизий и пробелов в основных нормативно-правовых актах, регулирующих сферу обеспечения национальной, информационной и кибернетической безопасности Украины, в том числе путем гармонизации украинского законодательства с международными правовыми актами в этой области.

Ключевые слова: кибербезопасность, киберзащита, объекты критической инфраструктуры, система обеспечения кибернетической безопасности.

This article is devoted to the organizational and legal mechanisms of the cyber security public administration and cyber security in Ukraine, the definitions of essence, the role in the system of strategic planning and management of the security and defense sector are given. Some aspects of cyber security in Ukraine have been evaluated. In addition, recommendations of improving the cyber security system in Ukraine are proposed, such as, proposals were made to eliminate the existing gaps in the main legal acts regulating the sphere of ensuring national, information and cyber security of Ukraine, including through the harmonization of Ukrainian legislation with international legal acts in this field.

Key words: cyber security, security defense, critical infrastructure, securement system of cyber security.

## Вступ

Однією з необхідних умов успішного формування та реалізацій державної політики у сфері кібербезпеки та кіберзахисту є її ефективне політичне, організаційно-правове, інформаційно-аналітичне, техніко-технологічне, науково-методологічне, методичне та інші види забезпечення. Моніторинг, аналіз та оцінку стану такого забезпечення та перспективи його розвитку на загальнодержавному рівні здійснюють, насамперед, у процесі проведення низки взаємопов’язаних оглядів сектору безпеки та оборони України, що згідно зі статтею 27 Закону України «Про національну безпеку України» охоплює: комплексний огляд сектору безпеки та оборони та такі його окремі складові як-от огляд: стану оборони, громадської безпеки та цивільного захисту, оборонно-промислового комплексу, розвідувальних органів України, загальнодержавної системи боротьби з тероризмом, стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. За результатами цих оглядів у визначеній законодавством послідовності формують концептуальні, стратегічні, планові та програмні документи з розвитку сектору безпеки та оборони, починаючи від загальної Стратегії національної безпеки України та її окремих складових, у тому числі, Стратегії кібербезпеки України та Національної розвідувальної програми, на основі середньострокового та короткострокового планування.

Законодавством визначено низку факторів ініціації довгострокових стратегічних документів. Так згідно зі статтею 26 Закону України «Про національну безпеку України» Стратегію національної безпеки України розробляють за дорученням Президента України протягом шести місяців після його вступу на пост, а на її основі мають бути сформовані інші документи стратегічного планування у сферах національної безпеки і оборони, а саме стратегія: розвитку людського капіталу, воєнної безпеки, громадської безпеки та цивільного захисту, розвитку оборонно-промислового комплексу, економічної, екологічної, інформаційної безпеки, кібербезпеки; також національна розвідувальна програма, стратегія з питань зовнішньополітичної безпеки, стратегія з питань державної безпеки, контррозвідки та боротьби з тероризмом.

Іншою причиною ініціації початку розробки системи взаємопов’язаних стратегічних документів може бути різка зміна ситуації та умов функціювання сектору безпеки та оборони, які не були передбачені на етапі її

формування, та які не можна компенсувати через їх коригування, що мало місце, наприклад, у 2015 та 2016 роках у зв'язку з агресією Росії проти України, коли були прийняті нові Стратегія національної безпеки України, Воєнна доктрина України, Доктрина інформаційної безпеки України, Стратегія кібербезпеки України тощо [1, 2].

Тому актуальність проблеми зумовлена недосконалістю наявного теоретико-методологічного апарату механізмів державного управління забезпеченням кібербезпеки громадян, суспільства та держави, зокрема щодо організації та проведення оглядів в цій сфері, вимогами законодавства, невідповідністю вимог щодо стану кібербезпеки та рівнем його забезпечення.

**Аналіз останніх досліджень і публікацій.** Проблеми забезпечення кібербезпеки та кіберзахисту громадян, супільства держави розглянуто у працях К. Александера (Alexander K.), Дж. Ліпмана (Liepman J.), В. Мазурова, Р. Олдрича (Aldrich R.), Є. Старостиної, М. Шмітта (Schmitt M.), А. Щетилова. Серед вітчизняних науковців необхідно виокремити праці В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, Д. Дубова, О. Задерейко, Н. Логінової, Д. Мялковського, В. Петрова, Ю. Прокоп, Т. Станіславського, Т. Тропініної, О. Трофименко та ін.

Однак, віддаючи належне працям вищевказаних дослідників, нині в Україні системних досліджень з питань огляду стану кібербезпеки та кіберзахисту, недостатньо.

**Мета роботи.** Визначення сутності, місця в системі стратегічного планування та управління сектором безпеки та оборони організаційно-правових механізмів державного управління забезпеченням кібербезпеки та кіберзахисту, аналізу їх стану, взаємодію між собою, обґрунтування пріоритетних напрямків розвитку та удосконалення понятійно-категоріального апарату.

## Виклад основного матеріалу

Загальну оцінку стану кібербезпеки в Україні наведено в Стратегії кібербезпеки України, що характеризується зростанням кількості та потужності кібератак, мотивованих інтересами окремих держав, груп та осіб, поширенням випадків незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства у мережі Інтернет.

Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

На рівень кібербезпеки та кіберзахисту в Україні впливає низка таких основних негативних чинників як-от:

- невідповідність інфраструктури інфокомунікацій держави, рівня її розвитку та захищеності сучасним викликам;
- недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів від кіберзагроз і недосконаліть організаційно-правових механізмів державного управління забезпеченням кібербезпеки та кіберзахисту;
- безсистемність щодо заходів кіберзахисту критичної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;
- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки;
- неузгодженість компетенції між суб'єктами забезпечення кібернетичної безпеки у виконанні окремих функцій і завдань держави у відповідному напрямку державної політики;
- відсутність універсальних вимог до технічних завдань на створення або модернізацію публічних реєстрів, інформаційно-телекомунікаційних систем та баз даних;
- відсутність в нормах законодавства України спеціальних заходів адміністративного та кримінального припинення протиправної поведінки громадян і юридичних осіб, що містить ознаки загроз для кібербезпеки, тощо.

Серед вказаних негативних факторів особливо небезпечне значення має недосконаліть організаційно-правових механізмів державного управління забезпеченням кібербезпеки та кіберзахисту, а саме їх неповнота, декларативність, суперечливість, нечіткість, фрагментарність, некоординованість і неузгодженість між собою.

Відповідно до рішення Ради національної безпеки та оборони України, затвердженого Указом Президента України «Про організацію планування в секторі безпеки і оборони України» від 16 травня 2019 року № 225/2019 [3], передбачено проведення ряду оглядів, зокрема оборонного, огляду загальнодержавної системи боротьби з тероризмом, огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом тощо.

Вказані огляди можуть проводитись або в рамках комплексного огляду сектору безпеки та оборони чи виокремлено. Нині більшість таких оглядів вже проведено.

У 2019 році рішеннями Уряду (Постанови Кабінету Міністрів України «Про затвердження Порядку проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ» від 22 травня 2019 р. № 07, «Про затвердження Порядку проведення огляду оборонно-промислового комплексу» від 22 травня 2019 р. № 490 та «Про затвердження Порядку проведення оборонного огляду Міністерством оборони» від 31 жовтня 2018 р. № 941 зі змінами згідно з Постановою Кабінету Міністрів України № 911 від 06.11.2019) та Президента України (Укази Президента України «Про Порядок проведення огляду розвідувальних органів України» від 9 серпня 2019 року № 589/2019 та «Про Порядок проведення огляду загальнодержавної системи боротьби з тероризмом» від 9 липня 2019 року № 506/2019) були розроблені та затверджені уніфіковані порядки проведення вищевказаних оглядів, за якими було оцінено стан готовності сектору безпеки та оборони у відповідних сферах (за виключенням огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, відповідний порядок якого так і не було затверджено Урядом, а сам огляд не здійснювався).

Результати зазначених оглядів є основою для формування сукупності взаємопов'язаних довгострокових документів, визначених Законом України «Про національну безпеку України», насамперед чергової Стратегії національної безпеки України та нових Стратегії воєнної безпеки України, Стратегії громадської безпеки та цивільного захисту України, Стратегії розвитку оборонно-промислового комплексу України, Стратегії кібербезпеки України, Національної розвідувальної програми, на базі яких розробляють Стратегічний оборонний бюлетень, державні цільові програми та інші середньострокові та короткострокові документи з планування у сферах національної безпеки та оборони.

Тому, з метою посилення правового, організаційного та методичного забезпечення проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури необхідно розробити та затвердити Кабінетом Міністрів України порядок його здійснення, а також із урахуванням міжнародного досвіду та багаторічного національного досвіду, наприклад, оборонного огляду Міноборони, розробити та прийняти низку таких підзаконних актів:

- рекомендації з планування огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури на основі спроможностей;
- порядок проведення перевірок правоохоронними органами діяльності розпорядників та адміністраторів публічних реєстрів, баз даних, а також інформаційно-телекомунікаційних систем на предмет виявлення і запобігання прояву загроз для кібернетичної безпеки держави, суспільства, окремих громадян і юридичних осіб;
- порядку організації та виконання проектів державно-приватного партнерства у сфері забезпечення кібернетичної безпеки держави, територіальних громад та міжнародних урядових організацій, чиї офіційні представництва розташовані на території України [4];
- порядку забезпечення кібернетичної безпеки державних и муніципальних ресурсів, розміщення або управління якими здійснюється з використанням технологій «хмарних» обчислень;
- план заходів з проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, які деталізують і конкретизують завдання та заходи, кількісні та якісні показники, виконавців, очікувані результати огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Практична реалізація наведених пропозицій безпосередньо відображає завдання діяльності держави щодо посилення технічного захисту інформації в публічних реєстрах та інформаційно-телекомунікаційних системах, узгодження структури даних, що в них зберігаються чи обробляються, а також модернізації ІТ-архітектури відповідних об'єктів з метою забезпечення їхньої інтероперабельності, технічної нейтральності та захищеності від зовнішніх загроз.

Саме ці завдання обумовили видання Президентом України 29.07.2019 Указу «Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг» за № 558/2019, основна мета якого полягає у посиленні безпеки національних електронних ресурсів і систем, з використанням яких здійснюється надання електронних адміністративних послуг чи обробка персональних даних громадян України та осіб, які на законних підставах перебувають у нашій державі [5].

Враховуючи присутність проблематики кібербезпеки майже в усіх сферах національної безпеки та оборони, визначених статтею 17 Конституції України та Законом України «Про національну безпеку України», важливим аспектом є включення до звітів про результати проведення комплексного огляду сектору безпеки та оборони та окремих його оглядів оцінок стану виконання завдань основними суб'єктами національної системи кібербезпеки в рамках їх компетенцій, передбачених статтею 8 Закону України «Про основні засади забезпечення кібербезпеки України», та забезпечення надання цієї інформації Державній службі спеціального зв'язку та захисту інформації України як «державному органу, що забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури».

Так, згідно з п. 1, п. 3–п. 5 ст. 27 Закону України «Про національну безпеку України» та ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» в окремі огляди повинні бути включені оцінки стану [6]:

- кібероборони – в оборонному огляді;
- боротьби з кіберзлочинністю – в огляді громадської безпеки та цивільного захисту;
- боротьби з кібершпигунством та кібертероризмом – в огляді загальнодержавної системи боротьби з тероризмом;
- загроз національній безпеці України у кіберпросторі – в огляді розвідувальних органів;
- забезпечення спроможностей основних суб'єктів національної системи кібербезпеки шляхом постачання нових і модернізації наявних зразків спеціальної техніки – в огляді оборонно-промислового комплексу України тощо.

В деяких порядках проведення окремих оглядів (оборонного огляду Міністерством оборони України, огляду оборонно-промислового комплексу Міністерства розвитку економіки, торгівлі та сільського господарства України, огляду загальнодержавної системи боротьби з тероризмом передбачено створення відповідних міжвідомчих (робочих) груп, до складу яких можуть бути включені і представники Державної служби спеціального зв'язку та захисту інформації України, через яких може здійснюватися необхідна комунікація в інтересах, у тому числі, формування загальної оцінки стану кібербезпеки та кіберзахисту. Але, як доводить практика, ефективність цього механізму взаємодії поки що достатньо низька і не в усіх оглядах він взагалі застосовується. Так, наприклад, в огляді громадської безпеки та цивільного захисту Міністерства внутрішніх справ України, де порядком проведення огляду взагалі не передбачено представників від інших державних органів та Національного інституту стратегічних досліджень, що ускладнює формування загальної оцінки стану кібербезпеки, оскільки питання боротьби з кіберзлочинністю є її важливою складовою.

Збирання та узагальнення інформації про стан кібербезпеки можливо здійснювати на рівні Уряду (Державної служби спеціального зв'язку та захисту інформації України), але за умов організації інформаційної взаємодії щодо результатів проведення оглядів розвідувальних органів (Служба зовнішньої розвідки України та Головне управління розвідки Міністерства оборони України) та загальнодержавної системи боротьби з тероризмом (Служба безпеки України) в частині загроз національній безпеці України у кіберпросторі та боротьби з кібершпигунством та кібертероризмом відповідно, а також на рівні Рада національної безпеки і оборони України (основний варіант, визначений законодавством) при формуванні чергової Стратегії кібербезпеки України, насамперед на базі Національного координаційного центру кібербезпеки, якій згідно із законодавством (Указ Президента України «Про Національний координаційний центр кібербезпеки від 7 червня 2016 року № 242/2016») є замовником цього документу та здійснює аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Але внаслідок недостатнього ресурсного забезпечення цього центру, насамперед кадрового, існує проблема результативності виконання покладених на нього завдань.

Інформаційну взаємодію окремих оглядів доцільно також організувати і на рівні Національного інституту стратегічних досліджень, який згідно із законодавством (Законом України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України») визначено відповідальним за науково-методичне забезпечення проведення комплексного огляду сектору безпеки і оборони та деяких його окремих складових.

Незважаючи на таку багатоваріантну можливість застосування механізмів взаємодії окремих оглядів щодо питань кібербезпеки, ні один з них на сьогодні не є дієвим. Тому з урахуванням організаційних змін в сфері кібербезпеки, зокрема створення Міністерства цифрової трансформації України та підпорядкування йому Державної служби спеціального зв'язку та захисту інформації України, необхідно уточнити їх повноваження, насамперед шляхом внесення відповідних змін до Законів України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України» та «Про національну безпеку України», у тому числі щодо правового механізму проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, зокрема механізму взаємодії окремих оглядів з питань кібербезпеки, так і в цілому механізм формування та виконання Стратегії кібербезпеки України, а також визначити головним координатором процесу проведення цього огляду саме Національний координаційний центр кібербезпеки України.

У контексті практичної реалізації вказаних змін, важливою проблемою, яка буде вимагати свого вирішення є нормативне визначення критеріїв розмежування компетенції уповноважених суб'єктів. На наш погляд, у значенні таких критеріїв можуть виступати завдання діяльності уповноважених суб'єктів владних повноважень, безпосередній зв'язок їхніх повноважень з правовими інструментами, що застосовуються у цілях організації та підготовки оглядів, зокрема: нормативне регулювання, моніторинг стану забезпечення кібербезпеки, запити на одержання службової інформації, доступ та допуск до державної

таємниці, перевірка об'єктів критичної інфраструктури тощо. Поряд з цим, важливою умовою подальшої реалізації вказаних рекомендацій залишається забезпечення виконання розпорядниками публічних реєстрів та інформаційно-телекомунікаційних систем функцій з організації експертно-технічного обстеження відповідної категорії інформаційних об'єктів з метою формування оглядів, проведення їх належного технічного, управлінського та безпекового аудиту, встановлення спроможності протистояти можливим кіберризикам і кіберзагрозам.

На відміну від всіх інших оглядів (комплексного та його окремих складових), визначення яких наведено чи безпосередньо в Законі України «Про національну безпеку України», чи у відповідних порядках на проведення окремих оглядів, в законодавстві відсутнє чітке визначення як «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури», так і «огляду національної системи кібербезпеки», передбаченого пп. 3 ст. 8 Закону України «Про основні засади кібербезпеки в Україні» та чинною Стратегією кібербезпеки України, а також їх взаємозв'язок між собою.

Серед фахівців представлено два основних підходи щодо розуміння взаємозв'язку між цими невизначеними термінами, але за якими згідно до законодавства необхідно проводити окремі відповідні огляди. Згідно з першим підходом вважається, що ці терміни ідентичні, тобто в різних законодавчих актах одну й ту ж процедуру огляду названо по-різному. З таким підходом важко погодитись, насамперед тому, що ці огляди відповідно до Закону «Про основні засади забезпечення кібербезпеки України» охоплюють в основному різні за масштабом та функціями об'єкти огляду. Так, основними об'єктами огляду національної системи кібербезпеки є:

- конституційні права і свободи людини і громадянина;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- об'єкти критичної інфраструктури.

Об'єктами кіберзахисту вищевказаним Законом України визначено:

- комунікаційні системи всіх форм власності, в яких обробляють національні інформаційні ресурси, та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
- об'єкти критичної інформаційної інфраструктури;
- комунікаційні системи, які використовують для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Порівняння цих наборів об'єктів показує, що другий перелік є складовим першого, де об'єкти критичної інфраструктури охоплюють об'єкти критичної інформаційної інфраструктури, а комунікаційні системи є важливими елементами організаційно-технічної системи держави, як і об'єкти критичної інфраструктури.

Теж саме стосується і суб'єктів забезпечення цих процедур. Перелік суб'єктів забезпечення кібербезпеки чітко визначено законодавством і системно представлено у вигляді ієрархічної моделі трьох взаємодіючих переліків суб'єктів забезпечення кібербезпеки: переліку суб'єктів загальнодержавного рівня координації (Президент України, Рада національної безпеки і оборони України, Національний координаційний центр кібербезпеки України, Кабінет Міністрів України), переліку суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, та переліку основних суб'єктів національної системи кібербезпеки.

Перелік суб'єктів забезпечення кіберзахисту законодавством конкретно не визначено, але його модель також має ієрархічну структуру і включає ті ж самі верхні ланки переліків суб'єктів, що і в моделі переліків суб'єктів забезпечення кібербезпеки. Нижча ланка цього переліку суб'єктів, виходячи з їх функцій, включає Державну службу спеціального зв'язку та захисту інформації України та підпорядковані їй Державний центр кіберзахисту та Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA.

Тому, відповідно до другого підходу вважається, що взаємозв'язок між вищевказаними процедурами та поняттями характеризується співвідношенням загального та часткового, де «огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури» необхідно розглядати як невід'ємну специфічну техніко-технологічну складову більш загальної процедури, а саме «огляду національної системи кібербезпеки». Інші складові «огляду національної системи кібербезпеки» спрямовані на отримання оцінки стану готовності системи забезпечення кібербезпеки, насамперед її основними суб'єктами національної системи кібербезпеки щодо виконання покладених на них завдань, у тому числі щодо боротьби з кіберзлочинами, кібертероризмом, кібершпигунством, до відбиття воєнної агресії у кіберпросторі (кібероборони), здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі тощо. Їх оцінка має здійснюватися в рамках проведення вищевказаних оглядів в інтересах оцінки стану кібербезпеки за відповідними напрямками.

Законом України «Про основні засади забезпечення кібербезпеки України» визначено терміни кібербезпека та кіберзахист, їх об'єкти та суб'єкти, поняття національної системи кібербезпеки, її основні суб'єкти, їх завдання, шляхи забезпечення функціювання цієї системи, аналіз яких дозволяє стверджувати що кіберзахист є складовою більш загального поняття кібербезпека. Кіберзахист, згідно із Законом України «Про основні засади забезпечення кібербезпеки України», в основному обмежується заходами криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури, кібербезпеки як захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі та «кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціювання комунікаційних, технологічних систем», з яких також випливає, що кібербезпека є більш загальним поняттям порівняно з кіберзахистом [7].

Відсутність визначення або неоднозначність цих термінів ускладнює, стримує процес розвитку цього огляду, вирішення відповідних практичних завдань при його реалізації.

Слід зазначити, що в Україні законодавча база з питань кібербезпеки та кіберзахисту в цілому створена, має ієрархічну структуру та знаходиться в перманентному динамічному розвитку, намагаючись відповідати сучасним світовим тенденціям, новим викликам та загрозам в цій сфері, потребам та вимогам громадян, суспільства та держави, міжнародним зобов'язанням України щодо надійного захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

У попередніх дослідженнях [8, 9], було запропоновано визначення «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури» як процедури періодичного спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем (надалі – «ІТС»), в яких обробляються та зберігаються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом; спостереження стану кіберзахисту – активне, систематичне, цілеспрямоване, планомірне і вивчення реального стану кіберзахисту, спрямованих на запобігання кіберінцидентам, виявлення, попередження та припинення кібератак, ліквідацію їх наслідків, здатності об'єктів критичної інформаційної інфраструктури до відновлення роботи після кібератак та кіберінцидентів.

Законодавчого упорядкування потребують відносини щодо забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків з метою формалізації яких у Державній службі спеціального зв'язку та захисту інформації України було розроблено, але так і не затверджено проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків». Відсутність цього документу суттєво знижує ефективність державної політики забезпечення кібербезпеки.

Особливо значних зрушень вона набула за останні п'ять років і станом на 2020 рік вона містить низку таких важливих актів національного законодавства як: Конституцію України, закони України «Про інформацію», «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні довірчі послуги», «Про захист персональних даних» тощо, а також підзаконні акти, затверджені Президентом України та Урядом, а саме: Про Стратегію національної безпеки України, Про Концепцію розвитку сектора безпеки і оборони України; Про Стратегічний оборонний бюлетень України, Про Національний координаційний центр кібербезпеки, Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації, Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку, Про схвалення Концепції створення державної системи захисту критичної інфраструктури [10], Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури тощо.

Міжнародні зобов'язання України в цій сфері складаються, насамперед, з Будапештської конвенції (Конвенція про кіберзлочинність Ради Європи), яка була ратифікована Україною у 2005 році. Вкрай важливим міжнародним документом в цій сфері є Директива щодо мережевої та інформаційної безпеки (Директива NIS або The Directive on security of network and information systems), яка була прийнята Європейським парламентом у 2016 році, яка передбачає низку організаційно-правових та комунікативних заходів, спрямованих на підвищення загального рівня кібербезпеки в ЄС. Незважаючи на те, що Директива NIS не є обов'язковою для України як країни не члена ЄС, її базові положення є корисним для формування національної публічної політики та адміністрування в сфері кібербезпеки та кіберзахисту.

Конституція України визначає національні цінності, які трансформуються в національні інтереси – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її

громадян – захист яких, згідно її ст.17 Конституції України є найважливішими функціями держави, справою всього Українського народу.

Це зумовлено проголошенням в нормах ст. 3 Основного Закону змістоспрямовуючого значення прав і свобод людини для визначення напрямів діяльності держави, визначення засад її юридичної відповідальності перед людиною за свою діяльність.

«Відповідно, як соціальні цінності, права і свободи людини не лише визначають міру можливої (дозволеної) поведінки, умови задоволення індивідуальних інтересів і потреб у публічно-правових відносинах, але й виступають засобом встановлення змісту та спрямованості діяльності держави, зумовлюють коло обов'язків суб'єктів публічного адміністрування, а також відображають критерії соціальної значущості конкретних цінностей, які повинні перебувати під охороною держави» [11, с. 136].

Саме Закон «Про основні засади забезпечення кібербезпеки України» визначає основні об'єкти кіберзахисту, які створюють критичну інфраструктуру країни, нормативно закріплює понятійний апарат у сфері кібербезпеки на найвищому рівні, регламентує принципи забезпечення кібербезпеки та національну систему кібербезпеки, окреслює державно-приватну взаємодію у сфері кібербезпеки та встановлює відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів щодо забезпечення кібербезпеки України [6].

Цей Закон України визначає також правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Але цей Закон України «Про основні засади забезпечення кібербезпеки України» є головним чином рамковим документом, він юридично визначає ключові поняття у сфері кібербезпеки і здійснює спробу, на нашу думку, не досить вдалу, розподілити сфери відповідальності державних органів у сфері захисту інформації. Частина законопроекту просто переказує ключові положення Стратегії кібербезпеки і не містить чогось нового. Закон визначає необхідність впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки і кіберзахисту.

## Висновки з дослідження і перспективи подальших розвідок у цьому напрямку

1. Необхідно забезпечити одночасну розробку та взаємоузгоджені за змістом зміни до Закону України «Про основні засади забезпечення кібербезпеки України» та проекту Закону України «Про об'єкти критичної інфраструктури та їх захист».

2. Внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України» щодо його деталізації та конкретизації механізмів реалізації шляхів державно-приватного партнерства в сфері кібербезпеки та проведення оглядів кібербезпеки та кіберзахисту.

3. Врахувати в Законах України «Про основні засади забезпечення кібербезпеки в Україні», «Про національну безпеку України», «Про Державну службу спеціального зв'язку та захисту інформації України» зміни, які відбулись у сфері кібербезпеки, а саме появу Міністерства цифрової трансформації України і підпорядкування їй Державної служби спеціального зв'язку та захисту інформації України.

4. Відповідно до п. 4 ст.10 Закону України «Про національну безпеку України» передбачити розробку «Білої книги кібербезпеки», не рідше ніж раз на три роки, а також перенести цю норму в нову редакцію Закону України «Про основні засади забезпечення кібербезпеки в Україні».

5. Розробити та прийняти порядок проведення «оглядів національної системи кібербезпеки» та «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури».

6. Адаптувати національне законодавство у сфері забезпечення кібербезпеки до міжнародного, насамперед, до NIS Директиви (The Directive on security of network and information systems).

7. Утворити у судах загальної юрисдикції України спеціальні колегії з розгляду справ, пов'язаних із розгляду IT-спорів та питаннями , пов'язаними із кібербезпекою.

8. Розробити та прийняти проект Державної цільової програми з розвитку кібербезпеки.

9. Гармонізувати міжнародні стандарти в сфері кібербезпеки.

10. Здійснити кодифікацію, розробити та прийняти Інформаційний кодекс України (Кодекс України про інформацію).

11. Забезпечити адаптацію наявної інфраструктури державних установ до вимог кібербезпеки, насамперед у частині роботи державних службовців із електронними засобами (е-пошти тощо), стаціонарного та мобільного зв'язку, користування відкритим сегментом глобальної мережі Інтернет.

12. Розробити механізм проведення регулярного аудиту об'єктів критичної інфраструктури та програми кібернавчання публічних службовців, уповноважених посадових осіб підприємств – адміністраторів публічних реєстрів, інформаційних систем.

13. Розробляти, впроваджувати, оновлювати різні освітні програми у закладах вищої освіти щодо кібербезпеки та кібергігієни з проведенням круглих столів, міжнародних конференцій, симпозіумів.

14. Стимулювати розвиток програм державно-приватного партнерства у сфері забезпечення кібербезпеки, включаючи аспекти оновлення національної інформаційної інфраструктури, за винятком критичної.

## Література


1. Указ Президента України від 15.03.2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». *Урядовий кур'єр* від 18.03.2016-№ 52.
2. Указ Президента України від 26.05.2015 року № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». *Урядовий кур'єр* від 29.05.2015-№ 95.
3. Указ Президента України від 16.05.2019 року №225/2019 «Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України». *Урядовий кур'єр* від 18.05.2019-№ 92.
4. Дубов Д.В. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с.
5. Указ Президента України від 29.07.2019 року № 558/2019 «Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг». *Урядовий кур'єр* від 31.07.2019-№ 144
6. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. С. 403.
8. Семенченко А.І., Мялковський Д.В., Станіславський Т.В. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури . Інвестиції: практика та досвід, м. Київ, № 18 вересень 2018 року. С. 87–95.
9. The Directive on security of network and information systems. [Електронний ресурс]. Режим доступу: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
10. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. *Урядовий кур'єр* від 10.01.2018-№ 5.
11. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект. Заярний О.А.: монографія / О.А. Заярний. Київ: Видавничий дім «Гельветика», 2017. 700 с.


## References


1. Decree of the President of Ukraine (2016). On the decision of the National Security and Defense Council of Ukraine dated On the Cyber Security Strategy of Ukraine. Government Courier (52). (in Ukrainian)
2. Decree of the President of Ukraine (2015) № 287. On the decision of the National Security and Defense Council of Ukraine On the National Security Strategy of Ukraine . Government Courier (95) (in Ukrainian).
3. Decree of the President of Ukraine (2019) № 225. On the decision of the National Security and Defense Council of Ukraine. On the organization of planning in the security and defense sector of Ukraine . Government Courier (92).(in Ukrainian)
4. Dubov D.V. (2018). Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine. Kyiv: NISD (in Ukrainian)
5. Decree of the President of Ukraine. (2019) № 558 On some measures to improve access of individuals and legal entities to electronic services" .Government Courier ( 144). (in Ukrainian)
6. On National Security of Ukraine: Law of Ukraine (2018). Bulletin of the Verkhovna Rada of Ukraine. (31). St. 241. (in Ukrainian)
7. On the basic principles of cybersecurity of Ukraine: Law of Ukraine. (2017). Bulletin of the Verkhovna Rada of Ukraine.(45). St.403. (in Ukrainian)
8. Semenchenko A.I., Mialkovskyi D.V., Stanyslavskyi T.V. (2018).Scientific and methodological approaches to the review of cyber protection of state information resources and critical information infrastructure. Investments: practice and experience.(18).P.87-95.(in Ukrainian)
9. The Directive on security of network and information systems Avaibale from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive(in English)[Accessed 15/03/2020]
10. The concept of creating a state system of critical infrastructure protection (2017) № 1009-r. Government Courier dated 10.01.2018-№ 5.(in Ukrainian)
11. Zayrnyi O.A. (2017). Legal support of the development of the information sphere of Ukraine: administrative-tort aspect. Kyiv: Vidavnichyi dim Gelvetika(in Ukrainian)


Одержано 02.03.2020

***Про авторів:***


*Семенченко Андрій Іванович,*
доктор наук з державного управління, професор,
директор Інституту вищих керівних кадрів.
Кількість наукових публікацій в українських виданнях – 160.
Кількість наукових публікацій в зарубіжних виданнях – 12.
http://orcid.org/0000-0001-6482-3872,

*Плескач Валентина Леонідівна,*
кандидат технічних наук,
доктор економічних наук, професор,
завідувачка кафедрою прикладних інформаційних систем.
Кількість наукових публікацій в українських виданнях – 188.
Кількість наукових публікацій в зарубіжних виданнях – 15.
http://orcid.org/0000-0002-4700-6704,

*Заярний Олег Анатолійович,*
доктор юридичних наук,
доцент.
Кількість наукових публікацій в українських виданнях – 52.
Кількість наукових публікацій в зарубіжних виданнях – 10,

*Плескач Марія Василівна,*
аспірантка.
Кількість наукових публікацій в українських виданнях – 15.
Кількість наукових публікацій в зарубіжних виданнях – 2.

***Місце роботи авторів:***

Національна академія державного управління
при Президентові України
03057, м. Київ, вул. Антона Цедіка, 20.
Тел.: (097) 3559 127.
E-mail: Andrii.Semencenko@gmail.com,

Київський національний університет імені Тараса Шевченка,
вулиця Володимирська, 60, Київ, 01033.
Тел.: (067) 3792 157.
E-mail: v_pleskach@ukr.net,

Київський національний університет імені Тараса Шевченка,
вулиця Володимирська, 60, Київ, 01033.
Тел.: (067) 3171 882.
E-mail: oleganalitik.knu@gmail.com,

Київський національний університет імені Тараса Шевченка,
вулиця Володимирська, 60, Київ, 01033.
Тел.: (093) 5809 672.
E-mail: pleskachmarija@gmail.com