УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук,* співробітник СБ України

ПОВНОВАЖЕННЯ СБ УКРАЇНИ ЯК СУБ'ЄКТА НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Анотація. *У статті досліджуються питання визначення повноважень Служби безпеки України як суб'єкта національної системи кібербезпеки з урахуванням процесів реформування державного органу спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку.*

Ключові слова*: Служба безпеки України, кібербезпека, повноваження, функція, державні електронні інформаційні ресурси.*

Summary. *The article deals with defining of the authority of the Security Service of Ukraine as a subject of national cybersecurity system regarding the reformation of the special governmental body with law enforcement functions ensuring state security.*

Keywords: *Security Service of Ukraine, Cybersecurity, Authority, Function, State Electronic Information Recourses*

Аннотация. *В статье исследуется вопросы определения полномочий Службы безопасности Украины как субъекта национальной системы кибербезопасности с учетом процессов реформирования государственного органа специального назначения с правоохранительными функциями, который обеспечивает государственную безопасность.*

Ключевые слова: *Служба безопасности Украины, кибербезопасность, полномочия, функция, государственные электронные информационные ресурсы.*

Постановка проблеми. Концепція розвитку сектору безпеки і оборони України, яка визначає шляхи формування національних безпекових та оборонних спроможностей, зорієнтована серед іншого на створення національної системи реагування на кризові ситуації, своєчасне виявлення, запобігання та нейтралізацію зовнішніх і внутрішніх загроз національній безпеці, гарантування особистої безпеки, конституційних прав і свобод людини і громадянина, забезпечення кібербезпеки [1].

Реформування Служби безпеки України відповідно до зазначеної Концепції спрямовуватиметься на посилення її спроможностей протидіяти сучасним зовнішнім і внутрішнім загрозам національній безпеці та здійснюватиметься у напрямі оновлення доктринальних і концептуальних підходів до організації діяльності Служби безпеки України, функціональної оптимізації її організаційної структури та вдосконалення матеріально-технічного забезпечення. Значна частина повноважень СБ України буде спрямована на вирішення завдань попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством; протидії кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога стосовно захисту якої встановлена законом, критичної інформаційної інфраструктури та її окремих об'єктів; здійснення тестування готовності захисту об'єктів критичної інформаційної інфраструктури до можливих кібератак та кіберінцидентів; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки [1; п. 3.9].

Тому вирішення питання щодо наділення СБ України окремими повноваженнями в означеній сфері потребує ґрунтовного наукового аналізу чинного законодавства України, а також місця СБ України у національній системі кібербезпеки.

Результати аналізу наукових публікацій свідчать про те, що питання діяльності СБ України у сфері забезпечення інформаційної безпеки держави було предметом досліджень багатьох українських учених, а саме М.М. Галамби, М.В. Гребенюка, О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, В.Б. Хлевицького, О.М. Юрченка та інших. Однак розкриття функцій та повноважень СБ України як суб'єкта національної системи кібербезпеки були предметом досліджень тільки частково.

Метою статті є розкриття повноважень СБ України як суб'єкта національної системи кібербезпеки.

Виклад основного матеріалу. Закон України "Про національну безпеку України" від 21 червня 2018 року визначив СБ України державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

1) протидію розвідувально-підривній діяльності проти України;

2) боротьбу з тероризмом;

3) контррозвідувальний захист… кібербезпеки… та інформаційної безпеки держави, об'єктів критичної інфраструктури [2, ст. 19].

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" національну систему кібербезпеки становлять суб'єкти забезпечення кібербезпеки та взаємопов'язані заходи політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [3, ст. 8].

Словосполучення "контррозвідувальний захист кібербезпеки" при визначенні відповідної функції СБ України видається не зовсім коректним. Вважаємо, що кращим для використання і позначення функції СБ України буде термін "контррозвідувальне забезпечення кібербезпеки" як складової національної безпеки.

Служба безпеки України визначена одним із основних суб'єктів національної системи кібербезпеки разом з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку України), Національною поліцією України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України [3, ст. 8].

Завданнями основних суб'єктів національної системи кібербезпеки відповідно є:

1) Держспецзв'язку забезпечує – захист у кіберпросторі державних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури, створення та функціонування Національної телекомунікаційної мережі; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформування про кіберзагрози та методи захисту від них; забезпечення впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури; забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA тощо. Варто відзначити, що впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних

складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань [3, ст. 8].

2) Національна поліція України – захист від злочинних посягань у кіберпросторі; здійснення заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Міністерство оборони України, Генеральний штаб Збройних Сил України – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); впровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану тощо.

4) розвідувальні органи України – здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

5) Національний банк України – опікується питаннями забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів; створює центр кіберзахисту НБУ, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

Служба безпеки України в свою чергу здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [3, ст. 8].

Безумовно, значну частину заходів щодо забезпечення кібербезпеки здійснює Держспецзв'язку України поряд із забезпеченням функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань [2, ст. 22].

Національна система кібербезпеки України на сьогодні перебуває у стадії свого формування, а тому існують питання, які потребують нагального вирішення. Так, наприклад, Закон України "Про національну безпеку України" передбачає здійснення комплексного огляду сектору безпеки і оборони, зокрема й огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Однак на сьогодні такий огляд не проведено. Більше того, Кабінет Міністрів України не затвердив порядок проведення комплексного огляду сектору безпеки і оборони у сфері кібербезпеки. У документах, які датуються 2015 роком і стосуються плану заходів з проведення комплексного огляду сектору безпеки і оборони України та методичних

рекомендацій щодо його проведення [4] відсутні питання огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. На нашу думку, такий огляд має стати основою для оновлення Стратегії кібербезпеки України, яка на сьогодні вже не повною мірою відповідає вимогам часу.

Для її оновлення існують й інші аргументи. Так, Закон України "Про національну безпеку України" визначає, що Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [2, ст. 31].

Разом з тим, варто відзначити, що в Україні Стратегія кібербезпеки України як "документ 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 щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів" [2, ст. 31] прийнята до закріплення відповідного визначення у Законі України "Про національну безпеку України" від 21.06.18 р., а саме Указом Президента України від 15.03.16 р. № 96/2016 [5]. Це об'єктивно призвело до того, що сучасна Стратегія кібербезпеки України не містить закріплення концептуальних підходів до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, а також, що найголовніше, – потреб бюджетного фінансування, достатніх для досягнення визначених цілей і виконання передбачених завдань, та основних напрямів використання фінансових ресурсів.

Законодавство України про контррозвідувальну діяльність [6] на сьогодні не містить норм щодо здійснення СБ України контррозвідувальних заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством. І хоча до підстав для проведення контррозвідувальної діяльності віднесено виконання визначених законом завдань щодо контррозвідувального забезпечення економічного, інформаційного, науково-технічного потенціалу, оборонно-промислового і транспортного комплексів та їх об'єктів, національної системи зв'язку, Збройних Сил України та інших утворених відповідно до законів України військових формувань, військово-технічного співробітництва [6, ст. 6], вважаємо за необхідне додатково передбачити такі підстави у Законі України "Про контррозвідувальну діяльність" саме у частині боротьби з кібертероризмом та кібершпигунством, а також протидії кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави.

Закон України "Про Службу безпеки України" також не передбачає повноважень СБ України як суб'єкта національної системи кібербезпеки, хоча передбачає функціональнування підрозділів контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [7]. У новій редакції зазначеного Закону безумовно будуть передбачені повноваження, визначені законодавством про кібербезпеку.

Враховуючи наукову і практичну проблему неімплементованості у чинне законодавство України положень Конвенції про кіберзлочинність у частині обов'язкового зберігання та надання операторами та провайдерами телекомунікацій інформації на вимогу правоохоронних органів, необхідної для розслідування кіберзлочинів [8], не зможуть бути ефективно реалізованими функції СБ України щодо

протидії злочинам проти миру і безпеки людства, які вчиняються у кіберпросторі, кібертероризму, кібершпигунству та кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України.

Крім того, за чинним кримінальним процесуальним законодавством СБ України не має повноважень щодо розслідування кібератак на критичну інформаційну інфраструктуру та державні електронні інформаційні ресурси, як передбачає законодавство України про кібербезпеку. Тому цей напрям удосконалення повноважень СБ України також вважаємо перспективним, особливо з урахуванням відсутності на даний час переліку об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури України.

Розслідування кіберзлочинів є важливою складовою забезпечення кібербезпеки держави. Однак, на сьогодні СБ України фактично позбавлена повноважень щодо оперативної і цілодобової підтримки від іноземних партнерів при запобіганні, виявленні, припиненні та розкритті злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, а також кібертероризму та кібершпигунства. Адже в Україні органом, на який покладаються повноваження щодо "створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України" [9]. Безумовно, при закріпленні повноважень СБ України у процесі її реформування мають бути передбачені можливості для оперативної і цілодобової підтримки відповідних розслідувань.

Висновки.

Підсумовуючи викладене, зазначимо, що у процесі реформування СБ України функція контррозвідувального забезпечення кібербезпеки має бути закріплена однією з пріоритетних з огляду на загрози і виклики національній безпеці в інформаційній сфері.

При удосконаленні повноважень СБ України як суб'єкта національної системи кібербезпеки, відповідального за запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, негласну перевірку готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидію кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на кіберінциденти у сфері державної безпеки мають бути враховані наступні пропозиції автора.

В Україні варто створити нормативно-правову основу для огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Такий огляд стане основою для оновлення Стратегії кібербезпеки України, яка на сьогодні не тільки не повною мірою відповідає вимогам часу, а й не містить окремих положень, передбачених Законом України "Про національну безпеку України" щодо формування та реалізації державної політики з безпечного функціонування кіберпростору і потреб бюджетного фінансування та основних напрямів використання фінансових ресурсів.

У роботі обґрунтовано необхідність внесення змін до законів України "Про контррозвідувальну діяльність" та "Про Службу безпеки України" саме у частині

боротьби з кібертероризмом та кібершпигунством, а також протидії кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави.

Вказано на доцільність внесення змін до кримінального процесуального законодавства України щодо наділення СБ України повноваженнями із розслідування кібератак на критичну інформаційну інфраструктуру та державні електронні інформаційні ресурси, як передбачає законодавство України про кібербезпеку.

Актуалізовано також необхідність наділення СБ України повноваженнями щодо оперативної і цілодобової підтримки від іноземних партнерів при запобіганні, виявленні, припиненні та розкритті злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, а також кібертероризму та кібершпигунства через контактну мережу, яка на сьогодні функціонує лишу у Міністерстві внутрішніх справ України.

Перспективами подальших наукових пошуків визначаємо питання повноважень інших суб'єктів національної системи кібербезпеки.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 4.03.16 р. "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.16 р. № 92/2016. *Офіційний вісник України*. 2016. № 23. Ст. 898.

2. Про національну безпеку України: Закон України від 21.06.18 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

4. Про затвердження плану заходів з проведення комплексного огляду сектору безпеки і оборони України та методичних рекомендацій щодо його проведення: Розпорядження Кабінету Міністрів України від 25.02.15 р. № 139-р. *Урядовий кур'єр*. 2015. № 41.

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

6. Про контррозвідувальну діяльність: Закон України від 26.12.02 р. № 374-IV. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89.

7. Про Службу безпеки України: Закон України від 25.03.92 р. № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.

8. Марущак А.І. Проблеми розслідування кіберзлочинів в Україні. *Економіка. Фінанси. Право*. 2018. № 1. С. 23-27.

9. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5. Ст. 71.

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